Olli Hönö

FROM MOONLIGHT MAZE TO SOLARWINDS: HOW RUSSIAN APT GROUPS OPERATE?

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2023

ABSTRACT

Hönö, Olli
From Moonlight Maze to Solarwinds: How Russian APT groups operate?
Jyväskylä: University of Jyväskylä, 2023, 131 pp.
Cyber Security, Master's Thesis
Supervisor(s): Lehto, Martti

The goal of this thesis was to study how the most advanced and sophisticated cyberattack groups, also known as Advanced Persistent Threat (APT) groups, operate. This was done by analysing data that has been made available by the cyber security industry on APT28, APT29, and Turla, all APT groups that have been connected to Russia. Russian connected groups were chosen because these groups have been considered as particularly active, the groups have been connected to high-profile attacks, and there exists a large amount of data on the groups. The goal of the thesis was motivated by the lack of peer-reviewed research on this topic despite the publicly available data on these groups. The thesis answered the questions "How do APT groups connected to Russia operate?" and "Do APT groups connected to Russia operate in a similar manner?".

The research was conducted by performing qualitative content analysis on the data that is available about these cyberattack groups. A model called the Unified Kill Chain, which was designed to increase the understanding of advanced cyberattacks, was used in the analysis to provide additional structure. The model provided ways to categorize and compare various tactics, techniques, and procedures used by the groups that were studied. The tactics, techniques, and procedures that were identified were used to create models which depict identified attacks by these groups. These tactics, techniques, procedures, and the models which were identified from the data were then used to answer the research questions.

The thesis showed that the cyberattack groups that were chosen to be studied operate with a wide selection of tactics, techniques, and procedures. The groups are capable of changing their tactics, techniques, and procedures if necessary. These groups generally perform their attacks by using malicious emails or by luring their victims into a compromised website with malicious content. These groups generally attack for the purpose of stealing sensitive information. The research also showed that the groups that were studied operate in mostly similar manners. However, some differences could be identified between the groups.

The commonalities among the groups show areas where defenders can focus on and hinder the activities of all of these groups. The differences identified between the groups can potentially offer analysts or researchers points to focus on in future work.

Keywords: Cyberattacks, Tactics, Techniques, Procedures, Advanced Persistent Threat

TIIVISTELMÄ

Hönö, Olli
Moonlight Mazesta Solarwindsiin: Miten venäläiset APT-ryhmät toimivat?
Jyväskylä: Jyväskylän yliopisto, 2023, 131 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Lehto, Martti

Tämän tutkimuksen tavoitteena oli tutkia miten kaikista kehittyneimmät kyberhyökkäyksiä tekevät ryhmät toimivat. Tutkimuksen kohde valittiin koska aiheesta ei ole merkittävästi vertaisarvioitua tutkimusta, vaikka dataa ryhmistä on julkisesti saatavilla. Tutkittaviksi ryhmiksi valikoitui APT28, APT29 ja Turla, kaikki kolme ovat Venäjään liitettyjä ryhmiä. Venäjään liitetyt ryhmät valittiin, koska nämä ryhmät tunnetaan aktiivisina, ryhmiä on yhdistetty useisiin korkean profiilin hyökkäyksiin ja ryhmistä on reilusti tietoa saatavilla. Näiden ryhmien toimintaa tutkittiin analysoimalla dataa, joka ryhmistä on saatavilla eri kyberturvallisuusalan toimijoilta. Tutkimuskysymyksiksi valikoitui ”Miten Venäjään liitetyt kehittyneet kyberhyökkäyksiä tekevät ryhmät toimivat?” ja ”Onko Venäjään liitetyillä kehittyneillä kyberhyökkäyksiä tekevillä ryhmillä keskenään samanlaiset toimintatavat?”

Tutkimus toteutettiin käyttämällä kvalitatiivista sisällönanalyysiä tutkimusmenetelmänä. Tutkimuksen apuna käytettiin myös mallia, joka on luotu kyberhyökkäyksien tutkimiseen. Tämä malli antoi rakenteen, jolla pystyttiin kategorisoimaan ja vertailemaan ryhmien käyttämiä taktiikoita, tekniikoita ja toimintatapoja. Näistä tunnistetuista taktiikoista, tekniikoista ja toimintatavoista luotiin malli, jolla kuvattiin kunkin ryhmän tekemiä hyökkäyksiä. Näiden datasta tunnistettujen taktiikoiden, tekniikoiden, toimintatapojen ja mallien avulla vastattiin tutkimuskysymyksiin.

Tutkimus osoitti, että nämä tutkitut ryhmät toimivat käyttämällä laajaa valikoimaa taktiikoita, tekniikoita ja toimintatapoja. Ryhmät kykenevät vaihtamaan käyttämiään taktiikoita, tekniikoita ja toimintatapoja tarvittaessa. Tutkitut ryhmät käyttävät yleensä hyökkäyksissään haitallisia sähköposteja tai houkuttelevat heidän uhrinsa murretuille verkkosivuille, joihin on lisätty haitallista sisältöä. Ryhmien hyökkäyksissä on yleensä tavoitteena arkaluonteisen tai salaisen tiedon varastaminen. Tutkimus myös osoitti, että ryhmät toimivat yleisesti ottaen samoilla toimintatavoilla. Joitakin eroja ryhmien toimintavavoissa oli kuitenkin löydettävissä.

Löydetyt yhtäläisyydet ryhmien toimintatavoissa antavat puolustajille kohteita, joihin voidaan keskittyä ja mahdollisesti estää kaikkien ryhmien hyökkäyksiä. Löydetyt eriäväisyydet ryhmien kesken antavat tutkijoille mahdollisia jatkotutkimuksien kohteita.

Asiasanat: kyberhyökkäykset, taktiikat, tekniikat, toimintatavat

GLOSSARY

Bootkit	Malicious software that targets the Master Boot Record and is loaded before the operating system, making it particularly difficult to detect (MITRE, 2023a).
Bruteforce	Form of attack where all possible logins, passwords, keys, or other alternatives are tried systematically to find the correct one (MITRE, 2023b).
Certificate	A cryptographic document that can be used, for example, for authentication or encryption (France, 2023).
Cookies	Data stored in a browser, often used to identify, track, or authenticate users (Kaspersky, 2023a).
DLL	Dynamic Link Library (DLL); a library that includes code that can be used by more than one program (Liang, Li, Rugerio, Chen, & Xu, 2023).
DLL injection	Technique where a DLL is injected into a process that is running on a Windows device (MITRE, 2022a).
DLL search order hijacking	Technique where the order in which DLLs are searched for in a system is abused to replace and load a malicious DLL (MITRE, 2023c).
DLL side loading	Technique where a legitimate application is used to load a malicious DLL (MITRE, 2023d).
Domain name	Piece of text that maps to an IP address. A domain name is usually used to refer to a website (Cloudflare, 2023).

Exploit	Often a piece of code or a program meant to take advantage of a vulnerability in a program or system (Cisco, 2023).
Javascript	Programming language often used in web pages to add functionality or dynamic content into them (Mozilla, 2023).
Kerberoasting	Technique where attackers attempt to obtain a specific, weakly encrypted, authentication ticket that can be attacked with a bruteforce attack to get user credentials stored inside (MITRE, 2023e).
Keylogger	Program or tool to record the keystrokes on a device, often done covertly (Malwarebytes, 2023a).
Living off the land	Method of attacking where the attackers use only legitimate and native tools that exist on the system (Kaspersky, 2023b).
LSASS	Local Security Authority Subsystem Service (LSASS) contains a variety of credentials which attackers sometimes try to access (MITRE, 2023f).
Malware	Short for malicious software. An umbrella term for any malicious program (Malwarebytes, 2023b).
Mimikatz	Tool used to steal Windows logins and passwords in various ways (Greenberg, 2017).
Network domain	Grouping of computers or other devices for administrative purposes within the same network (PDQ, 2023).
Password hash	Passwords are often encoded by programs into a long string of characters, called a hash, for added security (Jung, 2021).

Password spraying	Form of attack where lists of commonly used passwords are used against a large number of accounts (MITRE, 2023g).
Phishing	Technique of electronically delivered scam or other social engineering, often done via email (Jansson & Von Solms, 2013).
Powershell	Task automation and management program and language native to Windows (Wheeler & Buck, 2023).
Process injection	Technique where malicious code is injected into another computer process, often to avoid detection or to escalate privileges. (MITRE, 2023h)
PsExec	Tool that is native to the Windows operating system that can be used to execute processes remotely on other systems (Mihaiuc, Kim, & Kasprzyk, 2023).
Responder	Tool for stealing password hashes and other information remotely (Alert Logic, 2023).
Rootkit	Type of malicious software used to remotely control a compromised device with high level of privileges while hiding its presence (ENISA, 2023a).
Script	List of instructions that can be executed by a program or a computer that without being compiled. Often used to automate simple tasks (Techslang, 2019).
SMB	Server Message Block (SMB) is a network file sharing protocol (Ashcraft, Sharkey, Coulter, Batchelor, & Satran, 2021).
Social engineering	The act of manipulating people into giving confidential information or into performing other unsafe actions (ENISA, 2023b).

SSH tunneling	Technique of moving data via an encrypted Secure Shell (SSH) connection (MITRE, 2020a).
Supply chain attack	A type of attack where the less secure elements in the victims’ supply chain are targeted to compromise the victim (Asher-Dotan, 2023).
Token	Object containing authentication information used to authenticate a user (Okta, 2023).
TOR	The Onion Router (TOR); open-source software for communicating over an anonymous network of the same name (The Tor Project, 2023).
UEFI	Unified Extensible Firmware Interface (UEFI) is often used to refer to the interface that connects the computer’s hardware to its operating system (Minhas, 2022).
Vulnerability	Weakness or flaw in a software or a device that can be exploited (Mell, Scarfone, & Romanosky, 2007).
Watering hole	Attack where a website that is frequented by a desired victim is compromised in order to infect the victim (Haaster, Gevers, & Sprengers, 2016).
WMI	Windows Management Instrumentation (WMI); a Windows administration feature (White et al., 2023).

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Cyberattacks hit various Estonian institutions and businesses in 2007 during rising tensions between Estonia and Russia. Many in the west considered these to be the first cyberattacks by a state targeting another state (Landler & Markoff, 2007; Mite, 2007; Traynor, 2007). While these early cyberattacks were not particularly sophisticated or serious, the attacks were seen as a wake-up call for the West, for example, spurring the establishment of the NATO Cooperative Cyber Defence Center of Excellence in Estonia and the creation of the first NATO Policy on Cyber Defense (Juurvee & Mattiisen, 2020; Wiedemar, 2023). Since these early cyberattacks, the attacks have become more sophisticated, brazen, and serious as successful attacks against critical infrastructure like the one against the Iranian uranium enrichment facility at Natanz or the attacks against various Ukrainian power stations have shown (Greenberg, 2019; Zetter, 2014).

The hacking groups behind these attacks have also become more advanced, being capable of targeting a wide range of organizations with different types of attacks over the course of years, while also adapting and improving (Greenberg, 2019). Some of these most sophisticated cyberattacks have often been attributed to groups with connections to nation states and their military or intelligence services (Cybersecurity & Infrastructure Security Agency et al., 2022; Mandiant, 2013; National Cyber Security Centre UK, 2018; Sakaguchi, 2021).

As states are sponsoring and conducting cyberattacks more openly and often, they have been receiving increasing attention in the political sphere as well as the public eye (Buchanan, 2020). Cyberattacks have also been the subject of some academic research, but limited research exists about the most sophisticated hacker groups, the state sponsored, or state-controlled groups often referred to as Advanced Persistent Threat (APT) groups. The cyber security industry has a lot of knowledge and information about these groups, but it has not yet been fully taken advantage of in the academic research community. If this knowledge and information was included more extensively in research, it could improve the understanding of these groups and help the information security professionals defend our societies that are becoming more and more dependent on different information systems.

1.1 Research questions

The aim of this thesis was to gather, synthesize, and analyse the vast amount of information offered by the cyber security industry about the most sophisticated and advanced cyberattack groups. This was done by analysing their differences, similarities, and the methods they have used to understand these groups better. The study was done using scientific methods in order to derive new and valuable information regarding these advanced cyberattack groups. The groups chosen for this study are APT28, APT29, and Turla.

These advanced cyberattack groups that were chosen to be studied are often referred to as Advanced Persistent Threat (APT) groups. All three APT groups that were chosen for this thesis have connections to, and have been specifically attributed to, the Russian state. These groups were selected to give the most comprehensive view of Russian-connected APT groups as they have been connected to different Russian state organizations. Russian-connected groups were selected specifically because these APT groups have been identified as some of the most active in the world as well as being connected to some particularly high-profile attacks (Council on Foreign Relations, 2022; Greenberg, 2019). Additionally, there is a lot of information available on these APT groups. The research questions that were chosen for this thesis were divided into two main research questions with each having two sub-questions:

1. How do APT groups connected to Russia operate?
   - What tactics, techniques, and procedures do Russian connected APT groups use?
   - How are these tactics, techniques, and procedures used by the groups (in attacks/operations)?

2. Do APT groups connected to Russia operate in a similar manner?

   - Are the tactics, techniques, and procedures used by Russian connected APT groups similar between the groups?
   - Are the tactics, techniques, and procedures used by Russian connected APT groups used in a similar way between the groups?

The research questions were chosen to firstly understand the specific technical and tactical ways these groups perform their attacks and secondly to understand if the ways these groups operate are similar to each other. The answers to these questions should increase the understanding of these specific APT groups, APT groups connected to Russia, as well as possibly give some understanding of APT groups in general.

1.2 Thesis structure

The first section of the thesis introduces the broader topic that was chosen to be studied, the research questions, the existing research, and the thesis structure. The second chapter of the thesis covers the subject to be studied more extensively, and it also covers the context surrounding the subject as well as different models, known problems, frameworks and defines terms that relate to the subject and the thesis. Following that, the research methodology section explains the chosen research methodology, data collection and coding methods, and the justification for choosing the research method. The fourth section describes APT groups as a phenomenon, the APT groups that were studied, the operating procedures of the APT groups, and the model created of the operating procedures of each APT group. The fifth chapter covers the analysis of the findings from the previous chapter. The sixth chapter covers the results of the analysis and answers the research questions. The final chapter describes the thesis and discusses the results, possible implications of the findings, limitations of the study, possible applicability of the results, and suggestions on future research.

1.3 Existing research

The existing peer-reviewed research of APT groups has often focused on aspects other than the technical capabilities or tendencies of any specific groups. The existing research instead often focuses on studying APT groups generally or as a phenomenon: For example, Burita and Le (2021) studied APT groups and their activities in general, with no particular focus on any groups or aspects about their activities. Lemay et al. (2018) conducted a survey of publicly available reports on APT groups, offering a short description of many groups, but not going into great detail, and Hussain, Ahmad, & Ghouri, (2021) conducted a meta-analysis of APT research literature to find deficiencies in existing research and give suggestions for future research.

Another aspect the existing peer-reviewed research often focuses on is attempting to find different methods, models, or solutions to detect or defend against attacks by APT groups. For example, Alshamrani, Myneni, Chowdhary, and Huang (2019) conducted case studies about attacks by APT groups and suggested different monitoring and mitigation methods; Hasan, Shetty, Islam, and Ahmed (2022) suggested a new predictive defence strategy against APT attacks based on game theory; and Wen, He, and Yan (2017) suggested a new APT attack detection and prediction solution.

A third notable aspect that has been covered by existing peer-reviewed research is different models and frameworks of APT groups and attacks. For example, Bahrami et al. (2019) suggest a new taxonomy model for APT groups, Lehto (2022) analysed different existing models used to model APT attacks and suggested an improved one, Tatam, Shanmugam, Azam, and Kannoorpatti (2021) assessed multiple different APT attack modelling techniques and systems in different aspects, and Ahmad, Webb, Desouza, and Boorman (2019) studied the strategic aspects of APT groups and suggested a new model to assess the operations of APT groups.

While peer-reviewed research has not yet studied the technical aspects or capabilities of specific APT groups, some non-peer reviewed research on the topic has been done. Some master's thesis level research has also tried to answer similar questions as this paper or cover similar topics. These include, for example, Karsikas (2021), who conducted a multiple case study to compare APT groups related to China and Russia, Vatanen (2020), who also used a multiple case study as a research method to analyse cyberattacks attributed to Russia between 2007 and 2017, Bunda (2020), who conducted a case study of a specific APT group connected to Russia, Huhta (2021), who studied how Russia has conducted offensive cyber operations by using document analysis and Johansson (2021), who used grounded theory to study how the Russian and Chinese military intelligence organizations' use of cyber techniques has evolved.

2 ADVANCED PERSISTENT THREATS

The exact definitions of what is considered an Advanced Persistent Threat (APT) often differ slightly, but generally an APT is considered to be an adversary that is well resourced, sophisticated, experienced, and persistent in attacking some form of information system or infrastructure (Crowdstrike, 2022a; NIST, 2012). In addition to referring to a group or single attacking entity, the term APT can sometimes be used to refer to a specific type of attack or operation (Suojelupoliisi, 2021; U.S General Services Administration, 2022).

Whether referring to a group, entity, attack, or an operation the key aspects in the definitions generally revolve around the three parts of the acronym:

> **Advanced** - The members of the group, operators of the threat or technical or other aspects of the operation suggest an unusual level of sophistication or expertise in the attack. This sophistication or expertise can be shown in the ability to adapt to the situation, staying undetected or simply being able to use a wide variety of technologies and techniques. (ENISA, 2014; NIST, 2012; Suojelupoliisi, 2021)
>
> **Persistent** – The attacks conducted by the entity or group, or the methods used in the attack suggest the attackers have the determination, motivation, and financial means to attack persistently and over long periods of time until their objective has been met. If the attackers gain access to a desired system or network and then lose access, they will attempt to regain access instead of giving up. (ENISA, 2014; NIST, 2012; U.S General Services Administration, 2022)
>
> **Threat** – As Singer (1958) suggested, threat equals capability times intent. The group or the operators of the threat constitute a threat because they have the capability and the intent to act (ENISA, 2014). If defining APT as an operation or an attack instead of an actor or a group of actors, the APT can be seen as a threat because it threatens something seen as valuable, sensitive, and worth protecting (Suojelupoliisi, 2021; U.S General Services Administration, 2022).

Often the definition by the National Institute of Standards and Technology (NIST) has been cited as the most widely and generally accepted definition of an APT (Al-Matarneh, 2020; Niu, Zhan, Li, Yang, & Chen, 2016). Due to the prominence of the definition and the fact that it has changed very little between 2011 when it was first defined by NIST and 2022 in its latest form, this definition will be used in this paper when using the term APT. This first definition from NIST is as follows (NIST, 2011):

> "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives."

2.1 APT attack modelling

APT attacks and attackers have been represented and described by using different models and frameworks for different purposes. These models can be used, for example, by defenders to emulate an adversary by creating scenarios to test out defences, actively hunting threats in an environment instead of passively relying on monitoring and defences, supplementing cyber threat intelligence by giving more tools to understand the adversaries, simply to understand the phases of an attack, or as a basis for research or future models or frameworks (Lehto, 2022; Strom et al., 2020; Wen, He, & Yan, 2017).

There are a wide variety of models and frameworks for different purposes. Tatam, Shanmugam, Azam, & Kannoorpatti (2021) divide these into four different approaches: asset-centric, system-centric, threat-centric, and data-centric. As the goal of this thesis is to study the APT groups, the focus will be on threat-centric approaches.

2.1.1 Lockheed Martin Intrusion Kill Chain

One of the first methods to attempt to model specifically APT cyberattacks was the "Intrusion Kill Chain", also known as Cyber Kill Chain (CKC). This model was introduced in 2011 to specifically assist in combatting APT attacks by offering a new approach to study these intrusions. The "kill chain" refers to a set of steps that the attacker **must** progress through in **succession** to successfully complete their mission. One of the key aspects of the kill chain model is that the defender must only break the kill chain at one point to thwart the attack. This approach is based on methods used by the United States military, for example, to model Improvised Explosive Device (IED) attacks. (Hutchins, Cloppert, & Amin, 2011)

The steps of the Intrusion Kill Chain are (Hutchins, Cloppert, & Amin, 2011):

1. Reconnaissance – In this step the attacker chooses the target and gathers information about them. Practically this could mean using social media, other websites, or port scanning to gain information. (Dargahi et al., 2019; Hutchins, Cloppert, & Amin, 2011)
2. Weaponization – This step includes the attacker creating something malicious that can be delivered to the target, often called a payload. This payload is often some sort of malware disguised as a file or included in a seemingly innocuous Microsoft Word document. (Dargahi et al., 2019)
3. Delivery - The next step is delivering the payload to the target. Often the delivery can be done using an email attachment, a compromised website, or a USB-drive. (Hutchins, Cloppert, & Amin, 2011)
4. Exploitation – The exploitation step consists of the payload being triggered or executed. This can mean the payload using some vulnerability that allows it to be executed. (Hutchins, Cloppert, & Amin, 2011)
5. Installation – In this step the attacker or their payload will attempt to create backdoors to give the attacker remote access to the target or to spread around in the network (Dargahi et al., 2019).
6. Command and Control (C2) – This step typically consists of the attacker gaining control of the compromised target, usually through an outbound connection from the target towards the attacker (Hutchins, Cloppert, & Amin, 2011).
7. Actions on Objectives – In the final step the attacker can perform the actions on the target that lead to completing their original objectives. This could mean data exfiltration, data destruction, or even moving laterally into gaining access to additional targets. (Hutchins, Cloppert, & Amin, 2011)

Some have criticized the CKC for being too focused on a perimeter when, according to critique, this type of thinking fails to address some types of attacks, such as insider threats (Engel, 2014; Korolov & Myers, 2022).

2.1.2 MITRE ATT&CK

Adversarial Tactics, Techniques and Common Knowledge, or more commonly known ATT&CK, is a framework to describe or model possible adversarial actions (Bodeau, Fox, & McCollum, 2018). MITRE ATT&CK was created in 2013 by the American not-for-profit organization MITRE, and publicly released for the first time in 2015. ATT&CK was originally created to be able to systematically categorize the behaviour of adversaries during exercises within the MITRE organization itself. The ATT&CK model has since been used for many other purposes, been expanded, and updated multiple times. In addition to being a model or a framework, ATT&CK also includes a knowledge base that has a wide variety of categorized information about cyberattacks. This information includes different phases of cyberattacks, tactics, techniques, and procedures, also known as TTPs, used by different adversaries, information about the adversaries, and documented cases of attacks. (Strom et al., 2020)

The ATT&CK model is split into tactics, techniques, and sub-techniques. The techniques and sub-techniques are grouped into tactics. Tactics are used to explain the "why" of the underlying techniques and sub-techniques (Strom et al., 2020). One example is the tactic of "Credential Access", i.e., an adversary trying to gain access to access tokens, account names, or passwords, includes a technique of "Brute Force", which refers to the use of iterative or repetitive methods to gain access to an account. This technique in turn includes a sub-technique called "Password Guessing", which means the adversary simply guessing passwords in a repetitive or iterative manner. (MITRE, 2019a, 2022b)

The current version of ATT&CK (ATT&CK Matrix for Enterprise v.14) includes 424 sub-techniques and 201 techniques grouped into 14 tactics (MITRE, 2023i). These tactics include:

1. Reconnaissance – Adversary gathering information to be used to assist in the later steps, this information could be, for example, about the organization to be targeted, its personnel or infrastructure (MITRE, 2020b).
2. Resource Development – Adversary acquiring resources to assist and enable later steps. These resources could be, for example, server infrastructure, accounts, certificates, or malware. (MITRE, 2020c)
3. Initial Access – Adversary gaining the initial access into the desired network. These tactics could be, for example, spear phishing, which refers to specifically targeted phishing, compromising a supply chain, or exploiting a public-facing web application. (MITRE, 2019b)
4. Execution – Adversary enabling code they control to be executed in the victim network or device, such as through the adversary setting a scheduled task to execute their code or using a command-line interface (MITRE, 2019c).
5. Persistence – Adversary creating and maintaining a persistent foothold or a backdoor into the compromised network or device, such as through creating an additional system account or setting a program to run every time the system starts (MITRE, 2019d).
6. Privilege Escalation – Adversary gaining higher-level permissions. This could consist of stealing an account with higher privileges or modifying the domain policy in the environment. (MITRE, 2021)
7. Defense Evasion – Adversary avoiding detection, this could be done by using a hidden user or modifying logs (MITRE, 2019e).

8. Credential Access – Adversary stealing legitimate credentials, such as through password guessing or stealing credentials from password managers (MITRE, 2019a).
9. Discovery – Adversary gaining knowledge about a system and other systems in the same network, such as through network scanning or listing services running on the network (MITRE, 2019f).
10. Lateral Movement – Adversary moving in the network towards the target, such as through legitimate remote services or file sharing services (MITRE, 2019g).
11. Collection – Adversary collecting information that specifically relates to their goal, this could be done by using screen capture or collecting data from a file sharing server (MITRE, 2019h).
12. Command and Control – Adversary using a command & control channel to communicate with the compromised system, this could be done by using a legitimate remote access software or web service (MITRE, 2019i).
13. Exfiltration – Adversary stealing the data they have collected back to systems they control. This could be done through the command and control channel or through a cloud account. (MITRE, 2019j)
14. Impact – Adversary performing malicious actions to the systems or data, such as through data destruction or data encryption (MITRE, 2019k).

2.1.3 Mandiant's Attack Lifecycle Model

The Attack Lifecycle Model was created by the cyber security company Mandiant and originally used by the company in a 2012 technical report to discuss the remediation of targeted cyberattacks. The model is used to describe the sequence of events during a targeted attack as well as to assist organizations in planning their defense. The model suggests that the threats generally follow the presented sequence of events, but also concedes that sometimes the attacks can fall outside this model. (Aldridge, 2012) This same model was then used later in 2013 to describe the actions of a group named APT1 in one of the first publicly reported attribution reports (Mandiant, 2013).

Mandiant's Attack Lifecycle Model consists of eight stages that do not have to occur every time and including some stages that are often repeated in a loop. This loop is then repeated until their mission is completed, or they are removed from the network. (Mandiant, 2013) The stages in the model are:

1. Initial Reconnaissance – Attacker gaining information to identify targets, this could be by analysing the target organization or its employees (Aldridge, 2012).
2. Initial Compromise – Attacker gaining initial access to the target network, this could be done through spear phishing or a social media message containing malicious content (Mandiant, 2013).
3. Establish Foothold – Attackers strengthen their hold on the target network by creating a backdoor into the system (Mandiant, 2013).

4. Escalate Privileges – Attackers acquiring the necessary means to access the network or system that is required to reach their objective, this could be done through, for example, collecting usernames and passwords or certificates (Mandiant, 2013).
5. Internal Reconnaissance – Attackers gaining information about the target environment such as about the network, computers, and their users (Mandiant, 2013).
6. Move Laterally – Attackers gaining access to the required network, often done through compromised credentials (Mandiant, 2013).
7. Maintain Presence – Attackers further strengthening their foothold in the compromised system, often consisting of setting up new backdoors or other means of persistence (Mandiant, 2013).
8. Complete Mission – Attackers completing their initial mission, such as stealing intellectual property or other internal data (Mandiant, 2013).

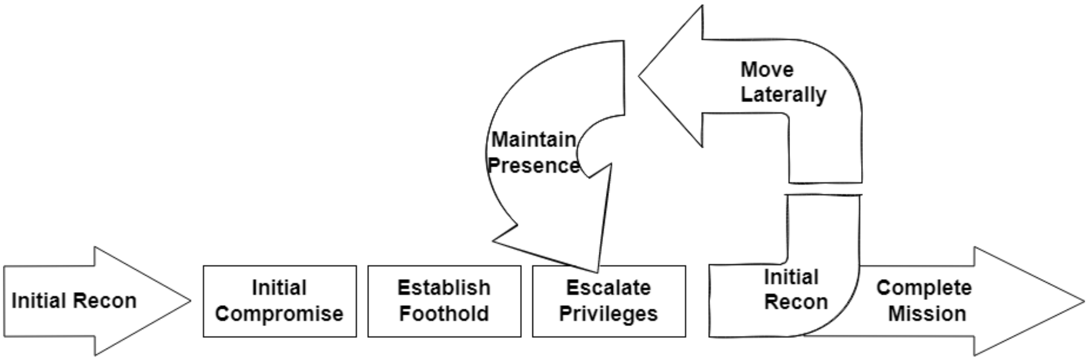


FIGURE 1 Mandiant's Attack Lifecycle Model (Mandiant, 2022a).

2.1.4 Unified Kill Chain

Unified Kill Chain (UKC) is a model suggested by Paul Pols in 2017 to directly improve on the CKC and the ATT&CK models. The UKC was created by combining some elements of ATT&CK and CKC as well as other kill chain variants to cover more attack paths and vectors. (Pols, 2018) The paper describing UKC notes some critique of CKC, notably the assumption that attacks must progress through every stage of the kill chain. This is deemed a faulty assumption and in the UKC this assumption is not followed, tactics can be skipped or repeated. UKC can be used to compare, analyse, and model attacks as well as aid in developing and improving defensive strategies. UKC also allows for structured analysis and comparison of threat intelligence of the tactical operations of threat actors. The UKC can be used to describe the tactics used by attackers in the order in which they typically appear. UKC can also be used to describe real life attacks to build **attack-specific** kill chains, which can be used to analyse attacks or to compare attacks. Another way the UKC can be used is to describe the typical modus operandi of a specific attacker in an **actor-specific** kill chain. This can be used to build defenses against specific attackers. (Pols, 2022)

The UKC includes 18 tactics which describe different phases of an attack. These tactics are further divided into three intermediate goals: **In**, **Through,** and **Out**. Each of these three intermediate goals describes a different larger aspect of the cyberattack and each of these three is its own loop. (Pols, 2022)

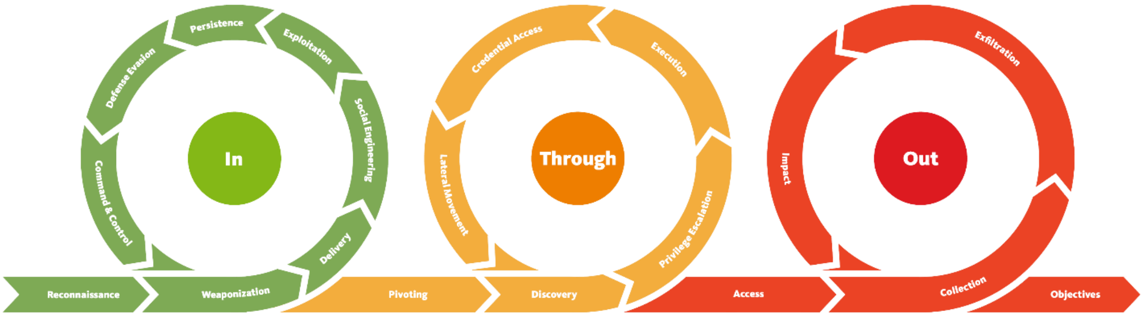


FIGURE 2 The Unified Kill Chain (Pols, 2022).

The "In" intermediate goal describes the phases an attacker may go through to breach into an organization. As sometimes these phases can be thwarted by a defender, they are depicted as a loop that can be repeated as often as necessary until the attacker has gained access. The "In" intermediate goal includes the following phases (Pols, 2022):

1. Reconnaissance – Researching, identifying, and selecting targets using reconnaissance.
2. Resource Development – Setting up infrastructure required for the attack.
3. Delivery – Transmission of the weaponized object to the target environment.
4. Social Engineering – The manipulation of people to perform unsafe actions.
5. Exploitation – Exploiting of vulnerabilities within systems, may result in code execution.
6. Persistence – Access, action, or change that allows the attacker persistence in the system.
7. Defense Evasion – Techniques specifically to avoid detection or other defenses.
8. Command & Control – Attacker's communication to the controlled system.

When the system is breached, and if the final objective requires additional access, the attack can proceed toward the next intermediate goal, "Through". Alternatively, if the breached system offers sufficient access, the attack can continue to the intermediate goal "Out". As with the intermediate goal "In" these phases can be thwarted by the defender or by other circumstances. Because of this the phases are depicted in a loop that can be repeated until the required access in gained.

The phases to reach the "Through" intermediate goal are the following (Pols, 2022):

9. Pivoting – Tunnelling traffic through the controlled system to other, not yet controlled, systems.
10. Discovery – Gaining information about a system and the surrounding systems.
11. Privilege Escalation – Gaining higher permissions on a system or a network.
12. Execution – Execution of attacker's code in the controlled system.
13. Credential Access – Gaining additional credentials within the system.
14. Lateral Movement – Gaining access and control of other systems by moving laterally.

After the required access is gained by the attacker, the attacker can move on to completing their final objectives. The final objectives are completed in the "Out" intermediate goal. Like the previous intermediate goals, this one is also a loop that can be repeated until the objectives are completed. The phases to reach the final objective in the "Out" intermediate goal are the following (Pols, 2022):

15. Collection – Identifying and collecting data from the target network or system.
16. Exfiltration – Removing that data from the target network or system to somewhere controlled by the attacker.
17. Impact – Manipulating, interrupting, or destroying the target system or its data.
18. Objectives – Other socio-technical objectives to achieve a strategic goal.

2.1.5 General APT cyber-attack model

General APT cyber-attack model is a general model suggested in 2022 by Lehto to improve on the shortcomings of previously suggested and used APT attack models and frameworks. The General APT cyber-attack model attempts to improve on the previous models and frameworks by, for example, including an early-attack phase that includes strategic decision-making that is done before the attack is even prepared and a clearly defined end state, both of which have been lacking in the previous models and frameworks. (Lehto, 2022)

The General APT cyber-attack model includes three phases: Early-Attack phase, Pre-Attack phase, and Attack phase. These phases are further divided into eight steps, which are again further divided when necessary. These phases and steps are (Lehto, 2022):

Early-Attack phase:

1. Strategic decision-making – A strategic decision is made about the target, objectives of the attack, and strategic context.

Pre-Attack phase:

1. Reconnaissance – First general reconnaissance is required to create situational awareness and to understand the targets required to achieve the objectives. Secondly scanning will attempt to find vulnerabilities in the target systems and to find more detailed information about the systems.
2. Weaponize – Attacker develops their malware or other exploitation method they plan to use on the target. In addition to malware, the exploitation method might be a malicious website.

Attack phase:

1. Access – Firstly the attacker penetrates the target network, by methods such as spear phishing or by using some vulnerability found in the systems. Secondly the attacker expands their foothold on the system by creating some persistence, such as a backdoor. Next the attacker executes their malicious payload to exploit the vulnerabilities found. After the exploitation the attacker can install further backdoors or other malicious tools necessary. Lastly the attacker actively tries to avoid being detected.
2. Lateral Movement – The attacker probes the network and tries to expand their access and escalate their privileges.
3. Command and Control – Attacker sets up a communication method from the compromised network back to a network they control. They can then control the operation from there.
4. Execution – The attacker executes the steps necessary to complete their mission, this might be data collection and exfiltration or data destruction.
5. End state – If the attacker's objective requires this, the attacker can quietly remove themselves from the systems at this point or remain in them to await possible further missions.

2.2 APT attribution

Attribution of APT attacks or groups is the method by which the actor or actors behind attacks or groups are identified. The level of identification or attribution can differ, it can be as specific as naming and even indicting specific people or simply naming a country of origin. (Steffens, 2020) The motive for and the level of attribution can vary: it can be an organization looking to understand the threats facing them, an individual simply looking to satisfy their curiosity, or a government looking for political or legal justification for a response against the attacker (Steffens, 2020; Stoll, 1998; Tsagourias, 2012).

On the level of states, as cyberattacks could lead to even an armed response, it is very important to get attribution right (Tsagourias, 2012). While the stakes of attribution can be very high, there is no well-defined and broadly accepted scientific method or model for attributing APT groups or attacks, though some research and industry literature exists on this subject. Attribution has even been called pseudoscience by critics and more of an art than science by some scholars (Rid & Buchanan, 2015; Steffens, 2020). However, it should be noted that this does not make attribution worthless. This can be seen by cyber security industry reports and experts attributing cyberattacks to specific military units or even specific persons which have then later been named in indictments by the United States government (Greenberg, 2019; Mandiant, 2013; The United States Department of Justice, 2014, 2018).

It should be noted that attribution of any specific attacks or groups will not itself be considered or questioned in this paper. However, the limitations, processes, and models for attribution will be discussed shortly.

2.3 The attribution problem

The problematic nature and difficulty of attribution has been often named "the attribution problem" and it has been discussed widely, from different points of view and for many years (Rid & Buchanan, 2015; Steffens, 2020; Tsagourias, 2012; Wheeler & Larsen, 2003). While there is no widely accepted consensus on the definition or the true scope of the attribution problem, there does seem to be wide agreement on, and acknowledgement of the problem itself (Betz & Stevens, 2011; Boebert, 2010; Clark & Landau, 2010; Morgan & Kelly, 2019; Mudrinich, 2012; Rid & Buchanan, 2015; Wheeler & Larsen, 2003). The attribution problem has even been called the biggest problem within the cyber arena (Singer & Friedman, 2014).

The difficulty of attribution arises from many sources, for example, the structure of the internet which supports anonymity, the ability to obfuscate code, the tendency for some adversaries to place decoy information, the transnationality of the internet causing juridical issues, and the technical complexity of modern breaches and malware (Clark & Landau, 2010; Mudrinich, 2012; Pahi & Skopik, 2019; Rid & Buchanan, 2015; Steffens, 2020).

2.3.1 Different naming conventions

The different naming conventions used by different cyber security companies and researchers for APT groups is an additional factor that has been noted to complicate attribution of APT groups (Lemay, Calvet, Menet, & Fernandez, 2018; Oosthoek & Doerr, 2021; Romanosky & Boudreaux, 2019). For example, the cyber security company Mandiant uses a simple numerical approach by naming each newly identified APT group with the acronym APT and a consecutive number, e.g., "APT28" followed by "APT29" (Romanosky & Boudreaux, 2019).

Another cyber security company Crowdstrike uses animal labels to refer to the country of origin for each group: for example, Panda for Chinese groups, Kittens for Iranian groups, and Bears for Russian groups. For example, according to Crowdstrike, the group that Mandiant calls "APT28" is "Fancy Bear" (Crowdstrike, 2022b; Romanosky & Boudreaux, 2019). Microsoft, on the other hand, previously used names of chemical elements to name APT groups, and then later switched to a weather theme, so the same group according to Microsoft was previously named "STRONTIUM" and is now referred to as "Forest Blizzard" (Microsoft, 2016, 2023; MITRE, 2022c). These differences make it more difficult to track APT groups and it is not always clear when different vendors and researchers are reporting on the same or different group (Lemay, Calvet, Menet, & Fernandez, 2018; Oosthoek & Doerr, 2021).

To minimize any confusion, the groups chosen for this paper will be discussed with only one name per group. As no one authoritative naming list exists, the names used, and any additional aliases for data gathering, will be from MITRE ATT&CK knowledge base and Malpedia. Both of these organizations are non-profit organizations, which should limit biases in reporting (Malpedia, 2023.; MITRE, 2023j). For the purpose of this study, it will be assumed that these naming schemes and lists are correct, are not a result of any misattribution, or have any unintended overlap.

2.4 Attribution models

In addition to models for APT attacks and attackers, there have also been multiple models and frameworks suggested to assist in different aspects of attribution of cyberattacks. Some models focus more on the detailed technical steps of an attribution process, like the MICTIC-framework by Steffens (2020), while others, like the Q-model by Rid and Buchanan (2015), focus more on assisting analysts in also asking non-technical questions with an eye towards political aspects.

2.4.1 Diamond Model

The Diamond model was suggested by Caltagirone, Pendergast, & Betzto (2013) to describe the methods used in intrusion analysis. It was designed to aid in different aspects of analysing intrusions, such as discovery, correlation, and synthesis of information from events as well as to aid in decision making. It provides definitions for terms of the core elements of an intrusion and aims to include scientific principles into intrusion analysis. The authors also define additional concepts in the paper, such as an extended diamond model, activity threads, and activity groups. The extended diamond model is an extended version of the core diamond model that includes additional features, for example, the relationships between the victim and the adversary. Activity threads are a way of representing an intrusion by listing and ordering the events included in it. Activity groups are used to group together similar activity threads and events to assist in analysis and to develop mitigation techniques to combat the specific intrusion activity. (Caltagirone, Pendergast, & Betz, 2013)

The core diamond model revolves around the four main features that, according to Caltagirone, Pendergast, & Betz (2013), are present in every intrusion event. These features are: adversary, capability, infrastructure, and victim. **Adversary** describes the actor or organization behind the attack, that is utilizing the capability against the victim to reach their goal. **Capability** describes the tools or techniques that the adversary uses to reach their desired goal. **Infrastructure** is being used to describe structures for communication that the adversary uses to deliver and control the capability or to otherwise communicate with the victim or the victim environment. The **victim** feature describes the entity, such as a person, IP address, or an organization, that is being targeted by the adversary with the chosen capability. In addition to the core features, the diamond model includes meta-features such as timestamp, phase, result, direction, methodology, and resources. These meta-features are used to order events into an activity thread and to analyse events further. (Caltagirone, Pendergast, & Betz, 2013)

While not a stated design goal for the diamond model, attribution is noted as being one analytic problem that could be answered using the aspects of the diamond model (Caltagirone, Pendergast, & Betz, 2013). The diamond model has also been taught and used within the cyber security industry for the purpose of assisting different aspects of attribution (SANS, 2022; Warner, 2021).

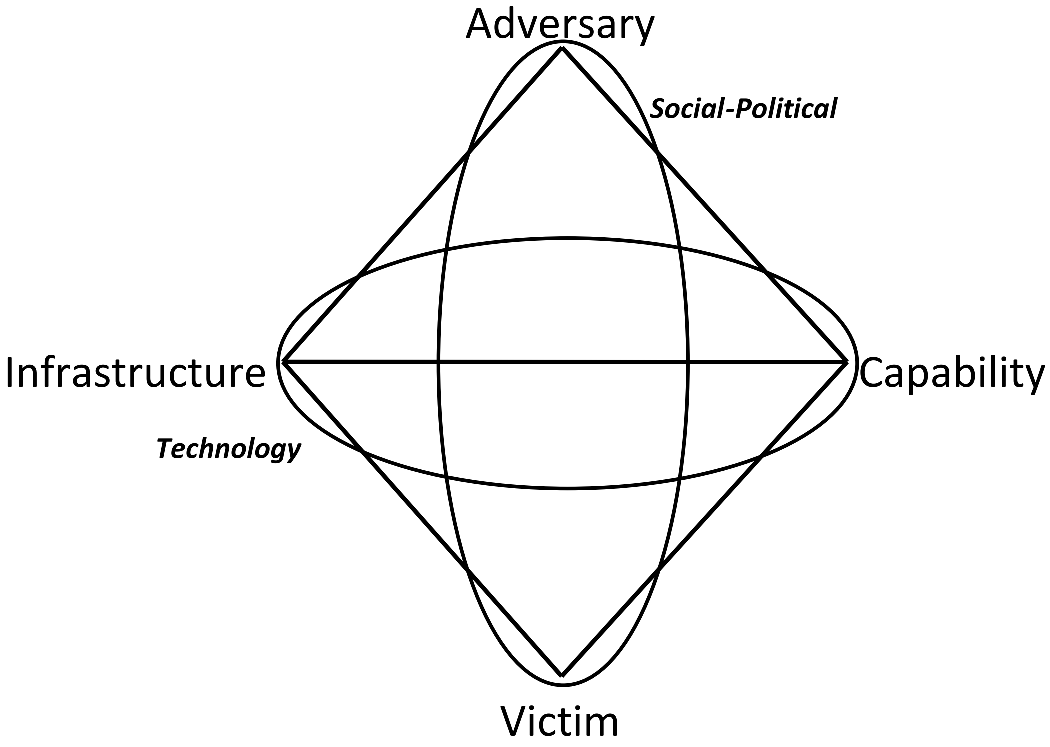


FIGURE 3 The extended Diamond Model (Caltagirone, Pendergast, & Betz, 2013).

2.4.2 Q Model

The Q model was created to explain, guide, and improve the process of attribution. It was introduced by Rid and Buchanan in 2015. It was designed to help, for example, analysts, investigators, national security officials, and decision makers to ask the correct questions regarding the attribution of cyberattacks. The model does not limit itself to any single aspect in cyberattack attribution; instead, it includes questions and steps to consider in the strategic, operational, tactical, and technical level. Uniquely among the models and frameworks described here, the Q model is the only model to also include the process of communicating the results of the attribution to the stakeholders. (Rid & Buchanan, 2015)

The different analytical aspects mentioned are divided into three different layers of analysis: the outermost layer includes technical and tactical analysis, the middle layer includes operational analysis, and the innermost layer is the strategic level analysis. The different layers of analysis are shown in the figure below (Figure 4). There is no direction required or set by the model, the analysis can go from strategic analysis towards the technical or tactical analysis or vice-versa. The communication process is outside the analytical process and is stated to be a goal on its own, separate from the analysis. Each of the analytical layers rely on their own expertise, data, and skills. While the analytical layers are considered separate, the different layers should be informed by each other. With the broad scope of the Q model, it is noted that attribution is a team sport and the skills required for the process of attribution make it implausible for a single person to do it alone. Each analytical layer attempts to answer a different question: the tactical and technical analysis attempts to answer the most technical *how* of the cyberattack, operational analysis attempts to identify the architecture of the attack and attackers' profile or answer the *what* question, and the strategic analysis attempts to identify aspects such as motive and significance of the attack or the "*who*" and "*why*" questions. (Rid & Buchanan, 2015)

Each of the analytical layers are made up of a variety of questions looking to answer the main *how*, *what*, *who,* and *why* questions. For example, the questions looking to answer the strategic *who* and *why* could be "Who benefited most?". The question on the operational level looking to answer the *what* question could be "Did the operation require target intelligence?". The tactical and technical layer questions could attempt to answer *how* by asking "What was the attack designed to do?". If the analysis were to move from technical and tactical to operational and finally to strategic the questions would become broader, or when moving the other direction, sparser. As the questions become broader the analysis is likely to become more uncertain when moving towards the strategic level. This is due to how technical or tactical questions such as "What was the exploit the intruder exploited" can be definitively answered while questions like "What was the attack's objective?" require some conjecture and hypotheses. In addition to the analytical questions attempting to answer the attribution questions, the communication aspect includes questions regarding what and how the communication should be made. Thus, according to the Q model, the process is a dynamic process of questions where the answers from one analytical layer inform the others. (Rid & Buchanan, 2015)

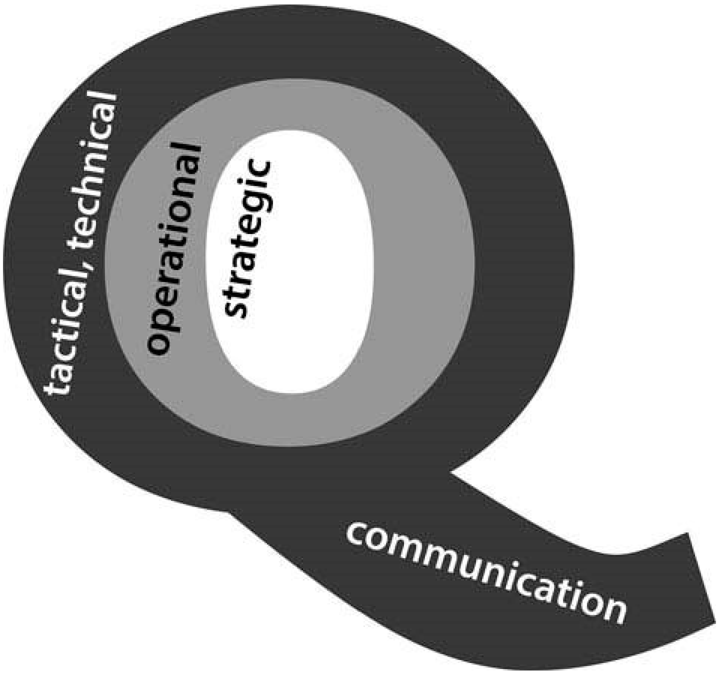


FIGURE 4 Q Models layers of analysis by Rid & Buchanan (2015).

2.4.3 Pyramid of pain

Pyramid of pain is a model to assist in using and understanding indicators of compromise that was suggested by Bianco (2013). Indicators of compromise refer mainly to technical artifacts or clues left behind by an attacker following a compromise (Bianco, 2013). The model describes the amount of trouble, or pain, the adversary would have to go through to change an aspect of their attack that has been detected or denied to them. These aspects of an attack are the different indicators the adversary might have. The pyramid of pain model has been used in the industry to aid in attribution, threat hunting, and as a basis for a machine learning attribution model (Agarwal, Walia, & Gupta, 2021; Al-Mohannadi, Awan, & Hamar, 2020; CyCraft Technology Corp, 2022; Gossi, 2020; Jansen, 2021; Wen, He, & Yan, 2017).

The model is comprised of six different categories of indicators of compromise that an adversary might have, which have been ordered into a pyramid shape. The higher the indicators are on the pyramid, the more difficult the indicators are to change for the attacker. The bottom of the pyramid includes the indicators that are the easiest for an attacker to change: these would be, for example, the hash values of a malicious file, which can be changed easily by changing the file contents, or an IP address used in the attack that can be changed by using a different server or connection point. The indicators that are highest on the pyramid are TTPs and tools which are difficult for an attacker to change. TTPs are things that take some time to form and get proficient at, tools are also time consuming to learn or create. (Bianco, 2013)

The pyramid of pain model suggests that adversaries are least likely to change their TTPs and tools among all the indicators that are visible to a defender or an analyst (Bianco, 2013).

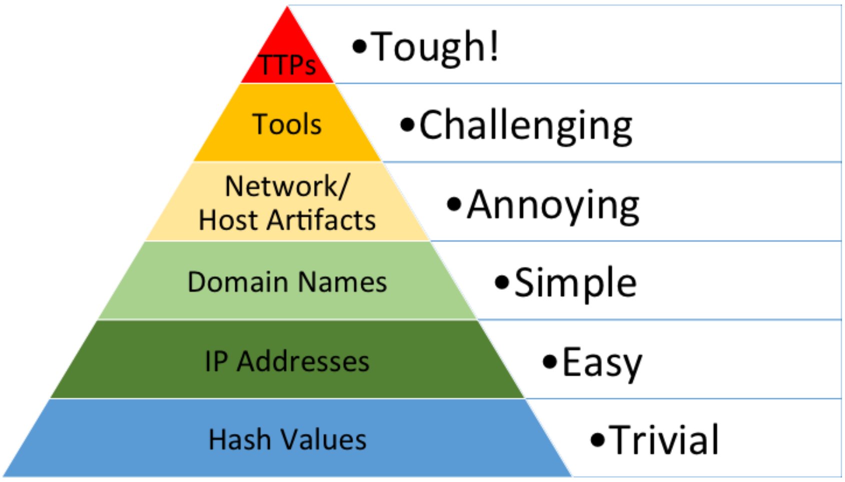


FIGURE 5 Pyramid of pain by Bianco (2013)

2.4.4 Cyber Attribution Model

The Cyber Attribution Model (CAM) was proposed by Pahi & Skopik (2019) to aid analysts in attribution and to counter technical and socio-political false flags that make attribution more difficult. The authors also state that the current existing models have limitations that the new model will address. The model also draws inspiration from the Diamond model. (Pahi & Skopik, 2019)

CAM consists of two main parts: Cyber Attack Investigation and Cyber Threat Actor Profiling. These, when combined, result in attribution. Both parts attempt to answer questions to achieve attribution. The Cyber Attack Investigation attempts to answer who is the victim and why, and what has happened and how. Cyber Threat Actor Profiling tries to answer who could be the perpetrator, what infrastructure they might have, and what capabilities and motivations they might have. The answering of the questions is guided by components called victimology, infrastructure, capabilities, and motivation. Both parts of the model take advantage of technical and socio-political indicators, which are designed to aid in the original goal of recognizing false flag operations. The technical indicators, such as malware, timestamps, and infrastructure, arise mostly from digital forensics. While the socio-political indicators consist of the application of different tools by the adversary with the goal of influencing perception, opinion, and behaviour of the target audience. (Pahi & Skopik, 2019)

After the investigation has been completed the results will be compared to the profiles of known threat actors (Pahi & Skopik, 2019).

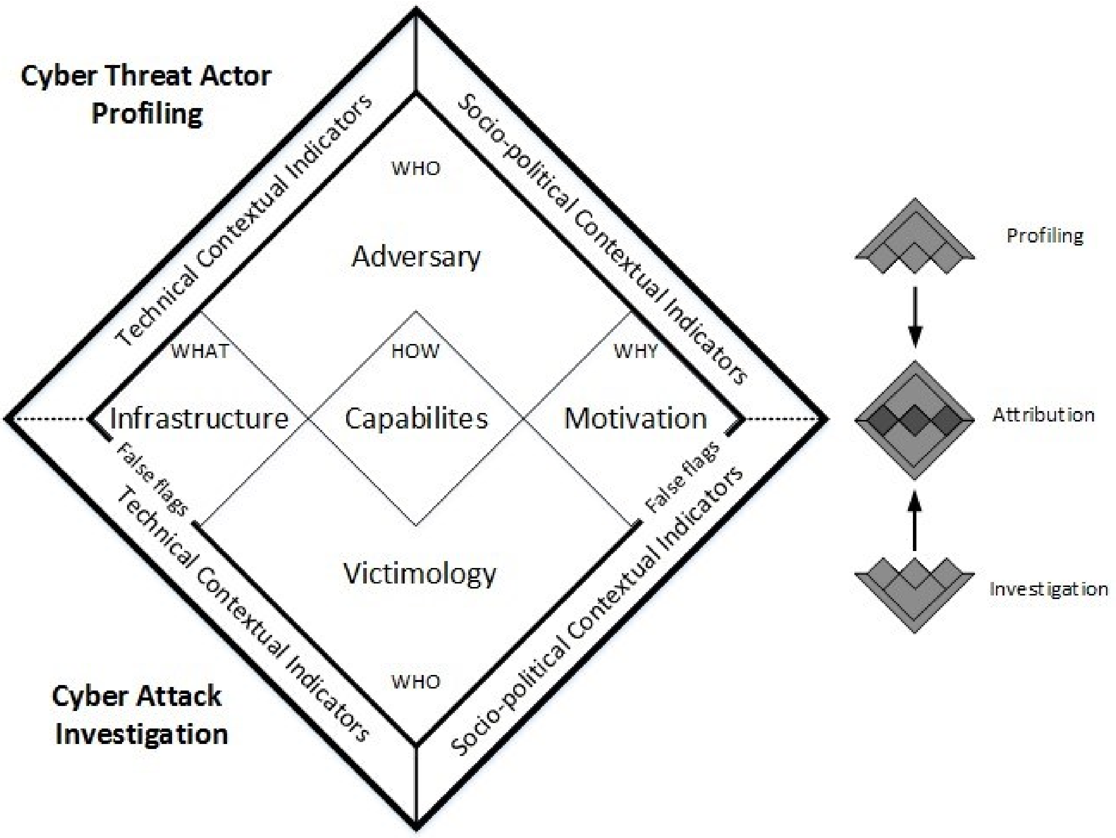

Cyber Threat Actor Profiling
Technical Contextual Indicators
Socio-political Contextual Indicators
WHO
Adversary
WHAT
HOW
WHY
Infrastructure
Capabilites
Motivation
False flags
Technical Contextual Indicators
False flags
Socio-political Contextual Indicators
Victimology
WHO
Cyber Attack Investigation
Profiling
Attribution
Investigation

FIGURE 6 Cyber Attribution Model (CAM) (Pahi & Skopik, 2019).

2.4.5 MICTIC Framework

The MICTIC framework was introduced in 2020 by Steffens to cover the aspects of cyberattack attribution (Steffens, 2020). The author describes the need for a publicly available and technically comprehensive attribution model citing the general lack of publicly available attribution processes and frameworks, as well as the lack of technical focus in the Q Model. The framework is based on the idea that APT attacks consist of multiple separate aspects instead of phases like in a kill chain. Each aspect is an artefact, resource, or activity related to the APT group that leaves some information which can be studied for the purpose of attribution. (Steffens, 2020)

These separate aspects put together form the acronym MICTIC: Malware, Infrastructure, Control servers, Telemetry, Intelligence, and Cui bono. The **malware** aspect describes the technical analysis of the malware used in the attack. This consist of reverse engineering and malware analysis to identify technical evidence from the malware. **Infrastructure** covers the way the command & control servers used by the attackers are set up. The infrastructure analysis generally consists of searching for registration information or infrastructure reuse, often through largely open sources. The aspect of **control servers** is similar, but it describes how the command & control servers are used by analysing information gained through access to the servers themselves. This type of analysis could be for example searching through logs found on the servers used by the attackers. **Telemetry** covers the analysis of data from different IT security products. This can mean, for example, studying reports by IT security vendors for the prevalence or occurrence of a certain malware family. The **intelligence** aspect refers to the analysis of information that can generally only be gained by intelligence agencies. This could be using signals intelligence to investigate the communications of the attackers. **Cui bono,** which means asking the question, “who benefits?”, covers the geopolitical analysis of the motivation of the attack. This type of analysis is done by studying for example the political or economic aspects of the victim or the possible attackers. (Steffens, 2020)

3 RESEARCH METHODOLOGY

The aim of the research aspect of this thesis was to study the available data on the three chosen APT groups in order to learn how they operate. Three APT groups were chosen in order to limit the scope of the thesis to a manageable size while also allowing for a wide selection of data to be studied. The Unified Kill Chain (UKC) was chosen as a model to assist in this analysis as it allowed for the most comprehensive way to compare the different groups. The UKC was used to create a model of each APT group which were studied to further understand how the chosen APT groups operate.

3.1 Qualitative research

Commonly it is seen that there are three approaches to research: quantitative, qualitative, and mixed (Williams, 2007). Qualitative research is often being described as studying words or text data as opposed to numbers or numerical data like in quantitative research, with mixed method research being between the two (Aspers & Corte, 2019; Creswell, 2014; Williams, 2007). Qualitative research has been specifically suggested to be suitable for situations where the existing research is lacking or when exploring a concept, problem, or phenomenon, or analysing the data for descriptions or themes, when a flexible end report is preferred, or when drawing broader interpretations from the data (Aspers & Corte, 2019; Creswell, 2014; Williams, 2007). These aspects fit the research questions and the planned thesis structure better than quantitative research. Additionally, the data to be studied will be mostly technical reports without much numerical data so the qualitative research approach is the most logical.

3.2 Content analysis

Content analysis is a very flexible research method which can be used in multiple ways. It has been described, for example, as a research method where meaning is interpreted by isolating smaller pieces of data and applying a framework to them to explain a phenomenon (Kleinheksel, Rockich-Winston, Tawfik, & Wyatt, 2020). There are both quantitative and qualitative research methods that use content analysis (Bengtsson, 2016). But even beyond that, the content analysis approaches also have been split up further. One way to divide content analysis methods describes them as either inductive, deductive, or abductive. An inductive approach is a search for pattern and moving from the concrete data towards an abstract theoretical understanding, while the deductive approach was described as the opposite, testing existing theories by moving from the theory towards specific data. The abductive approach was described as a combination of both, moving between inductive and deductive approaches. (Graneheim, Lindgren, & Lundman, 2017)

Another categorization of content analysis divides them into three approaches: conventional content analysis, directed content analysis, and summative content analysis. In conventional content analysis the researcher does not have preconceived categories for the data, instead the categories should emerge from the data. In directed content analysis the researcher takes advantage of existing theory to help with initial coding. Summative content analysis includes counting occurrences of specific keywords to understand the context in which the words are used. (Hsieh & Shannon, 2005)

Some key aspects and similarities can be found from the different approaches described. These aspects can be seen to describe a general process of content analysis (Bengtsson, 2016; Elo & Kyngäs, 2008; Hsieh & Shannon, 2005; Kleinheksel, Rockich-Winston, Tawfik, & Wyatt, 2020):

1. Getting an initial familiarization of the data.
2. Identifying a unit of meaning, such as a sentence with something interesting to the researcher.
3. Coding or shortening the units of meaning into a short label that describes them.
4. Categorization of these codes to identify themes and to combine codes.
5. Themes or abstractions can then be used in analysis to describe behaviours, draw conclusions, or to answer the question “How?”.

From the various approaches described, directed content analysis was chosen for this study. There are many existing models that could be taken advantage of in the coding and categorization phase and the description fits the study structure with its simplicity as well as the goal of the study. The directed content analysis method suggested by Hsieh & Shannon (2005) was combined with the key aspects identified from the other approaches to form the chosen research method, which is described further below.

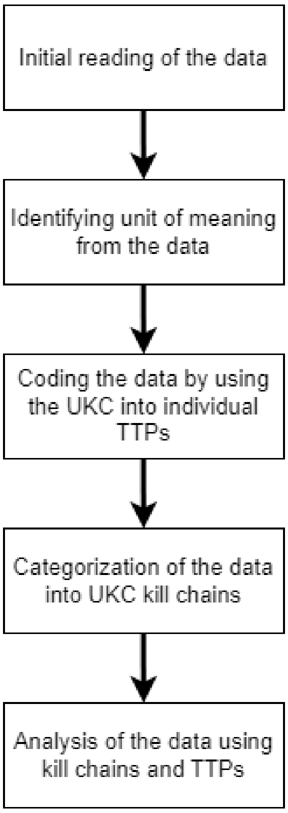

Initial reading of the data
Identifying unit of meaning from the data
Coding the data by using the UKC into individual TTPs
Categorization of the data into UKC kill chains
Analysis of the data using kill chains and TTPs

FIGURE 7 Research method chosen for the thesis.

3.2.1 Initial reading

The initial reading of the data is often described as a way for the researcher to familiarize themselves with the data as a whole and to choose the unit of meaning and initial codes used for the analysis (Bengtsson, 2016; Elo & Kyngäs, 2008; Hsieh & Shannon, 2005). In the chosen approach the coding was done with the help of an existing model. The initial reading was used to familiarize the researcher with the data available and to identify what units of meaning were to be used for coding, keeping in mind the chosen model, and how they could be identified from the data. This first step then informed and enabled the latter steps.

3.2.2 Identifying units of meaning

The units of meaning are the initial and smallest pieces of data used for the analysis. The unit of meaning can be, for example, a paragraph or a sentence. (Bengtsson, 2016; Kleinheksel, Rockich-Winston, Tawfik, & Wyatt, 2020) The units of meaning identified during the initial reading were picked from the data. The small pieces of data were highlighted from the large body of data and noted to aid in the coding process. In this thesis the units of meaning were all the different descriptions of specific TTPs that could be found from the data by interpretive analysis of the data. This interpretative analysis to identify the TTPs was done in a similar manner to the process outlined in the paper which initially defined and described the UKC (Pols, 2018). These identified TTPs were then later used in the analysis phase.

3.2.3 Coding the data

Coding of the data is done to condense and label the units of meaning into shorter and more manageable descriptive categories, which will make further analysis easier (Elo & Kyngäs, 2008; Hsieh & Shannon, 2005; Kleinheksel, Rockich-Winston, Tawfik, & Wyatt, 2020). For this thesis the coding of the data was done by fitting the identified units of meaning, each identified TTP, to the categories and their respective descriptions presented in the UKC. This process was outlined in the paper describing the way the UKC was designed (Pols, 2018, 2022). This process is done by using the set of 18 phases or tactics set out in the UKC as the categories. Alongside the phases, the UKC includes descriptions that were used to categorize the identified TTPs into these phases (Pols, 2022). These phases were thus considered the codes for this thesis.

3.2.4 Categorization of the data

Data that has been coded can then be further categorized by their context to help with identifying themes and to give further structure to the data (Hsieh & Shannon, 2005; Kleinheksel, Rockich-Winston, Tawfik, & Wyatt, 2020). Categorization was also be done by using the UKC, as it includes a tested framework for combining the TTPs into a structured model, meaning the UKC kill chain. The TTPs were placed into kill chains, with each kill chain representing an identified attack for each group, the groups tendencies, or capabilities. These kill chains were added into a table where one kill chain was represented by a column that had every TTP identified in the attack, each column depicting one attack, and one table for each group. Each individual kill chain was an attack-specific kill chain, which were then combined into what could be considered an actor-specific model, or a set of kill chains. This model, consisting of the table of kill chains, was then used alongside the TTPs that were identified, to compare the groups. The kill chains identified at this step and further descriptions and references to them were also added to the appendix to aid in possible replication studies.

3.2.5 Analysis of the data

The identified kill chains and TTPs were used to identify relationships, themes, patterns, or similarities between the groups. This was done by comparing each group's TTPs that were identified for each UKC phase against each other. The kill chains were analysed by comparing each group's attacks, divided into three separate phases. The three separate phases were the initial attack paths, compromise phase, and actions after the compromise. The TTPs and kill chains were also analysed as wholes to identify themes that could be seen beyond individual TTPs or phases of the kill chain. This analysis was done by examining the data for patterns or themes that come up repeatedly. These relationships, themes, patterns, and similarities that could be identified from the data were then used to analyse the way the groups operate and finally to answer the research questions.

3.3 Data collection

When conducting a qualitative content analysis, the data that is to be studied is generally collected before the data analysis begins, in what is referred to as a preparation or planning phase (Bengtsson, 2016; Elo & Kyngäs, 2008). The data source in qualitative content analysis is often different interviews, but due to the nature of the studied phenomenon, this is not possible in this case (Bengtsson, 2016; Elo et al., 2014; Elo & Kyngäs, 2008; Kleinheksel, Rockich-Winston, Tawfik, & Wyatt, 2020).

There are some limitations in the data that was used in the study, which is notable, as data collection is an important aspect of qualitative content analysis, especially in the context of reliability and trustworthiness (Elo et al., 2014). The existing data about the operating procedures of APT groups mostly consists of reports covering different incidents or the groups themselves from different cyber security vendors, industry researchers, governmental agencies, and some limited academic research (Lemay, Calvet, Menet, & Fernandez, 2018; Pols, 2018). This was a key limiting factor in the breadth and variety of views in the data that was studied. The cyber security vendors and industry researchers have their own interests, commercial or otherwise, that might impact the way these reports are written. This should be acknowledged when reading the data, the results of the analysis, and the findings.

The data collected for this research consisted of freely and publicly available reports, papers, articles, and other documents that depict the three chosen groups, their activities, incidents they are involved or implicated in. The period for data collection was also limited to avoid being overwhelmed with additional data during the analysis stage.

As described above, these reports mostly come from the cyber security industry and some public government documents. The data was collected by searching for material regarding these specific groups from search engines such as Google, Google Scholar, and JYKDOK as well as searching from industry information repositories such as Malpedia, MITRE ATT&CK knowledge base, and VX-Underground. The data collection began in October of 2022 (15.10.2022) and ended in June of 2023 (30.06.2023).

4 APT GROUPS

As described in an earlier chapter, the term APT has been used to refer to exceptionally advanced forms of attacks, attackers, or operations. Within research literature the groups behind these attacks have also been referred to as threat actors, threat groups, APT threats, APT actors, and APT groups among other terms (Ahmad, Webb, Desouza, & Boorman, 2019; Alshamrani, Myneni, Chowdhary, & Huang, 2019; Burita & Le, 2021; Lehto, 2022; Lemay, Calvet, Menet, & Fernandez, 2018; Vogler & Connell, 2016). The situation is similar within the cyber security industry. For example, Microsoft appears to use the terms activity group and threat actor seemingly interchangeably, while Crowdstrike uses threat actor group, threat actor, adversary group, and APT also seemingly interchangeably (Meyers, 2020; Microsoft, 2016, 2021). Mandiant on the other hand has a process where threat actor is an umbrella term and threat actors are initially classified as "UNC" or uncategorized actors and if enough information is gathered the threat actor can eventually "graduate" to an APT group or a "FIN" group for targeted financial threats (Vanderlee, 2020).

Ever since the first major public report on APT groups, the groups have been accused of wide range of serious attacks: espionage against companies or governments, sabotage of physical infrastructure, disinformation campaigns, website defacement attacks, distributed denial-of-service attacks, and data destroying attacks (Greenberg, 2019; Mandiant, 2013; U.S General Services Administration, 2022; Zetter, 2014). Many APT groups have been connected to multiple different intelligence agencies, militaries, national security organizations, and states in general by cyber security researchers, journalists, and governments (Bienstock, 2022; Mandiant, 2013; The United States Department of Justice, 2014, 2018; Välisluureamet, 2018; Zetter, 2014).

The APT groups chosen for this study were selected to give a broad view into the most prominent, active, and sophisticated groups, that were also connected to the same country. These groups and the operations they have been connected to, TTPs that the groups have been known to use or have the capability to use, and the kill chains that were formed from the data are discussed and described in detail in the following section.

4.1 APT28 (also known as: Fancy Bear, STRONTIUM, Forest Blizzard, Sofacy, Sednit, Pawn Storm)

APT28 is a sophisticated APT group that is thought to have been active since at least 2004 (ESET, 2016; FireEye, 2014). While the group has many aliases, the name APT28 has been most widely used. APT28 has been also referred to as "Sofacy" by Kaspersky and Palo Alto, "Sednit group" or "Sednit" by ESET, "Fancy Bear" by Crowdstrike, "STRONTIUM" and later "Forest Blizzard" by Microsoft, "Threat Group 4127" and "Iron Twilight" by Secureworks, and "Pawn Storm" by Trend Micro (Anthe et al., 2015; Creus, Halfpop, & Falcone, 2016; Crowdstrike, 2019; ESET, 2016; Kaspersky Labs, 2018a; Secureworks, 2016, 2017; Trend Micro, 2020).

The group has been connected to multiple cyberattacks that have often targeted governmental organizations, such as various embassies, political parties, ministries of defence, and ministries of foreign affairs (ESET, 2016, 2018a; Trend Micro, 2020). Most notably the group has been connected to the attack against the Democratic National Committee (DNC) leading up to the 2016 presidential election in the United States (Crowdstrike, 2020). Other typical target organizations include defence related organizations such as NATO and OSCE, defence contractors, and armed forces (FireEye, 2014; Kharouni et al., 2014; Trend Micro, 2020). These targeted organizations are often in eastern Europe such as Ukraine and Latvia, Caucasus, like Georgia or Azerbaijan, or in NATO countries such as the United States, France, Belgium, Turkey, or Germany (ESET, 2018a; Hacquebord, 2018; Kaspersky Labs, 2018a). The group has also had targets in Russia, these include individual citizens like activists, journalists, and politicians as well as media organizations and even the dissident music group "Pussy Riot" (FireEye, 2017; Hacquebord, 2017).

APT28 itself has been connected to Russia with many different levels of specificity and certainty. Some cyber security researchers, analysts, and organizations simply suggest the group is working from Russia or originates from Russia while noting that they have similar strategic interests to the Russian government (Benchea, Vatamanu, Maximciuc, & Luncaşu, 2015; Crowdstrike, 2019; Guibernau, Towne, & Wells, 2022). Some cyber security researchers go further and suggest APT28 is sponsored by, or is working on behalf of, the Russian government (FireEye, 2014, 2017; Secureworks, 2016). Many different branches of the United States government and the Estonian foreign intelligence service go further still and state that APT28 is associated with Russian military intelligence agency GRU, with the United States Department of Justice even naming specific units and individuals within the GRU in their indictments (National Security Agency & Federal Bureau of Investigation, 2020; The United States Department of Justice, 2018; Välisluureamet, 2018).

Another notable APT group called "Sandworm" has also been connected to the GRU and even sometimes included under the umbrella of APT28. These two groups will be considered separate for the purposes of this thesis and its analysis because most cyber security researchers seem to consider these groups separate entities (Leonard, 2022; Microsoft Digital Security Unit, 2022; Sadowski & Hall, 2022).

APT28 has been most often connected to espionage style operations where the seeming main intention is to gather information in a covert manner by gaining access to the target's internal networks and systems (FireEye, 2014; Hacquebord, 2017; Kharouni et al., 2014). In addition to these espionage operations, the group has another notable modus operandi which is sometimes called "hack-and-leak". This consists of first attacking an organization and gaining access to sensitive information, which is then selectively leaked using different hacktivist personas (FireEye, 2017; Hacquebord, 2017; Sadowski & Hall, 2022).

There are individual reports indicating the group also conducted some operations that do not fit either of these methods. APT28 has been connected to one destructive sabotage operation, one operation to create malware to aid in the destruction of Ukrainian artillery, and a harassment campaign targeting military spouses in the United States (Meyers, 2016; Satter, 2018; Suiche, 2017).

APT28 is thought to have created and developed its own extensive set of malware and tools that the group uses in its attacks (ESET, 2016; FireEye, 2014, 2017). These tools include multiple backdoor malware, credential stealing malware, malware designed only to download or extract another payload, a proxy tool, and even malware for infecting networks that are not connected to the internet by using USB drives (Calvert, 2014; ESET, 2016; FireEye, 2014). Despite having access to these custom-made malware, the group has also been known to sometimes use multiple publicly available open-source hacking tools (Anthe et al., 2015; Benchea, Vatamanu, Maximciuc, & Luncaşu, 2015; Lee & Falcone, 2018; Lee, Harbison, & Falcone, 2018; Mandia, 2017; Secureworks, 2017; Smith & Read, 2017).

4.1.1 Identified TTPs

The capabilities APT28 has, as well as different TTPs used by APT28 in various attacks, were identified by studying various technical reports and whitepapers. In total 45 different publications were studied to identify the usage of, or capability to use TTPs that were then categorized into phases of the Unified Kill Chain. These publications include various reports and articles that outline individual attacks, campaigns that include many attacks as well as whitepapers that describe the group itself and the malware used by the group. The following identified and categorized TTPs represent the totality of the TTPs that APT28 has used, or has the capability to use, not any specific attacks or TTPs used in a specific attack.

Reconnaissance: APT28 has been identified performing some reconnaissance before conducting some of its attacks. Extensive and aggressive scanning of specific ports, more targeted scanning of specified IP address ranges, as well as unspecified methods of open-source intelligence (OSINT) have been identified as reconnaissance methods used by APT28 (Anthe et al., 2015; Benchea, Vatamanu, Maximciuc, & Luncaşu, 2015; Trend Micro, 2020). In addition, it has been noted that some attack methods which APT28 relies on hint at some reconnaissance having been made, but the techniques have often not been specified (Mueller, 2019; Suiche, 2017; United States Department of Homeland Security & Federal Bureau of Investigation, 2016).

Resource Development: All the reported attacks by APT28 include some form of resource development. APT28 has often registered domain names that resemble some legitimate domain names, which is a technique known as typosquatting, to make their phishing or other attacks appear more credible (Benchea, Vatamanu, Maximciuc, & Luncaşu, 2015; ESET, 2016; FireEye, 2017; Kharouni et al., 2014). The group is also known to have created specially crafted malicious documents, malicious websites, multiple types of malware, and specifically targeted phishing emails (Calvert, 2014; ESET, 2014a, 2016; Mueller, 2019; Trend Micro, 2015). APT28 also used link shortening services, such as Bitly to hide their real malicious links (ESET, 2016; SecureWorks, 2016). APT28 has deployed a wide variety of custom Windows and Linux malware that can be used for multiple purposes which has required significant development effort (ESET, 2016). The group has also been known to have deployed a rare malware for Apple iPhones, another malware targeting Mac computers, and a rootkit for the UEFI firmware of a machine (Creus, Halfpop, & Falcone, 2016; Hacquebord & Mercês, 2015; Ilascu, 2018).

Delivery: APT28 most commonly uses spear phishing emails and websites compromised with malicious code, which the target is likely to visit, also known as a watering hole attack, as its initial delivery method (Anthe et al., 2015; ESET, 2016; FireEye, 2017). The spear phishing messages used by APT28 often include a malicious document, or they can lead to credential theft (ESET, 2018a; Kaspersky Labs, 2018a; Kharouni et al., 2014). The group has also used spear phishing emails to link to a watering hole website (ESET, 2016; Kharouni et al., 2014; Trend Micro, 2015). APT28 has also delivered its malware by gaining access through prior credential theft, through default credentials for a vulnerable service, and by using infected USB-drives (Calvert, 2014; Mueller, 2019; Suiche, 2017). In many operations APT28 also used their malware as a secondary delivery method to download a second or third stage payload to the compromised system or device (ESET, 2016, 2018a; Kharouni et al., 2014). In some instances, APT28 has also been identified using certutil.exe, a command line tool that is native to many Windows operating system versions, to download their tools (Lee & Falcone, 2018; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021). The group has also at least attempted password spraying to gain initial access into networks (Microsoft Threat Intelligence Center, 2020a).

Social Engineering: APT28 often uses social engineering methods, especially in their spear phishing lures as they attempt to get the victim to open links or malicious documents, or to perform other actions to allow for exploitation (ESET, 2018a; Hacquebord, 2018; Jazi & Santos, 2022). Social engineering was also used by the group for spear phishing email and network domain credentials, as well as to trick their victims into allowing access to their email accounts via a malicious application using Open Authentication (OAuth) requests (Anthe et al., 2015; Hacquebord, 2017; Mueller, 2019). APT28 has also used decoy documents that are meant to trick the victim while malicious actions are taking place (Kharouni et al., 2014).

Exploitation: The group has used a very wide variety of exploits against vulnerabilities in many software products, such as Oracle Java, Internet Explorer, Microsoft Office, Adobe Flash Player, Firefox, Windows operating systems, and Adobe Acrobat PDF reader. Many of the vulnerabilities abused were what are called zero-day vulnerabilities, where the vulnerabilities are unknown to the software vendor at the time they were used, though some vulnerabilities were first identified by other groups and then repurposed by APT28. (ESET, 2016; Kaspersky Labs, 2015; Mehta, Leonard, & Huntley, 2014) During just the year 2015 the group was identified as having used six different zero-day exploits (ESET, 2016). Most of the vulnerabilities that APT28 exploited were used via a malicious website that targeted browsers or browser plugins, or with malicious documents targeting common office applications like Microsoft Word or Adobe Reader. The vulnerabilities were mostly used to gain an initial foothold. (ESET, 2014a, 2016; Kharouni et al., 2014; Trend Micro, 2015) APT28 has also known to exploit some Microsoft Exchange Server vulnerabilities to gain access to the victim network (National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021). The group has been identified exploiting multiple Windows vulnerabilities and one Java vulnerability to achieve privilege escalation (Anthe et al., 2015; Benchea, Vatamanu, Maximciuc, & Luncaşu, 2015; European Repository on Cyber Incidents, 2023; FireEye, 2015a; Hacquebord, 2017). In one case APT28 has also used a UEFI vulnerability to avoid a defense feature (Ilascu, 2018).

Persistence: The different malware used by APT28 have capabilities for creating persistence in the victims' systems and networks, some of the malware even having multiple persistence methods (Creus, Halfpop, & Falcone, 2016; ESET, 2016, 2018; Mehta, Leonard, & Huntley, 2014). These capabilities include taking advantage of Windows services and Windows registry as well as more advanced bootkits and rootkits that are more difficult to spot (ESET, 2016). The group has been the first to have used rootkits inside the UEFI. UEFI rootkit moves the persistence into the UEFI firmware of a machine, which allows for the persistence method to remain even after reinstalling the operating system, also notably even after replacing the hard drive. (Ilascu, 2018)

Defense Evasion: Some of the malware used by APT28 include features that make detecting the malware and its actions harder, like using identifiers and names of legitimate software, and some capabilities that can be used to actively avoid detection, such as searching for known security software or injecting into browsers to hide their command & control traffic. The group often uses encrypted communication between its malware and command & control servers to make detection or analysis more difficult. (ESET, 2016; FireEye, 2014) The group has also taken advantage of Google Drive for its command & control connections, likely to avoid detection (Hacquebord & Remorin, 2020). APT28 has also used some specific techniques to evade defences, for example obfuscation in malicious documents to avoid signature-based detection, deleting logs, and hiding or deleting files related to their malware (Anthe et al., 2015; Lee & Falcone, 2018; Lee, Harbison, & Falcone, 2018; Mueller, 2018).

Command & Control: Most of the malware used by APT28 have some capability to communicate with their command & control servers. Some of the malware use this communication to receive commands to perform or payloads to deploy from the command & control servers while other malware send back the information the malware has gathered (ESET, 2016; FireEye, 2014). APT28 has also been suspected of using a compromised system as its command & control server (SecurityScorecard, 2022). The group often encrypts and encodes their communications to and from the command & control servers (ESET, 2018a; FireEye, 2014; Trend Micro, 2015). APT28 malware can communicate with the command & control servers through multiple network protocols such as HTTP, FTP, POP3, and SMTP or through a proxy tunnel created with the group's own Xtunnel tool (Anthe et al., 2015; ESET, 2016; Hacquebord & Mercês, 2015). Xtunnel is a tool created by APT28 that acts as a proxy tunnel for the command & control traffic of another infected device that is not directly connected to the internet (ESET, 2016). In one case, APT28 has been found to have used this tool to exfiltrate over 70 gigabytes of stolen data from networks and devices that were not directly connected to the internet (Mueller, 2019).

Pivoting: APT28 has two different malware that have the pivoting capability as their main function: Usbstealer which can be used to reach networks isolated from the internet by infecting USB-drives and Xtunnel that is used as a relay to reach devices without access to the internet (Calvert, 2014; ESET, 2016). APT28 has also been identified as having used this capability to pivot by allowing their malware to reach devices outside their initial foothold and to expand their access in multiple attacks (Guarnieri, 2015; Mueller, 2019; Secureworks, 2017).

Discovery: APT28's malware has capabilities that allow the group to further examine an infected machine and its network. These capabilities consist mostly of discovery features built into the malware as well as the possibility to run operating system commands or read files on the system to gather information on the device and the network it exists in (ESET, 2018a; FireEye, 2014; Mehta, Leonard, & Huntley, 2014). APT28 has also performed fingerprinting via Javascript that was embedded into compromised websites to gather information on the victim's system (Anthe et al., 2015; ESET, 2014a). The group has also been known to perform scanning of internal networks and manually searching for files and information from internal information repositories found in the victim environment (Suiche, 2017). APT28 has used discovery capabilities mostly through first stage malware, possibly to confirm if the attacked target is suitable for further action (ESET, 2018a; Lee, Harbison, & Falcone, 2018).

Privilege Escalation: APT28 has been identified using multiple techniques for privilege escalation. Most commonly the group has performed privilege escalation by exploiting various vulnerabilities (FireEye, 2015; Kaspersky Labs, 2018a). These vulnerabilities have mostly been exploited via malicious documents but also with tools that the group has used, including a custom version of Mimikatz (Anthe et al., 2015; Benchea, Vatamanu, Maximciuc, & Luncaşu, 2015). APT28 has also used DLL search order hijacking, process injection, privileged credentials stolen with a tool called Responder, creation of new privileged accounts, and scheduled task creation for privilege escalation (ESET, 2016, 2019; Lee, Harbison, & Falcone, 2018; Smith & Read, 2017; Suiche, 2017).

Execution: The group has been found to have used many techniques to execute code on devices they have gained access to. Often APT28 gained the initial execution through various exploits or through social engineering a victim to open malicious documents or other files (ESET, 2018a; Falcone, 2018; FireEye, 2015a; Kaspersky Labs, 2018a). After an initial execution the group often used the malware that gained the initial foothold to deliver and execute additional tools or payloads. Often the code execution was performed via rundll32.exe, a program that is native to Windows operating systems (Benchea, Vatamanu, Maximciuc, & Luncaşu, 2015; Kaspersky Labs, 2015; Kharouni et al., 2014). Some malware used by APT28 could also perform this payload execution using their own features (ESET, 2016; Falcone & Lee, 2016). The group has also used the Windows command prompt cmd.exe to perform the initial execution, the execution of additional payloads, or the execution of commands sent from command & control servers (ESET, 2019; Falcone, 2018; Jazi & Santos, 2022; Lee & Falcone, 2018). APT28 has sometimes also used Powershell to perform the initial payload execution and in at least one instance to execute additional commands (Falcone, 2018; Hacquebord & Remorin, 2020; Sherstobitoff & Rea, 2017). In at least one instance APT28 has used regsvr32.exe, another Windows native command line program, to execute malicious code by executing it as a service (ESET, 2019). APT28 has also used regsvr32.exe to execute a malicious DLL (ESET, 2019).

After performing the initial execution, the group has used open-source remote execution tools like Winexe and Remcom to perform execution on remote targets (Anthe et al., 2015; Secureworks, 2017).

Credential Access: APT28 has used various tools and methods for stealing credentials from their victims. The group has, for example, gained access to email and network domain credentials by various forms of spear phishing, stealing credentials from internal information repositories, creating additional accounts, using their own malware to steal any stored passwords, bruteforcing credentials, and employing password stealing tools like Mimikatz and Responder (Anthe et al., 2015; Hacquebord, 2017; Jazi & Santos, 2022; Smith & Read, 2017; Suiche, 2017; Trend Micro, 2020). In addition, APT28 has also used their malware to steal browser cookies and to steal Wi-Fi passwords. The group has used various living off the land methods to steal the LSASS process memory, which contains password hashes from the device, as well to steal the whole active directory database that contains all password hashes from the whole network domain (Jazi & Santos, 2022; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021; Smith & Read, 2017). APT28 has also been known to have a keylogger module in its malware, though it is not clear if it has been used specifically for credential access purposes (ESET, 2014a).

These stolen credentials have been used, for example, to gain initial access in their operations, to send out more email phishing messages, to expand their access, or to gather and steal information (Hacquebord, 2017; Mueller, 2019; Trend Micro, 2020).

Lateral Movement: APT28's Xtunnel tools main capability can be used to make lateral movement easier and more effective as the tool creates a connection between an initially infected pivot machine and another machine that can't be directly accessed by the attacker (ESET, 2016). USBStealer is another APT28 malware that has the capability to perform lateral movement, specifically for networks isolated from the internet, as its main function (Calvert, 2014).

The group has been known to use Xtunnel after gaining initial access to a network, possibly to aid in lateral movement (ESET, 2016; Mueller, 2019). In addition to Xtunnel and USBStealer, APT28 has also used Mimikatz, Winexe, and Remcom specifically for lateral movement. Mimikatz has been used by APT28 to perform a pass-the-hash attack as well as to steal passwords to enable lateral movement. Winexe and Remcom have been used to execute remote command. (Anthe et al., 2015; Guarnieri, 2015; Secureworks, 2017) The group has also used a notorious exploit called EternalBlue, native Windows commands such as "net use", and specifically created accounts to move laterally within a network (National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021; Smith & Read, 2017; Suiche, 2017).

Collection: Malware created by APT28 give the group capabilities for collecting data or facilitating the collection of data. While many of the first stage malware are capable of only collecting limited amounts of information about the infected machine, the later stage malware seems to be designed specifically for the collection of information or espionage (ESET, 2016; FireEye, 2014). These espionage malware allow the group to collect users' keystrokes, take screenshots, collect data from browsers, list contents of directories, and collect specific files the group is interested in, even from removable drives (ESET,2016; FireEye, 2014; Jazi & Santos, 2022). Some malware used by APT28 have been set to automatically collect and search for files with specific file extensions as well as files with filenames matching certain search terms (Calvert, 2014; ESET, 2016; Kaspersky Labs, 2018a).

In addition to their malware searching for files, APT28 has been identified searching for files manually with specific search terms (Mueller, 2019). APT28 has also used scripts to collect data (Guarnieri, 2015). After gaining access to a network, the group has been identified searching for files from network shares as well as other internal data repositories and email inboxes (National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021). APT28 has also been known to use the archiving tool WinRAR to package their stolen files (National

Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021).

Exfiltration: Multiple APT28 malware have capabilities for exfiltrating data from compromised networks. These capabilities are mostly included in the later stage malware, which are often deployed after an initial compromise using a first stage malware (ESET, 2016; Kaspersky Labs, 2018a). APT28 has been known to use these capabilities to exfiltrate even tens of gigabytes of data (Mueller, 2019). Often these exfiltration methods include encryption, either by encrypting the data sent or by using an encrypted communication method (ESET, 2016; FireEye, 2014; Kaspersky Labs, 2015, 2018). The group has also been known to use proxy servers for exfiltration, possibly to make tracking them down more difficult (Mueller, 2019). APT28 malware has capabilities for exfiltrating data with HTTP and IMAP protocols (Hacquebord & Mercês, 2015; Jazi & Santos, 2022). The group has been identified even using the victim's own email server to exfiltrate data by sending emails from the server as well as staging data there before downloading it with a simple web request (FireEye, 2014; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021). APT28 has also used Google Drive for the purpose of exfiltrating collected information (Hacquebord & Remorin, 2020).

Impact: APT28 has performed some impact techniques in their attacks. The group has been known to input faulty configurations into systems to make them malfunction, wipe configurations, deface social media sites, conduct a denial-of-service attack, and destroy data from victim systems (FireEye, 2017; Suiche, 2017).

Objectives: Objectives of APT28's attacks are commonly identified as the stealing of confidential and sensitive information (ESET, 2018a; Kharouni et al., 2014). The group has stolen specifically politically sensitive data as well as data from some organizations that are not particularly political (FireEye, 2017; Mueller, 2019). Sometimes in addition to stealing the data, the group has leaked the data to further their goals (FireEye, 2017; Mueller, 2018). APT28 has been also identified performing sabotage-type operations where the objectives have been to cause destruction of data (FireEye, 2017; Suiche, 2017). In one instance it has been suspected that an APT28 operation was conducted to identify the location of military units to assist the Russian military in the war in Ukraine (Meyers, 2016).

4.1.2 ATP28's kill chains

To identify APT28's kill chains that include the aforementioned TTPs, the same 45 publications regarding APT28's capabilities, attacks, campaigns, and the group itself were reviewed. Different reports and whitepapers were studied to identify the longest and most complete kill chains depicting APT28's actions. As many of the reports were describing malware or malware campaigns connected to APT28 instead of thorough incident reports, the identification of the kill chains required some interpretative analysis. From the 45 publications, 14 kill chains were identified. One kill chain identified from the reports was found to be a duplicate, and it was left out of further analysis. The remaining 13 kill chains can be seen in the table (Table 1) marked C1-1, C1-2 etc. in no particular order. These kill chains show the sequence of events within one realized attack, the described tendency of the group, or their capabilities. The sequence of events is described by indicating the occurrence of a TTP by a number representing the UKC phase the TTP belongs to. The numbers and the UKC phase they represent are included in the leftmost column in the table. The sequence of events begins at the top row of each column with events unfolding down the column. Due to the limited nature of some of the reports, some TTPs in the kill chains are interpreted from the context of the report and included in the kill chain despite the report being unclear of the occurrence of said TTP. These interpretations were marked with a ~~strikethrough~~. The interpretations consisted of, for example, including the TTPs of defense evasion and persistence into kill chains where a specific malware was used that is known to perform defense evasion and persistence techniques, even if that report did not mention the use of these techniques. Additionally, a **black line** is included into the table to indicate the point at which an initial compromise of one device was complete and the initial attack phase was over as the attackers connected to a command & control server. This analysis process was done by closely following the process described in the original paper defining the Unified Kill Chain (Pols, 2018).

All the kill chains identified had almost identical initial steps. Most kill chains began with resource development, delivery, and social engineering. The only outliers were two kill chains that also included an initial reconnaissance phase which could be identified before the resource development phase (C1-8, C1-9). The manner and type of resource development performed, delivery method used, and social engineering taken advantage of differed somewhat between the kill chains.

APT28's initial attack paths can be divided into three main categories. The most common initial attack path identified within the reports was spear phishing to deliver a malicious document (C1-1, C1-2, C1-4, C1-6, C1-7, C1-10, C1-11, C1-13). Often the malicious documents used by APT28 exploit some vulnerability to allow for the attack to move forward (C1-2, C1-3, C1-4, C1-5, C1-10, C1-11) or simply relied on social engineering to skip the exploitation by convincing a victim to perform some unsafe actions (C1-1, C1-6, C1-7, C1-13). However, even when exploits were used, the attacks still often included some social engineering techniques prior to the exploitation. The second most common attack path was spear-phishing emails leading to a watering hole attack (C1-8, C1-12). While watering hole attacks also included aspects of social engineering, the attacks relied on exploiting vulnerabilities to allow for further exploitation of the system.

The last clearly identified initial attack path was spear phishing of credentials that leads into credential access for the initial access (C1-9). While only one clear kill chain was identified from the reports that used this initial attack path, multiple reports do suggest that APT28 also used this method in other instances (Microsoft Threat Intelligence Center, 2020a; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, &

National Cyber Security Centre UK, 2021; Suiche, 2017). For the remaining kill chains (C1-3, C1-5) a delivery method was not known.

After gaining initial access, most of the kill chains include setting up persistence (C1-1), performing defense evasion techniques (C1-2, C1-3, C1-7, C1-11, C1-12, C1-13) or both (C1-5, C1-6, C1-10) before connecting to the command & control server. In some individual kill chains discovery (C1-1, C1-13), additional delivery (C1-10, C1-13), or privilege escalation is performed (C1-6, C1-8) before the command & control connection is achieved. Before a command & control server is contacted the use of delivery techniques refers to the initial malware extracting or "dropping" the malicious payload in some way to the device that is being compromised.

After contacting the command & control server most kill chains show the attackers performing additional delivery of tools or malware to the compromised system from the command & control servers using the initial malware (C1-1, C1-2, C1-3, C1-4, C1-8, C1-11, C1-12, C1-13). These second-stage malware or tools were then used to further the attack and conduct the actions on the target system to reach the objective of the attack.

After gaining access and delivering the necessary tools to the target systems, the kill chains differ slightly. In many attacks, the kill chains show that APT28 was then able to perform the final steps of collection and exfiltration (C1-1, C1-2, C1-3, C1-8) without needing additional steps or in some cases after performing code execution (C1-5, C1-6, C1-10, C1-13).

The remaining the kill chains show the attackers did sometimes require additional privileges and performed privilege escalation (C1-11, C1-12), which sometimes required credential access (C1-4, C1-9). The elevated privileges then led APT28 to move laterally before performing the final steps of collection and exfiltration (C1-4), or in one case only after pivoting inside the victim network before collection, exfiltration, additional defense evasion, and finally reaching their objectives (C1-9).

In some kill chains the privilege escalation allowed them to perform additional persistence, discovery, and defense evasion techniques before contacting the command & control servers again and delivering more tools. These tools allowed them to perform execution, collection, and exfiltration to end the final kill chains (C1-11, C1-12).

TABLE 1 Identified APT28 kill chains[1]

		C1-1	C1-2	C1-3	C1-4	C1-5	C1-6	C1-7	C1-8	C1-9	C1-10	C1-11	C1-12	C1-13
1	Reconnaissance	2	2	2	2	2	2	2	1	1	2	2	2	2
2	Resource Develop.	3	3	~~3~~	3	~~3~~	3	3	2	2	3	3	3	3
3	Delivery	4	4	4	4	4	4	4	3	3	4	4	4	4
4	Social Engineering	12	5	5	5	6	~~3~~	3	4	4	5	5	10	3
5	Exploitation	6	12	7	12	5	12	12	5	13	12	12	5	12
6	Persistence	10	~~7~~	12	8	12	7	7	12	12	3	7	12	7
7	Defense Evasion	8	8	4	3	7	11	5	11	8	6	8	7	3
8	Command & Control	3	3	8	~~7~~	8	6	8	8	13	7	3	8	12
9	Pivoting	15	~~6~~	3	6	~~12~~	10	12	3	11	8	5	3	10
10	Discovery	16	15	15	13	~~15~~	~~8~~		6	14	~~12~~	11	5	8
11	Privilege Escalation		16	16	11	~~16~~	~~12~~		15	9	~~15~~	6	11	3
12	Execution				14		~~15~~		16	15	~~16~~	10	6	12
13	Credential Access				~~12~~		~~16~~			16		7	10	~~15~~
14	Lateral Movement				~~15~~					7		8	7	~~16~~
15	Collection				~~16~~					18		3	8	
16	Exfiltration											8	3	
17	Impact											~~12~~	8	
18	Objectives											~~15~~	~~12~~	
												~~16~~	~~15~~	
													~~16~~	

4.2 APT29 (also known as: Cozy Bear, NOBELIUM, Midnight Blizzard, The Dukes, CozyDuke, IRON RITUAL, IRON HEMLOCK)

APT29 is a sophisticated APT group that multiple research groups have identified as having been active since at least 2008 (Faou, Tartare, & Dupuy, 2019; F-Secure, 2015a). However, the cyber security company Sekoia.io believes that APT29 has in fact been active since 2004 (Sekoia.io, 2023). The group has many aliases, though APT29 has remained as the most prominent one as it often connects the different names. The group has also been called "The Dukes" by F-Secure, "Cozy Bear" by Crowdstrike, "NOBELIUM" and then later "Midnight Blizzard" by Microsoft, and "IRON RITUAL" as well as "IRON HEMLOCK" by

[1] References: **C1-1**: ESET, 2018a, **C1-2**: Kharouni et al., 2014, **C1-3**: Jazi & Santos, 2022, **C1-4**: Smith & Read, 2017, **C1-5**: Creus, Halfpop, & Falcone, 2016, **C1-6**: Lee, Harbison, & Falcone, 2018, **C1-7**: Lee & Falcone, 2018, **C1-8**: Anthe et al., 2015, **C1-9**: Mueller, 2018, **C1-10**: Falcone & Lee, 2016, **C1-11**: ESET, 2016, **C1-12**: ESET, 2016, **C1-13**: ESET, 2019

Secureworks (Crowdstrike, 2022c; F-Secure, 2015a; Microsoft, 2023; Van Geluwe De Berlaere, 2022).

The group has been known to often target governmental organizations such as embassies, ministries of defence, or ministries of foreign affairs especially in western or ex-USSR countries as well as some government adjacent organizations like NATO, research institutions, think tanks, or political parties (Aimé, 2022; Cash et al., 2021; Faou, Tartare, & Dupuy, 2019; F-Secure, 2015a). APT29 has also targeted some organizations that are from industries which are not directly government linked like media, pharmaceutical, healthcare, IT, and telecommunications (Aimé, 2022; Dunwoody et al., 2018; National Cyber Security Centre UK, 2020). There is also some indication that APT29 has for a limited period targeted Russian speaking drug dealers (F-Secure, 2015a).

APT29 is known for some especially high-profile attacks that have been attributed to it, such as the breach of multiple organizations worldwide with a supply chain attack by breaching a company called "Solarwinds" and an attack against the DNC starting in 2015, where APT29 was identified as having breached the DNC systems before APT28, in apparently separate operations (Crowdstrike, 2020; FireEye, 2020).

In a similar way to APT28, APT29 has been connected to the Russian government with differing levels of confidence and specificity. The governments of the United States and United Kingdom, the Dutch intelligence service AIVD as well as the cyber security company Mandiant have connected APT29 to Russian foreign intelligence service SVR, while other organizations like Microsoft willing to only go as far as describing APT29 as a "Russian nation-state actor" and F-Secure stating that they are likely a group working for, or being sponsored by, the Russian government (Bienstock, 2022; Burt, 2021; F-Secure, 2015a; Michael, 2020; Modderkolk, 2018;National Cyber Security Centre UK, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Security Agency, 2021; National Security Agency, Cybersecurity & Infrastructure Security Agency, & Federal Bureau of Investigation, 2021). There isn't complete agreement in attribution of APT29 however, the Estonian foreign intelligence service connects the group to the Russian federal security service FSB as well as to the SVR (Välisluureamet, 2018).

APT29 has been connected to attacks where the apparent goal has been to covertly collect information from the targets by accessing their networks then expanding their privileges and access to reach the most sensitive information which has then been exfiltrated (F-Secure, 2015a; Mandiant, 2022b; National Cyber Security Centre UK, 2020; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). Though it should be noted that one malware attributed to APT29 has capabilities outside information gathering, a module for denial-of-service attacks and a module for posting spam on a Russian social media network. There are however no indications that APT29 has used these capabilities in their operations (Faou, Tartare, & Dupuy, 2019; F-Secure, 2015a).

The group is believed to have access to malware development capabilities which has led to the group using many different malware types, written in multiple different programming languages, and the malware being developed further to avoid detection (Faou, Tartare, & Dupuy, 2019; FireEye, 2015b; Recorded Future, 2023). For example, the group was identified as having operated 9 distinct malware types with differing features just between 2008 and 2015 (F-Secure, 2015a). It is however not clear if the group is writing its own malware or if the group is working with outside developers. Similarities that have been identified between malware connected to APT29 and malware connected to Turla could suggest the groups share developers or that the groups are otherwise connected (Kucherin, Kuznetsov, & Raiu, 2021). Recent reporting on documents leaked from a Russian IT company "NTC Vulkan" suggest that the company develops software tools for multiple APT groups that are connected to the Russian state, including APT29. According to the reporting the company has created tools for supporting and automating certain aspects of cyberattacks, but it is not clear if these supportive tools are being used by APT29 or if company is creating any malware used by APT29. The article does state that an employee from the company took part in an operation spreading MiniDuke, one malware used by APT29, which indicates a close relationship between APT29 and the company. (Antoniadis et al., 2023)

APT29 has been observed as having an exceptionally high level of operations security. This appears to be to obfuscate the true origin of their attacks, to avoid detection by defenders, and to thwart the attempts by security researchers to identify the group's operations and malware (Bienstock, 2022; FireEye, 2020; Mandiant, 2022b; Microsoft Threat Intelligence Center, 2021a; Recorded Future, 2022). This however contrasts with the first thorough report on the group by researchers, which describes APT29's campaigns as mostly fast "smash-and-grab" operations, where being identified is not an issue (F-Secure, 2015a). This could suggest that the group has evolved its operating procedures over time or the priorities for the group have changed.

4.2.1 Identified TTPs

The different capabilities, tactics, techniques, and procedures of APT29 were analysed through various reports and whitepapers that describe operations conducted by APT29, malware used by APT29 and the group itself. For this purpose, 64 different publications were studied to identify APT29's use of, or the capability to use, the various TTPs which were divided into the phases of the Unified Kill Chain. The following TTPs represent the totality of the TTPs that APT29 has used, or has the capability to use, not any specific attacks or TTPs used in a specific attack.

Reconnaissance: Cyber security researchers have observed APT29 using tracking URLs in initial phishing emails as a form of reconnaissance to record which targets that have clicked on the links and when they have done so (Barnett, 2021; Microsoft Threat Intelligence Center, 2021b). Governmental agencies from the United States and United Kingdom have also identified APT29 having actively scanned for known vulnerabilities in multiple software products in their target's networks (National Cyber Security Centre UK, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Security Agency, 2021; National Security Agency, Cybersecurity & Infrastructure Security Agency, & Federal Bureau of Investigation, 2021). APT29 has also been observed scanning external services of their target to find an access vector after being initially removed from a network (Crowdstrike, 2022c).

Resource Development: APT29 has conducted some form of resource development in every kill chain that was identified from the material. Often this consists of developing or modifying the malware used for each attack (FireEye, 2015b; F-Secure, 2015a). APT29 has also been known to register typosquatting domain names, but also some malware used by APT29 takes advantage of Domain Generation Algorithms (DGA) so the attacker can register domain names in advance, knowing which domain names are generated by their malware and when (Eckels, Smith, & Ballenthin, 2020; Recorded Future, 2022). The group has also used a specific domain name provider that accepts bitcoin as payment and that has also been used by other APT groups in the past (Smith, Leathery, & Read, 2021). APT29 has also set up command & control channels by using legitimate services like Twitter, Github, Trello, Dropbox, and Slack. (FireEye, 2015b; QiAnXin Technology, 2022; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022).

Delivery: Email is APT29's most common initial delivery method in the group's operations, this has often meant emails with a download link to a malicious file or malicious file as an attachment in the email (Adair, 2016; Faou, Tartare, & Dupuy, 2019; F-Secure, 2015a). APT29 has also used supply chain attacks as its delivery method. This became more widely known with the notorious Solarwinds compromise where a software update, tampered to include malware by APT29, was downloaded by 18000 different Solarwinds customers (Ramakrishna, 2021). However, even before the Solarwinds attack APT29 has used a form of supply chain attack, the group has injected their malware into software that was uploaded to torrent sites (F-Secure, 2015a). The group has also run a malicious TOR network node that injects their malware into software as it was being downloaded (Lehtiö, 2014). The group has often used their initial access malware to deliver additional malware, however often only in specific cases where the victim was deemed interesting enough to warrant additional attention (Faou, Tartare, & Dupuy, 2019; F-Secure, 2015a; Polish Military Counterintelligence Service & CERT-PL, 2023). APT29 has also been identified using stolen credentials as its initial access method into a system. Interestingly, it has been suggested that in one case APT29 obtained the stolen credentials from a third party, the operator of an unrelated info-stealer malware that had compromised the victim earlier (Jenkins, Sarah, Parnian, & Bienstock, 2021). Mandiant has also suggested that APT29 has also used web server compromises and password spraying as its initial access vector (Mandiant, 2022b).

Social Engineering: In most operations APT29 employs some form of social engineering techniques. This is often related to some sort of email lure where the apparent contents of the emails are made to appear relevant to the victim or otherwise pique the victim's interest (Microsoft Threat Intelligence Center, 2021b;

Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). The group's use of social engineering also extends to creating decoy documents that are shown to a victim as a malicious program is starting to distract the victim, and to modifying shortcut files to appear as a document file instead of a malicious program (Tivadar, BALÁZS, & Istrate, 2013; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022).

Exploitation: APT29 has used multiple exploits to deploy their malware, to gain access to the victim system, and to gain higher privileges on a target system. Two of the vulnerabilities identified as being exploited by APT29 were zero-days at the time they were used. The group has used vulnerabilities in Adobe Reader and Acrobat products as well as Microsoft Word to create exploits within malicious documents which would allow the group's malware to be deployed. (ESET, 2014b; Hirvonen, 2014; Tivadar, BALÁZS, & Istrate, 2013) The group also used multiple vulnerabilities found in Microsoft Windows operating systems in order to achieve privilege escalation (ESET, 2022; F-Secure, 2015a). The group has also attempted to exploit vulnerabilities in multiple brands of network devices or network software such as Fortinet and Cisco routers, Citrix and Pulse Secure networking solutions, and Zimbra and Microsoft Exchange email servers (Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; National Cyber Security Centre UK, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Security Agency, 2021). APT29 has also been identified using an exploit for Apple iPhones (Microsoft Threat Intelligence Center, 2021b).

Persistence: The group has been identified using a wide variety of persistence methods to maintain their access to a compromised system. These techniques include creating or modifying registry keys, modifying crontab, adding accounts, creating windows services, and creating scheduled tasks (Crowdstrike, 2022c; Dunwoody, 2017a; F-Secure, 2015b; Recorded Future, 2023). Researchers have also identified multiple malware types connected to APT29 which appear to have maintaining persistence as the main goal (F-Secure, 2015a; Nafisi & Lelli, 2021).

Defense Evasion: APT29 has used many different techniques for defense evasion. Most notably APT29 used Twitter as a part of its infrastructure as early as 2011 in order to avoid detection, as connections to Twitter would seem normal in most networks. Using this technique APT29's malware search for tweets from a specific Twitter account which contain the address for the command & control servers in encrypted form (Tivadar, BALÁZS, & Istrate, 2013). This technique was further improved later to include an algorithm that generated a new Twitter account name for every day, which the malware would look for, so only the group itself would know which accounts to create and use. To complicate detection even further another improved version was created to take advantage of a technique called steganography. In this version the tweets would include images that would contain the address to the command & control server in hidden form. (FireEye, 2015b) This similar technique of using legitimate online services as a part of the attackers' infrastructure was later continued with services like Trello, Slack, Notion, Dropbox, and Google Drive (Harbison & Renals, 2022; QiAnXin

Technology, 2022; Recorded Future, 2023; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). The group has also taken advantage of the TOR network to avoid detection, with a technique called domain fronting (Dunwoody, 2017b). APT29 has also often simply used encrypted communication to avoid detection (Dunwoody, 2017a; Symantec, 2017). The group also used a domain generation algorithm (DGA), which can be used to generate new domain names with a certain logic, in order to avoid detection by predictable domain names. The domain names generated with the domain generation algorithm were notably used for command & control servers in the compromise of Solarwinds. Instead of a completely random domain name, which could draw more attention, only the beginning of each domain name was generated to include encoded information about the compromised system with the ending being consistent and disguised as outwardly legitimate. (Symantec, 2021a) APT29 has also used a very wide variety of more common defence evasion techniques such as HTML smuggling, where malicious data is embedded into an HTML file, using legitimate software for DLL side loading, signing their malware, checking for security products on systems they have compromised, encrypted and compressed payloads, renaming tools and removing them after use, using multiple sets of credentials during a compromise, clearing logs, disabling logging and security products, and changing command & control server host names and IP addresses they connect from to match the victim's environment (Aimé, 2022; Crowdstrike, 2022c; Faou, Tartare, & Dupuy, 2019; Harbison & Renals, 2022; Mandiant, 2022b; Raiu, Soumenkov, Baumgartner, & Kamluk, 2013).

Command & Control: APT29 malware include methods for communication with command & control servers, often also including an alternative method as a backup (F-Secure, 2015a; Nafisi & Lelli, 2021; PwC, 2020). Notably APT29 has used multiple legitimate services as a part of its command & control network as described earlier. The group has also been noted as using typosquat domain names for its command & control servers and sometimes registering the domain names as early as a year before using them (Aimé, 2022; Recorded Future, 2022). It has been suggested that APT29 has also possibly used compromised infrastructure as command & control servers (Crowdstrike, 2022c). For some attacks APT29 has also prepared unique command & control servers for each compromised host to make finding all compromised hosts more difficult (Microsoft Threat Intelligence Center, 2021c). For its communications with the command & control servers APT29 has used multiple protocols, these include HTTP, DNS, FTP and WebDav (F-Secure, 2015a; PwC, 2020). APT29 has also been known to use named pipes for communication within a local network (Faou, Tartare, & Dupuy, 2019).

Pivoting: APT29 has used the SSH tunnelling technique to pivot and use already compromised systems and devices for lateral movement (Crowdstrike, 2022c). The group has also used the commercial penetration testing product Cobalt Strike to create tunnels for pivoting purposes as well abusing compromised "jump hosts" to pivot further into the victim networks (Barnett, 2021; Jenkins, Sarah, Parnian, & Bienstock, 2021). APT29 has also built some pivoting capabilities into one of their own malware called FatDuke (Faou, Tartare, & Dupuy, 2019).

Discovery: Malware used by APT29 often includes capabilities for gathering information about the compromised system. This information has been used, for example, to decide if the victim is interesting enough to warrant further attention, to check if it has been compromised already, or to create a unique fingerprint as an encryption key to a malicious payload (ESET, 2014b; Tivadar, BALÁZS, & Istrate, 2013; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). APT29 has also used other methods for discovery: the group has used living off the land techniques like Powershell and used some popular open-source tools such as AdFind and BoodHound (ANSSI, 2021; Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; Crowdstrike, 2022c). Some malware used by APT29 also has features to perform discovery of the network and the network domain that the compromised system is in (Eckels, Smith, & Ballenthin, 2020; ESET, 2014b; Microsoft Threat Intelligence Center, 2021d).

Privilege Escalation: APT29 has been found to have used multiple Windows operating system vulnerabilities to achieve privilege escalation after an initial compromise (ESET, 2022; F-Secure, 2015a). These vulnerabilities have been used with a specific privilege escalation module of their CosmicDuke malware and through a specific tool (ESET, 2022; F-Secure, 2015a; Van Geluwe De Berlaere, 2022).

The group has also used various living off the land techniques, such as modifying shortcuts, stealing credentials by dumping the memory of the LSASS process with Windows Task Manager, creating scheduled tasks, or exploiting the "sticky keys" feature for privilege escalation (Dunwoody, 2017b; Jenkins, Sarah, Parnian, & Bienstock, 2021; Mandiant, 2022b). APT29 has also used Mimikatz on multiple occasions to steal credentials, possibly to escalate privileges. Sometimes this has been done by downloading the tool on a compromised machine using their existing tools. (Crowdstrike, 2022c; F-Secure, 2015a) These stolen credentials have then sometimes been used to escalate privileges further, by forging authentication tokens to reach the desired system or level of access (Microsoft 365 Defender Team, 2020).

Execution: APT29 has used a variety of methods for executing their code on a compromised machine. The initial code execution has often been achieved with email-based attacks by social engineering a user into executing the malicious payload, notably very often using shortcut files (Baumgartner & Raiu, 2015; Microsoft Threat Intelligence Center, 2021b; Polish Military Counterintelligence Service & CERT-PL, 2023). APT29 has also used exploits that were embedded into documents for the initial code execution (ESET, 2014b; Tivadar, BALÁZS, & Istrate, 2013). The group has used Powershell, cmd.exe, and rundll32.exe in combination with these malicious files and shortcut files to perform code execution (Aimé, 2022; Dunwoody et al., 2018; Harbison & Renals, 2022).

After the initial execution phase the group has used their malware to execute additional payloads or commands (Barnett, 2021; F-Secure, 2015a; Hirvonen, 2014; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). Many malware used by APT29 execute additional payloads or commands via built-in capabilities like Powershell or cmd.exe (Levene, Falcone, & Wartell, 2015; Microsoft

Threat Intelligence Center, 2020b; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). APT29 has also used some of these same built-in capabilities to perform execution manually, these include many Windows native tools like cmd.exe, wscript.exe, WMI, Powershell, Remote WMI, Azure's built-in "Run Command" feature, PsExec, and local as well as remote task scheduling (Crowdstrike, 2022c; Faou, Tartare, & Dupuy, 2019; Jenkins, Sarah, Parnian, & Bienstock, 2021; Microsoft Threat Intelligence Center, 2021c; Nafisi & Lelli, 2021). In some situations, the group has used DLL side loading and DLL search order hijacking to execute their malicious DLL-files (Harbison & Renals, 2022; Nafisi, 2021). APT29 has also been identified using an open-source tool Sharp-SMBExec to perform code execution via the SMB protocol on remote machines (ESET, 2022).

During the Solarwinds compromise the group managed to sneak their code into a legitimate component of the Solarwinds product and cause their code to be loaded as the program ran normally (Microsoft Threat Intelligence Center, 2020b). In the same attack APT29 added an Image File Execution Options Debugger value for a native Windows executable, dllhost.exe, which caused their code to be executed when the executable was run coincidentally during normal operations (Microsoft Threat Intelligence Center, 2021c).

Credential Access: APT29 has used a variety of methods and tools to gain access to credentials. These methods and tools have been used to steal email credentials, network domain credentials, certificates, cryptographic secret keys, Wi-Fi passwords, browser passwords, passwords for instant messaging services, password hashes, and cookies (Crowdstrike, 2022c; F-Secure, 2015a; Hirvonen, 2014). Notably multiple malware used by APT29 have password, certificate, or other credential stealing as one of their features and some seem to have been used mainly for that reason (F-Secure, 2015a; Mandiant, 2022b; Nafisi, 2021; Symantec, 2021b). One APT29 malware also has a separate keylogger module, though it is not clear if it has been used for credential access, as the same tool also has other password stealing features (Hirvonen, 2014).

The group has also used various other tools for credential access. These include Mimikatz, DSInternals, Responder, custom credential stealing tool named MAMADOGS, Procdump, and a custom tool to dump credentials from Solarwinds Orion databases (Crowdstrike, 2022c; Jenkins, Sarah, Parnian, & Bienstock, 2021; Mandiant, 2022b; Microsoft Threat Intelligence Center, 2021d; Symantec, 2021b).

APT29 has also attempted to gain credential access by searching for stored passwords inside compromised systems, searching through email boxes, modifying accounts, bruteforcing accounts, forging authentication tokens, adding more keys or passwords, precomputing cookies, and kerberoasting (Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; Mandiant, 2022b; Microsoft, 2020; Microsoft Threat Intelligence Center, 2021c; National Cyber Security Centre UK, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Security Agency, 2021; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). Additionally, in one instance APT29 has possibly even purchased stolen credentials from a third party (Jenkins, Sarah, Parnian, & Bienstock, 2021).

Lateral Movement: APT29 has employed multiple methods for lateral movement. These methods often rely on stolen passwords or other credentials (Jenkins, Sarah, Parnian, & Bienstock, 2021; Microsoft Threat Intelligence Center, 2022; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). ATP29 has also used various tools to perform lateral movement. The group has used their own Raindrop malware, Mimikatz, and a tool called SMB beacon from Cobalt Strike for lateral movement (Crowdstrike, 2020; Symantec, 2021b; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). The group's FatDuke malware also has features that support lateral movement inside a local network (Faou, Tartare, & Dupuy, 2019).

In addition to stolen credentials, malware, and additional tools, the group has also used some living off the land methods for lateral movement. These include remote WMI, PsExec, SMB tools, SSH tunneling, remote scheduled task creation, Remote Desktop Protocol (RDP) tool, and the creation of a certificate to imitate privileged accounts for lateral movement (Crowdstrike, 2022c; Faou, Tartare, & Dupuy, 2019; Jenkins, Sarah, Parnian, & Bienstock, 2021; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022).

Researchers have noted that APT29's lateral movement is exceptional as they sometimes use different credentials for lateral movement and perform reconnaissance before their lateral movement, change credentials for each lateral movement hop, and prepare their lateral movement by checking for, and if necessary, removing security products that are running on the systems (Jenkins, Sarah, Parnian, & Bienstock, 2021; Microsoft Threat Intelligence Center, 2021c).

Collection: Many APT29 malware have specific modules or features specifically to allow for information collection (Faou, Tartare, & Dupuy, 2019; F-Secure, 2015a; Symantec, 2017). The malware used by APT29 have capabilities for listing the contents of directories, stealing specific token signing certificates for Azure Directory Federation Service (ADFS), stealing browser data, logging keystrokes, taking screenshots, stealing various passwords and cryptographic secret keys as well as stealing files from removable drives (Hirvonen, 2014; Mandiant, 2022b; Tivadar, BALÁZS, & Istrate, 2013). Some APT29 malware collect information by searching for files with specific file extensions, specific filenames, or files that were created after a specific time (F-Secure, 2015a; Hirvonen, 2014).

The group has also used some living off the land methods to perform information collection, namely Powershell, as well as some built-in features of browsers and operating systems (Crowdstrike, 2022c; Jenkins, Sarah, Parnian, & Bienstock, 2021). APT29 has also collected data by stealing emails from victims' inboxes, collecting data from various internal repositories, cloud storage as well as shared network drives (Bienstock, 2022; Crowdstrike, 2022c; Mandiant, 2022b; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). Before exfiltration APT29 has been known to archive stolen data by using a legitimate file archiving program 7-Zip (Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; Microsoft Threat Intelligence Center, 2021c).

Exfiltration: Many APT29 malware have capabilities for the exfiltration of data from the victim machine to attacker controller infrastructure, ranging from individual files to lists of files (Faou, Tartare, & Dupuy, 2019; Levene, Falcone, & Wartell, 2015; Tivadar, BALÁZS, & Istrate, 2013). The malware used by APT29 can perform exfiltration via HTTP, FTP, and WebDav protocols (F-Secure, 2015a). APT29 often uses encryption in its exfiltration techniques, either by encrypting the data to be exfiltrated or exfiltrating via an encrypted connection (Barnett, 2021; Hirvonen, 2014; Mandiant, 2022b). The group has also used additional techniques outside their malware for exfiltration. APT29 has exfiltrated data by mapping OneDrive as a network share, using a native API offered by a legitimate service, and downloading data staged to a victim's email server with a HTTP request (Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; Microsoft 365 Defender Team, 2020; Microsoft Threat Intelligence Center, 2021c).

Impact: APT29 was identified using an impact technique in the compromise of Solarwinds. During the compromise the group inserted malicious code into the source code of the product, which was then delivered to victims (Microsoft Threat Intelligence Center, 2020b). One APT29 malware has a specific module for Denial-of-service attacks, however there is no indications that the group has used the tool to perform denial-of-service attacks (F-Secure, 2015a).

Objectives: APT29's objectives have been identified as the stealing of various forms of information from their victims (Hirvonen, 2014; Polish Military Counterintelligence Service & CERT-PL, 2023; Symantec, 2017). It has also been suggested that APT29 aims specifically for long term persistence in the victim system to allow their objectives to be met (F-Secure, 2015a; Microsoft Threat Intelligence Center, 2021c; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). APT29 has been identified stealing specifically politically sensitive information as well as information relating to intellectual property (National Cyber Security Centre UK, 2020; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022).

4.2.2 ATP29's kill chains

APT29 kill chains were identified using the same method as with APT28. In total the same 64 publications about APT29 were examined as for the previous section and from them 13 kill chains were identified. These publications consisted of reports, whitepapers, and articles which were studied to identify the longest and most complete kill chains depicting APT29's operations. As many of the reports consisted of analysis of malware capabilities instead of thorough incident reports, the identification of the kill chains required some interpretative analysis in some cases, similar to the analysis of APT28 kill chains. Here, too, the interpretations made will be marked with a ~~strikethrough.~~ The 13 identified kill chains are listed in the table (Table 2) marked C2-1, C2-2 etc. in no particular order. Using the same visualization method as in the earlier section, the kill chains show the sequence of events within one realized attack, the group's described tendency, or capability to attack. The sequence of events is described by indicating the occurrence of a TTP by a number representing the UKC phase the TTP belongs to. The numbers and the UKC phase they represent are included in the leftmost column in the table. The sequence of events begins at the top row of each column with events unfolding down the column. A **black line** was included in the table to note the point at which one system was considered as compromised and command & control connection is established, and the initial compromise phase was over.

APT29's kill chains had almost identical initial steps with two kill chains being the outliers. One of the outlier kill chains (C2-8) included a reconnaissance step that could be identified before resource development, delivery, and social engineering. The other outlier kill chain (C2-6) began with resource development and delivery, before including impact techniques. All the other kill chains started with the same steps: resource development, delivery, and social engineering before deviating as the kill chain advanced. However, the types and methods for resource development, delivery, and social engineering differed somewhat between the kill chains.

Almost all the identified APT29 kill chains had spear phishing through email as the initial attack path. However, there was some variance in how the spear phishing was done: some attacks were done with a malicious document that contained an exploit within the email attachment (C2-1, C2-10, C2-13), while some attacks used different packaged or archived file as the email attachment, which then contained the malicious files (C2-2, C2-3, C2-4, C2-7, C2-8). In some attacks links were used within the emails or in decoy files that led to a malicious download (C2-9, C2-11, C2-12).

The attacks that used a malicious document with exploits (C2-1, C2-10, C2-13) also took advantage of social engineering. Social engineering was used to get the victim to open the initial email or email attachment. Attacks which did not use exploits often relied on additional social engineering, initially to trick the victim to open the links or documents and then separately to execute malicious programs or perform other unsafe actions (C2-2, C2-3, C2-8, C2-9, C2-11, C2-12).

In the remaining kill chains the initial access vector was uncertain (C2-5, C2-6). However, in the C2-5 kill chain a malicious document was used, and it was suspected to have been sent via email as well, so for the purpose of this analysis the initial attack path for C2-5 will be considered to be spear phishing. The uncertain kill chains also include the Solarwinds compromise kill chain (C2-6) where the initial attack vector into the final victim network was through the supply chain attack, but the attack vector into Solarwinds itself is unknown. The Solarwinds compromise continues from the unknown initial delivery by impacting the Solarwinds source code (C2-6). It should also be noted that APT29 has been known to conduct some other attacks without email as the initial access vector (Jenkins, Sarah, Parnian, & Bienstock, 2021; Lehtiö, 2014).

After initial access was gained, the kill chains continued in varying order starting with defense evasion (C2-2, C2-3, C2-6, C2-7, C2-8), additional delivery where another payload is extracted from the initially delivered material (C2-4, C2-9, C2-11, C2-12), or code execution following exploitation or social engineering (C2-1, C2-5, C2-10, C2-13). The C2-7 kill chain is the only one identified that did not include additional delivery and C2-6 was the only one that did not include execution in the initial attack phase. These steps are often followed by the setting up of persistence (C2-4, C2-5, C2-9 C2-10), performing discovery techniques (C2-1, C2-2, C2-6, C2-7, C2-13), and additional occurrences of delivery, social engineering, or defense evasion (C2-3, C2-8, C2-12). If execution has was not reached earlier, execution is usually reached here (C2-2, C2-3, C2-8, C2-11, C2-12) before ending the initial attack phase by connecting to the command & control server.

Almost all APT29's kill chains include the delivery of further payloads after the command & control stage, only two kill chains being the outliers (C2-6, C2-12). Often the kill chain was advanced further only if the victim was deemed interesting enough (Faou, Tartare, & Dupuy, 2019; Polish Military Counterintelligence Service & CERT-PL, 2023; Symantec, 2017). For most identified kill chains, the delivery of additional payloads or tools leads to execution (C2-1, C2-2, C2-3, C2-4, C2-8, C2-9, C2-10, C2-11). For other kill chains, the execution is preceded by other steps, performing persistence techniques for C2-7 and defense evasion, persistence, connections to command & control server, and second occurrence of defense evasion for C2-5. In the remaining kill chain additional discovery is performed before delivering another payload through the command & control server and only then reaching execution (C2-13).

Some kill chains end after reaching execution (C2-3, C2-8, C2-9, C2-11, C2-13), with some ending after first performing collection and exfiltration (C2-1, C2-10, C2-12). One kill chain ends after credential access and collection (C2-4). The remaining kill chains have a more unique path.

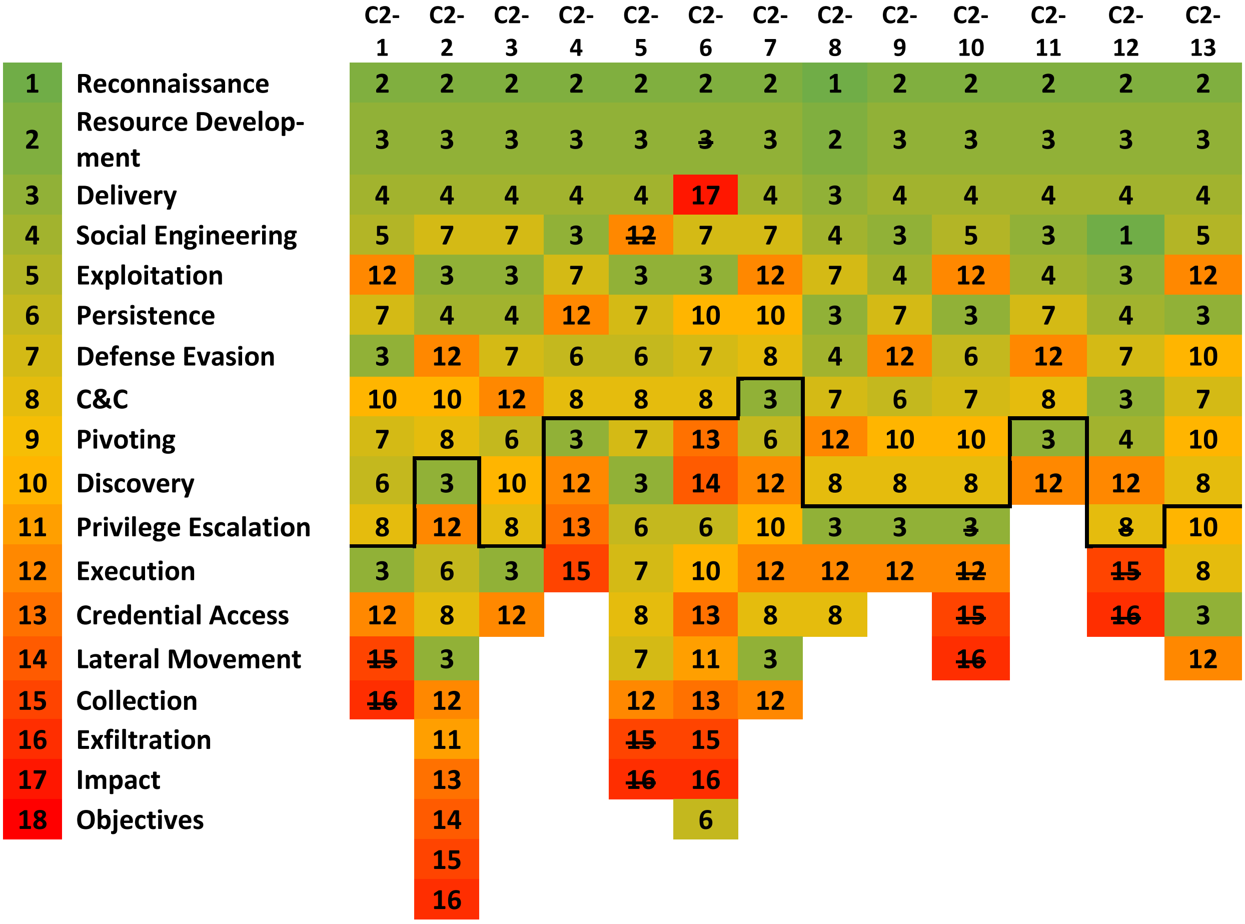
The longest APT29 kill chain C2-2 continued after the initial attack phase with delivery and execution as mentioned earlier, which were then followed by performing persistence techniques before delivering another additional payload from a command & control server. This leads to execution, privilege escalation, and credential access into lateral movement which allowed APT29 to perform the final steps of collection and exfiltration.

For the kill chain C2-5 the initial attack phase was followed by more defense evasion and the delivery of another payload. This payload was used for additional persistence and performed additional defense evasion. Command & control server was contacted again before more defense evasion techniques were performed. This was followed by execution that led APT29 to perform the final steps of collection and exfiltration.

The Solarwinds compromise depicted in C2-6 continued from the initial attack phase by credential access techniques which led to lateral movement. This was followed by persistence and discovery before additional credential access techniques were performed that led to privilege escalation. APT29 then performed collection, exfiltration, and finally adding their final persistence.

The last unique kill chain C2-7 performed additional delivery, persistence, and execution after the command & control server connection like other kill chains. This was followed by discovery, additional execution, and the delivery of yet another payload via command & control server which was then followed by execution as the final step.

TABLE 2 Identified APT29 kill chains[2]



		C2-1	C2-2	C2-3	C2-4	C2-5	C2-6	C2-7	C2-8	C2-9	C2-10	C2-11	C2-12	C2-13
1	Reconnaissance	2	2	2	2	2	2	2	1	2	2	2	2	2
2	Resource Development	3	3	3	3	3	~~3~~	3	2	3	3	3	3	3
3	Delivery	4	4	4	4	4	17	4	3	4	4	4	4	4
4	Social Engineering	5	7	7	3	~~12~~	7	7	4	3	5	3	1	5
5	Exploitation	12	3	3	7	3	3	12	7	4	12	4	3	12
6	Persistence	7	4	4	12	7	10	10	3	7	3	7	4	3
7	Defense Evasion	3	12	7	6	6	7	8	4	12	6	12	7	10
8	C&C	10	10	12	8	8	8	3	7	6	7	8	3	7
9	Pivoting	7	8	6	3	7	13	6	12	10	10	3	4	10
10	Discovery	6	3	10	12	3	14	12	8	8	8	12	12	8
11	Privilege Escalation	8	12	8	13	6	6	10	3	3	~~3~~		~~8~~	10
12	Execution	3	6	3	15	7	10	12	12	12	~~12~~		~~15~~	8
13	Credential Access	12	8	12		8	13	8	8		~~15~~		~~16~~	3
14	Lateral Movement	~~15~~	3			7	11	3			~~16~~			12
15	Collection	~~16~~	12			12	13	12						
16	Exfiltration		11			~~15~~	15							
17	Impact		13			~~16~~	16							
18	Objectives		14				6							
			15											
			16											

4.3 Turla (also known as: Snake, WhiteBear, Venomous Bear, Waterbug, Uroburos, Pacifier APT)

Turla is one of the longest operating APT groups identified as it has been connected to one of the earliest known APT campaigns, "Moonlight Maze", that began at the latest in 1996 (Federal Bureau of Investigation et al., 2023; Guerrero-Saade, Raiu, & Rid, 2018). Before this connection was made it was widely thought that the group had only begun its activities in 2004 (Leonardo, 2020; Office of Information Security Securing One HHS & Health Sector Cybersecurity Coordination Center, 2022; Unterbrink, 2021). Like previous groups Turla has also been identified with multiple different names, with Turla seeming to be the most prominent name for the group. Turla has also been named "Snake" by BAE

[2] References: **C2-1**:Raiu, Soumenkov, Baumgartner, & Kamluk, 2013, **C2-2**: Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022, **C2-3**: Harbison & Renals, 2022, **C2-4**: F-Secure, 2015b, **C2-5**: Faou, Tartare, & Dupuy, 2019, **C2-6**: Microsoft 365 Defender Team, 2020, **C2-7:** Microsoft Threat Intelligence Center, 2021d, **C2-8**: Cash et al., 2021, **C2-9**: QiAnXin Technology, 2022, **C2-10**: Tivadar, BALÁZS, & Istrate, 2013, **C2-11**: Microsoft Defender Security Research Team, 2018, **C2-12**: Microsoft Threat Intelligence Center, 2021b, **C2-13**: ESET, 2014b

Systems, “Venomous Bear” by Crowdstrike, “Waterbug” by Symantec, “Uroburos” by G Data, and “Pacifier APT” by Bitdefender (BAE Systems, 2014; Bitdefender, 2015b; Crowdstrike, 2022d; Rascagnères, 2014; Symantec, 2016). The WhiteBear alias was given by Kaspersky to a group believed to be a subgroup of Turla (Kaspersky Labs, 2017). Interestingly Crowdstrike has recently removed mentions of “Venomous Bear” from their lists of adversaries.

Turla has been connected to multiple high-profile attacks on specific government entities such as the US Central Command, Finnish and Austrian Foreign Ministries, German Foreign Office, and the French Armed Forces (Faou, 2020a). The group has been noted as being particularly careful and selective in its target selection and often specifically targets governmental organizations such as ministries of foreign affairs, embassies, consulates, as well as defence and military organizations, and research and education organizations (Faou, 2020a; Federal Bureau of Investigation et al., 2023; Kaspersky, 2023c; Kaspersky Labs, 2014a). These targeted organizations are from most regions of the world with a noted focus on Europe, the Middle East, Central Asia, and the United States (Google Threat Analysis Group, 2023).

Like the previous groups Turla has been connected to the Russian government by multiple organizations. Some organizations like the cyber security companies Kaspersky, Proofpoint, and Crowdstrike going only as far as noting that the group is Russian-speaking or Russian-originating, while Google and cyber security company Sekoia.io attributing the group more specifically to the Russian Federal Security Service FSB (Couchard & Arquillière, 2022; Crowdstrike, 2022d; Google Threat Analysis Group, 2023; Huss, 2017; Kaspersky Labs, 2019). Governments have also connected Turla to the FSB. In a joint advisory multiple governmental organizations from the United States, United Kingdom, Canada, New Zealand, and Australia have attributed Turla to a specific unit within the FSB (Federal Bureau of Investigation et al., 2023). In a separate publication, the Estonian foreign intelligence service has also connected Turla to the FSB and even named the same unit (Välisluureamet, 2018).

Turla has been known to perform attacks where the goal has been to collect sensitive information from carefully selected targets while maintaining their access and staying undetected (Faou, 2019; Faou, 2020a; Federal Bureau of Investigation et al., 2023). This information collection often appears to be done for espionage purposes (Faou, 2020b; Federal Bureau of Investigation et al., 2023; Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023; Office of Information Security Securing One HHS & Health Sector Cybersecurity Coordination Center, 2022).

Turla has used many custom malware in its operations. These include first stage malware like Tavdig or Skipper that the group uses to perform initial reconnaissance and deploy tools or additional malware, second stage malware like Carbon or Gazer which can be used to ensure persistence or to steal sensitive information from the victim, rootkit malware like Snake that are specifically designed to be very difficult to detect and remain hidden to steal information, malware specifically targeting email servers and clients, and even one Android malware (ESET, 2017a, 2017b, 2018, 2019; Federal Bureau of Investigation et al., 2023;

Kaspersky Labs, 2014a; Leonard, 2022). The group has also used some open-source tools like Mimikatz and Metasploit as well as taking advantage of code from an open-source project (GovCERT.ch, 2016).

There are some indications that the operators and developers for Turla are not the same people. The governmental organizations from the United States, United Kingdom, Canada, New Zealand, and Australia that attributed Turla to a unit inside FSB, consider the Snake malware to have been developed by FSB officers from a specific FSB office in Rayzan while the operation of the malware is done from another FSB office (Federal Bureau of Investigation et al., 2023). As noted in the APT29 section, some similarities were identified with a malware used by APT29 and another malware used by Turla. Additional similarity was also found with Turla and APT28, as Turla has used a technique in almost an identical way as APT28 (Kaspersky Labs, 2018b; Kucherin, Kuznetsov, & Raiu, 2021).

Turla has often been described as particularly innovative and willing to evolve its tools and techniques (Bartholomew, 2017; Cyware, 2020; Greenberg, 2023). This can be seen in some of the unique ways the group has operated, for example: Turla has taken over infrastructure of another APT group and used it to expand their foothold for their own operations, registered expired command & control domain names for a generic common malware to gain control of it, and used satellite-based internet links to maintain anonymity (Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023; National Cyber Security Centre UK, 2017; Tanase, 2015). In addition to being described as very selective in its targeting, the group has also been described as particularly stealthy, even being willing to remove their own tools and lose control of a compromised device to avoid being detected (ESET, 2018b, 2019a; Faou, 2020a; Kaspersky Labs, 2018b).

4.3.1 Identified TTPs

The capabilities, tactics, techniques, and procedures of Turla were analysed through various reports, articles, and whitepapers that describe attacks performed by Turla, malware used by Turla and the group itself. For this purpose, 65 different publications were studied to identify Turla's usage of, or capability to use, the TTPs divided into phases of the Unified Kill Chain. The TTPs listed and categorized below represent the totality of TTPs that Turla has used, or has the capability to use, not any specific attacks.

Reconnaissance: Turla has been identified performing different reconnaissance activities to research its victims. The group has used externally hosted image files embedded into documents to identify potential victims and to gain information about their systems (Couchard & Arquillière, 2022). Turla has also used watering hole attacks to perform profiling of possible victims and their device as well as attempting to track the future web browsing activities of possible victims (FireEye, 2015c). Turla has also scanned for devices infected by APT34, an Iranian APT group, to identify potential victims for themselves as they took over the infrastructure of APT34 (National Security Agency & National Cyber Security Centre UK, 2019).

Resource Development: In every Turla operation some form of resource development was present. For most attacks this means the development of the malware that was used, as many malware used by Turla are actively developed, sometimes for years (ESET, 2017a, 2017b, 2019; Federal Bureau of Investigation et al., 2023). Other resource development methods that were identified include setting up a satellite internet infrastructure, compromising and setting up web sites that are used for watering hole attacks, crafting malicious documents, and buying domain names for typosquatting or command & control use (Couchard & Arquillière, 2022; Faou, 2020c; Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023; Symantec, 2016; Tanase, 2015).

Delivery: Turla has used multiple delivery methods in its attacks to gain access into the victim networks and devices. One of the earlier Turla malware, named agent.btz, is a self-replicating and self-spreading malware. Agent.btz can spread itself through removable storage devices such as USB-drives and through shared network drives (Shevchenko, 2008). Other more common delivery methods for Turla are spear phishing emails that include malicious attachments and watering hole attacks that can deliver different exploits or malicious installers which the user is tricked into executing (Faou, 2020c; Kaspersky Labs, 2014a; Symantec, 2016). The group has also taken over the infrastructure of another APT group and used it as a delivery method to its victims (National Security Agency & National Cyber Security Centre UK, 2019). Turla has also used their own initial access malware to deliver more sophisticated malware, lateral movement tools, or various scripts after an initial compromise (ESET, 2018c; Faou & Dumont, 2019; Kaspersky Labs, 2014a). Turla has also used certutil.exe to deliver additional tools on a compromised machine (Symantec, 2019).

Social Engineering: In many operations Turla has taken advantage of social engineering tricks to confuse or trick victims into performing certain actions. The group has used social engineering often in conjunction with different email attachment files. Turla has for example used file names that create a sense of urgency, double file extensions like "document.doc.js", and created malicious documents that try to trick the victim into enabling macros in a Word document by claiming the document is "protected" and enabling macros is required to open it. (Bitdefender, 2015b) Turla has also used decoy documents to trick a victim while a malicious file has also been delivered (Huss, 2017). Additionally, the group has also tricked victims into running malicious installers which install a legitimate program as well as their malware (Faou, 2020c; Symantec, 2016).

Exploitation: Turla has used some exploits to gain code execution, deploy their malware, bypass security features, or in some cases to perform privilege escalation. The group has used exploits by creating malicious documents, including them into their watering hole websites or malware, or by using additional tools (BAE Systems, 2014; Kaspersky Labs, 2014a; Symantec, 2016). Two of the vulnerabilities that Turla has been known to exploit were zero-day vulnerabilities at the time. One zero-day exploit known to be used by Turla was for Adobe

Acrobat which was abused by creating a malicious PDF document that was sent to a victim as an email attachment. The group then used another exploit in combination to gain escalated privileges. (Symantec, 2016) The security feature bypass Turla performed was achieved by the Snake malware exploiting a vulnerability in the virtualization software Virtual Box (BAE Systems, 2014). Turla also used exploits with their watering hole attacks. The watering hole attacks have attempted to exploit a known Java vulnerability, but also some unknown exploits for Flash and Internet Explorer (Kaspersky Labs, 2014a). Turla has also exploited a similar zero-day vulnerability as APT28, both groups used malicious documents which targeted similar zero-day vulnerabilities in Microsoft Office (Jiang et al., 2017).

Persistence: Turla has used a wide variety of persistence methods, one malware used by Turla even has six different modes to set up persistence. The group also has two malware likely designed specifically to stay hidden and maintain persistence if their primary malware is identified and removed. (ESET, 2017; Faou & Dumont, 2019; Unterbrink, 2021) Besides using malware, the group has also used many other techniques to maintain persistence, like setting up a triggerable reverse shell, stealing existing accounts' passwords, or creating new accounts (Faou, 2020a; Federal Bureau of Investigation et al., 2023).

Defense Evasion: Turla has been identified using different forms of defense evasion in their operations. Some of the defense evasion techniques identified are more direct, like the sophisticated way Snake malware bypasses a kernel security feature called PatchGuard by abusing a vulnerable driver, or the way KopiLuwak malware checks for the existence of Kaspersky antivirus programs on a compromised device (BAE Systems, 2014; Huss, 2017). Other techniques Turla has used include creating malicious services that masquerade as legitimate ones, using living off the land methods like certutil.exe to execute commands, using steganography to hide command & control messages inside files, exfiltrating data only during a specified time of day, malware communicating to the command & control server by injecting into legitimate processes, encrypting communications to and from their command & control server, hiding malware related files, signing their malware, and even using Instagram posts as a proxy to a command & control server in a similar way to APT29 (BAE Systems, 2014; Bitdefender, 2015b; Boutin, 2017; Faou, 2019; Federal Bureau of Investigation et al., 2023; Kaspersky Labs, 2014a; National Cyber Security Centre UK, 2017).

Command & Control: Turla uses command & control servers in their operations and the malware used by Turla often even have alternative capabilities to connect to command & control servers should one fail (Faou, 2020a; G Data SecurityLabs, 2014; Levene, Falcone, & Halfpop, 2017). With the Snake malware Turla has created its own custom communication method that works on top of multiple different network protocols. These include lower-level protocols like TCP, UDP, and ICMP as well as higher level protocols like HTTP, SMTP, and DNS. (Federal Bureau of Investigation et al., 2023) Turla also has multiple malware with the capability for the infected devices to communicate directly, in a peer-to-peer fashion, with other devices infected by the same malware. This allows for command & control communication to and from infected systems that are not directly connected to the internet. (Accenture, 2020; ESET, 2017b; Federal Bureau of Investigation et al., 2023) This communication is often achieved via named pipes (Accenture, 2020; ESET, 2017b). Turla also has one malware with capabilities for communication over the FTP protocol (Levene, Falcone, & Halfpop, 2017).

The group has often used compromised servers for command & control purposes, but in some cases also as proxy command & control servers that relay the traffic to the real command & control servers (Kaspersky Labs, 2014a; Levene, Falcone, & Halfpop, 2017). As mentioned earlier, Turla has also innovated some ways they do command & control, they have used satellite-based Internet links to increase anonymity, used data hidden inside PDF or JPG files to issue commands and to exfiltrate data, and used legitimate services like Instagram or Github for their command & control infrastructure (Boutin, 2017; ESET, 2018b, 2019a; Faou, 2020b; Kaspersky Labs, 2014a; Levene, Falcone, & Halfpop, 2017).

Pivoting: Turla has used the technique of tunnelling traffic through already compromised systems in some of its operations. This was done in some cases to contact the command & control server, to exfiltrate data out of a system, or in some cases to obfuscate the real command & control server (GovCERT.ch, 2016; Kaspersky Labs, 2014a). Some malware used by Turla also have features specifically to perform pivoting through other machines (Accenture, 2020; Federal Bureau of Investigation et al., 2023).

Discovery: Within its operations Turla has often been identified performing wide ranging discovery techniques to gain information about the compromised system and to give a unique "fingerprint" to compromised systems (Kaspersky Labs, 2014a, 2019). The group has often simply used various scripts and native operating system commands to perform this information gathering (Bartholomew, 2017; G Data SecurityLabs, 2014). Many malware used by Turla have a set of discovery techniques or commands that are performed automatically (Bartholomew, 2017; Kaspersky Labs, 2014b, 2019). The group has also been identified using additional tools to perform discovery, such as network enumeration. This has been done using custom tools as well as legitimate tools like dnsquery. (Federal Bureau of Investigation et al., 2023; GovCERT.ch, 2016; Symantec, 2016) Turla has also used discovery techniques to aid in selecting targets for further exploitation. This has been done in watering hole attacks where some limited information is gathered about the victim's system, such as browser or plugin versions (Kaspersky Labs, 2014a). One of the fingerprinting scripts used by Turla has been found to have been taken from the BEEF framework, which is a publicly available browser exploitation framework (GovCERT.ch, 2016).

Privilege Escalation: Turla has been known to sometimes perform privilege escalation techniques during its operations. In some cases, the group has done this by exploiting different vulnerabilities. These include multiple different Windows privilege escalation vulnerabilities and a vulnerability in the virtualization software VirtualBox. (Kaspersky Labs, 2014a; Symantec, 2016) The vulnerability in VirtualBox allows the attackers to escalate privileges of their Snake malware by installing a kernel mode driver. This allows the malware to stay exceptionally well-hidden. (BAE Systems, 2014) Turla has also used the open-source exploitation tool Metasploit, the password stealing tool Mimikatz, as well as the group's own custom tools to perform privilege escalation (ESET, 2018c; GovCERT.ch, 2016; Symantec, 2016). The group has also used service creation for privilege escalation and DLL injection possibly for privilege escalation (Accenture, 2020; Federal Bureau of Investigation et al., 2023).

Execution: Researchers have identified Turla using many methods for code execution on compromised devices. To gain the initial execution of their malware, the group has often used social engineering, various exploits via malicious documents, Javascript added into compromised websites, or exploits delivered via watering hole websites (Bartholomew, 2017; Bitdefender, 2015b; Kaspersky Labs, 2014a). The various first stage malware used by Turla are often capable of delivering and executing additional payloads as well as executing commands received from command & control servers (Kaspersky Labs, 2018b, 2019). Some of the malware and malicious files take advantage of native programs found in Windows like wscript.exe, rundll32.exe, cmd.exe, and Powershell as well as the Linux shell to in order to execute payloads or run commands sent to them (Bartholomew, 2017; Faou, 2020a; Levene, Falcone, & Halfpop, 2017; Rascagnères, 2014).

After the initial execution phase the group has used other living off the land capabilities offered by the operating systems to execute code: Python scripts, WMI, regsvr32.exe, and PsExec (Faou, 2020; Faou & Dumont, 2019; Kaspersky Labs, 2018; Symantec, 2019). Turla has also used legitimate administrative tools that are not native to the systems to execute code or commands, such as winrs.exe and IntelliAdmin (Kaspersky Labs, 2014a; Symantec, 2019). Turla has used two techniques specifically for executing malicious DLL-files, DLL search order hijacking and DLL side loading (Faou, 2020; Federal Bureau of Investigation et al., 2023b).

Credential Access: Turla has been known to occasionally use credentials stealing during their operations, often to perform lateral movement or to gain administrator access (Federal Bureau of Investigation et al., 2023; GovCERT.ch, 2016; Symantec, 2016). The group has often relied on tools to gain credential access. The group has been known to use Mimikatz, a custom password stealing tool, an unspecified password hash dumper, and a keylogger. (G Data SecurityLabs, 2014; Kaspersky Labs, 2014a; Symantec, 2016, 2019) Turla has also taken advantage of Powershell, batch scripts, and shell scripts for credential access techniques (Guerrero-Saade, Raiu, & Rid, 2018; Symantec, 2016, 2019).

Lateral Movement: Turla has been known to perform lateral movement continually, patiently, and persistently by searching for and identifying potential systems to compromise before stealing the necessary credentials (Federal Bureau of Investigation et al., 2023; GovCERT.ch, 2016). To perform the lateral movement the group has relied heavily on stealing passwords and using built-in commands and tools like "net use" and WMI (Federal Bureau of Investigation et al., 2023; GovCERT.ch, 2016; Kaspersky Labs, 2014a). Turla has also delivered and used additional lateral movement tools, namely PsExec, winrs.exe, and IntelliAdmin

(Kaspersky Labs, 2014a; Symantec, 2019). The group has also used their own malware for lateral movement (ESET, 2017b; Faou, 2019). Many of the group's other malware allow for peer-to-peer communication, which allows infected systems to communicate with each other to enable lateral movement inside local networks, even without direct communication to the command & control servers (ESET, 2018; G Data SecurityLabs, 2014).

Collection: Turla has been known to perform various forms of data collection after compromising a victim. The malware used by Turla can list files and directories, search for files with specific file extensions, steal emails, take screenshots, take pictures using the victim's webcam, collect Wi-Fi information, and steal data from removable drives (Bitdefender, 2015b; ESET, 2018b; Faou, 2019, 2020b; Kaspersky Labs, 2018b; Levene, Falcone, & Halfpop, 2017). Turla has also used some additional tools to perform the collection and staging of files, logging keystrokes, as well as collecting data from a victim's database server (Faou, 2020a; Federal Bureau of Investigation et al., 2023; Symantec, 2016).

The group has also been identified collecting information with scripts that execute various operating system commands (Guerrero-Saade, Raiu, & Rid, 2018; Symantec, 2016). In addition to information collection with scripts or malware, the group has been identified collecting information manually (Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023). Turla has been known to stage collected data for exfiltration by using rar and tar tools to create archives of the data (Guerrero-Saade, Raiu, & Rid, 2018; Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023).

Exfiltration: During its operations Turla has been known to exfiltrate the sensitive information they have stolen (Federal Bureau of Investigation et al., 2023; Symantec, 2016). Many of the group's malware has specific capabilities to facilitate exfiltration and to make it difficult to detect (Bartholomew, 2017; ESET, 2018b; Faou, 2020b; Federal Bureau of Investigation et al., 2023; Tanase, 2015). This includes the capability to exfiltrate individual files and files from a specified directory as well as an API like function included into the group's Kazuar malware that makes it possible to request files from a compromised system (ESET, 2017b; Huss, 2017; Levene, Falcone, & Halfpop, 2017). The malware used by Turla can exfiltrate data via HTTP, SMTP, and ICMP protocols (G Data SecurityLabs, 2014; Huss, 2017). Some Turla malware can also exfiltrate stolen data by embedding data into PDF or JPG files, which are then sent via email to the group (ESET, 2018b; Faou, 2019). The group often encrypts the data that is exfiltrated or encrypts the communication between the command & control servers and their malware (Bitdefender, 2015b; Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023; Kaspersky Labs, 2014a). One malware used by Turla has been identified using the victim's browser and its cache to perform data exfiltration in a unique way (Bitdefender, 2017).

Turla has also used techniques that do not rely on the capabilities of their malware to perform exfiltration. The group has taken advantage of Dropbox, OneDrive, Box, and Gmail as services where data is exfiltrated to (Faou, 2020a, 2020b; Faou & Dumont, 2019; Symantec, 2019). Turla has used shared network drives, wget, a standalone custom tool, and the official API of a legitimate service to exfiltrate data to these legitimate services (Faou, 2020a, 2020b; Symantec, 2019). The group has also performed additional steps to make their exfiltration techniques difficult to detect, such as only exfiltrating only during specific times of the day and using proxy servers during the exfiltration (Faou, 2019; Symantec, 2016).

Objectives: The objectives for Turla's operations have been identified as the collection and stealing of sensitive information from its victims (National Cyber Security Centre UK, 2017; Vergeer, de Mik, Sahertian, van Dantzig, & Zheng Hu, 2017). Turla has been identified stealing information regarding international relations as well as other sensitive information relating to diplomatic communications (Federal Bureau of Investigation et al., 2023).

4.3.2 Turla's kill chains

Turla's kill chains were identified using the same method as with the previous sections regarding APT28 and APT29. In total the same 65 publications about Turla and its operations were examined as for the TTP section previously and from them 13 kill chains were identified. These examined publications consisted of reports, whitepapers, and articles and they were studied to identify the longest and most complete kill chains depicting Turla's operations. Because some of the reports consisted of analysis of malware capabilities instead of thorough incident reports, the identification of the kill chains required some interpretative analysis in some cases, in the same way as with the reports regarding APT28 and APT29. In the same way as with APT28 and APT29 kill chains, these interpretations made were marked with a ~~strikethrough~~ line. Additionally, a **black line** was included to demarcate the point at which the compromise of an initial device was complete, and the initial compromise phase was considered over. The 13 identified kill chains are listed in the table below (Table 3) and were marked C3-1, C3-2 etc. in no particular order. Using the same visualization method as in the earlier sections, the kill chains show the sequence of events within one realized attack, the described tendency of the group, or their capability to attack. The sequence of events is described by indicating the occurrence of a TTP by the number representing the UKC phase the TTP belongs to. The numbers and the UKC phase they represent are included in the leftmost column in the table. The sequence of events begins at the top row of each column with events unfolding down the column.

The identified kill chains had mostly similar initial steps. Most kill chains (C3-3, C3-4, C3-6, C3-7, C3-8, C3-9, C3-13) began with initial reconnaissance, resource development, delivery, and discovery. Most of the remaining kill chains (C3-1, C3-2, C3-5, C3-10, C3-11) began with resource development and delivery. The only outlier was C3-12 which started from the delivery phase followed by social engineering. The techniques used for these steps were different between the kill chains.

Within the identified kill chains, watering hole attacks were the most common initial attack path (C3-3, C3-4, C3-6, C3-7, C3-8, C3-9, C3-11, C3-13). The watering hole attacks mostly followed a similar initial kill chain pattern: some form of initial reconnaissance was performed to identify IP addresses of the targets and after the victim browsed to a compromised website, a fingerprinting script was delivered through the browser to perform initial discovery. This allowed only the desired targets to be forwarded to the malicious content, which was delivered through exploits (C3-3, C3-7, C3-9) in some cases or by various malicious installers that the victim was social engineered into running (C3-4, C3-6, C3-8, C3-13). The watering hole attack that did not fit this description (C3-11) was lacking the initial reconnaissance, but otherwise had a similar initial kill chain with a malicious Adobe Flash installer being served from a watering hole site. Half of the watering hole attacks included defense evasion before connecting to the command & control servers (C3-4, C3-6, C3-8, C3-9), in other attacks the command & control servers were connected to after execution (C3-3, C3-7) or after the initial discovery (C3-11, C3-13).

In addition to watering hole attacks, the group has used spear phishing for its initial attack path (C3-1, C3-2, C3-5) as well as two initial delivery methods that are similar to supply chain attacks (C3-10, C3-12). In the identified spear phishing attacks, the group used both malicious documents, which included an exploit that allowed for code execution (C3-1, C3-5), as well as social engineering to trick a user to open a malicious installer (C3-2) to reach execution. Two of these attacks (C3-1, C3-2) continued with Turla performing discovery and defense evasion techniques, before reaching out to the command & control server, with the C3-1 kill chain also including privilege escalation before discovery. In the remaining spear phishing kill chain (C3-5), the attackers moved from execution directly to connecting to the command & control server.

The two attacks that are similar to supply chain attacks include Turla creating malicious installers masquerading as legitimate software that were spread in an unknown way (C3-10), though the nature of the software the installers were masquerading as suggest they might have been simply shared publicly. The remaining attack (C3-12) was done by registering the command & control domain name of a commodity malware, which allowed Turla to gain control of the devices infected by the malware. In the case of the malicious installers (C3-10), the group social engineered the victim to run one of the malicious installers, leading to execution and connecting to the command & control server after persistence was gained. In the remaining kill chain (C3-12), the attack begun as an infected USB drive was delivered to a victim and the victim was social engineered to open a shortcut file from the USB drive, which led to execution. This was followed by the malware performing persistence and defense evasion techniques, before Turla registered the command & control domain name used by the malware and actually gained control.

After the initial attack phase in the phishing and watering hole attacks, the group commonly performed discovery and delivery techniques in varying orders (C3-1, C3-2, C3-5, C3-6, C3-7, C3-8, C3-9) and in some cases privilege escalation prior to performing the discovery techniques (C3-3, C3-4). In the remaining kill chains (C3-10, C3-11, C3-12, C3-13), Turla performed delivery, social engineering, persistence, and execution in varying orders before discovery techniques were performed. Notably, discovery techniques were identified in every kill chain after the connection to command & control servers.

Some kill chains finished in a straightforward manner after these steps. The previous steps were followed up by credential access, which led to lateral movement, collection, and exfiltration, before finally delivering an additional payload as the final step (C3-1, C3-2). For some kill chains an additional and final payload was delivered after the lateral movement, but before the final steps of collection and exfiltration were performed (C3-5, C3-6, C3-7).

In most of the remaining kill chains, additional defense evasion and command & control connection was performed after the discovery step (C3-3, C3-4, C3-13), in some cases also including persistence techniques (C3-8, C3-9). Two of these kill chains then finished similarly to the earlier kill chains, credential access was performed, which led to lateral movement, and the final steps of collection and exfiltration (C3-8, C3-9). For one kill chain (C3-13), collection was only preceded by execution. The other kill chains (C3-3, C3-4) required an additional delivery before performing the similar finishing steps, credential access into lateral movement, followed up by collection, exfiltration, and the final step of delivery of a final payload.

The remaining kill chains (C3-10, C3-11, C3-12) progressed from the discovery step with connection to command & control servers and delivery, in varying order. This was followed with execution, which finished one kill chain (C3-11), collection and execution followed by exfiltration to finish another kill chain (C3-12), and the final kill chain included execution followed by another connection to command & control servers before collection (C3-10).

TABLE 3 Identified Turla kill chains[3]

		C3-1	C3-2	C3-3	C3-4	C3-5	C3-6	C3-7	C3-8	C3-9	C3-10	C3-11	C3-12	C3-13
1	Reconnaissance	2	2	1	1	2	~~1~~	~~1~~	1	1	2	2	3	~~1~~
2	Resource Develop.	3	3	2	2	3	2	2	2	2	~~3~~	3	4	2
3	Delivery	5	4	3	3	4	3	3	3	3	4	10	12	3
4	Social Engineering	4	12	10	10	5	10	10	10	10	12	8	6	10
5	Exploitation	12	10	5	4	12	3	5	3	5	6	4	7	8
6	Persistence	11	7	3	3	~~8~~	4	3	4	12	8	3	2	4
7	Defense Evasion	10	8	12	12	3	12	12	12	7	12	12	8	12
8	Command & Control	7	10	8	7	10	7	~~8~~	7	8	3	6	3	3
9	Pivoting	8	~~3~~	11	8	13	~~8~~	3	8	10	6	3	12	10
10	Discovery	10	~~13~~	10	11	14	3	10	10	3	10	12	10	7
11	Privilege Escalation	~~3~~	14	7	10	3	10	13	3	6	3	10	8	8
12	Execution	~~13~~	15	8	7	15	13	14	6	7	8	8	3	~~3~~
13	Credential Access	14	~~16~~	10	8	16	14	3	7	8	12	~~3~~	12	~~12~~
14	Lateral Movement	15	3	~~3~~	10		3	15	8	13	8	~~12~~	15	~~15~~
15	Collection	~~16~~		~~13~~	~~3~~		15	16	13	14	~~15~~		16	
16	Exfiltration	3		14	~~13~~		16		14	15				
17	Impact			15	14				15	16				
18	Objectives			~~16~~	15				16					
				3	~~16~~									
					3									

[3] References: **C3-1**: Kaspersky Labs, 2014a, **C3-2**: Kaspersky Labs, 2014a, **C3-3**: Kaspersky Labs, 2014a, **C3-4**: Kaspersky Labs, 2014a, **C3-5**: Symantec, 2016, **C3-6**: Symantec, 2016, **C3-7:** Symantec, 2016, **C3-8**: GovCERT.ch, 2016, **C3-9**: GovCERT.ch, 2016, **C3-10**: Kaspersky Labs, 2019, **C3-11**: Faou, 2020c, **C3-12**: Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023, **C3-13**: Boutin, 2017

5 ANALYSIS

The TTPs identified from the reports and the identified kill chains will be used to compare the APT groups in this section. The relationships, themes, patterns, differences, and similarities between the groups identified from the analysis will be the basis that is used to answer the research questions. The analysis will focus on comparing the identified TTPs and kill chains.

5.1 TTP analysis

5.1.1 Reconnaissance

Only a few different reconnaissance techniques were identified overall, possibly because reconnaissance, especially before an attack has taken place, is difficult to identify. The reconnaissance techniques that were identified between all the groups were mostly similar. APT28 and APT29 both have been identified scanning for vulnerabilities in systems they are planning to target while Turla has been identified scanning for devices compromised by another APT group (National Cyber Security Centre UK, 2020; National Security Agency & National Cyber Security Centre UK, 2019; Trend Micro, 2020). APT29 has also been identified using tracking links to perform reconnaissance and Turla has been identified using a spear phishing document simply for reconnaissance, which are somewhat similar techniques (Barnett, 2021; Couchard & Arquillière, 2022).

5.1.2 Resource Development

Resource development techniques were often not specified in reports as it is not easy to identify steps the groups have taken prior to an attack, but every group was found to have performed some resource development. Even if the techniques are not visible to researchers or defenders, these techniques are required to create the malware, phishing emails, and malicious sites that are used by the groups.

The resource development techniques that were identified were mostly common between the groups. Each of the groups has been found to have set up domain names, in some cases specific typosquat domain names (Couchard & Arquillière, 2022; FireEye, 2014; Recorded Future, 2022). All groups have also been known to create phishing documents and various malware (Bitdefender, 2015b; ESET, 2016; FireEye, 2017; F-Secure, 2015a; Kharouni et al., 2014). APT28 and Turla have also been known to set up malicious watering hole websites (ESET, 2014a; Faou, 2020c; FireEye, 2017; Kaspersky Labs, 2014a).

5.1.3 Delivery

Some more variance was found in delivery techniques. All groups used some common delivery methods, but the use of email was clearly the most common initial delivery technique as it was used multiple times by all groups (Adair, 2016; ESET, 2016; Symantec, 2016). After an initial delivery all groups have also used their first stage malware or the access, they have gained to deliver additional malware or tools to the victim environment (ESET, 2018a; Faou, Tartare, & Dupuy, 2019; Kaspersky Labs, 2014a). In addition to email and first stage malware delivery, APT28 and Turla have used watering holes and infected USB-drives for the initial delivery of malware or other malicious objects (Calvert, 2014; Faou, 2020; FireEye, 2017; Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023). Turla and APT28 have also both used certutil.exe to deliver their tools or malware to compromised devices (Lee & Falcone, 2018; Symantec, 2019). Some similarity can also be seen with APT28 and APT29, both have used stolen credentials and password spraying as initial access methods (Jenkins, Sarah, Parnian, & Bienstock, 2021; Mandiant, 2022; Microsoft Threat Intelligence Center, 2020; Mueller, 2019).

Uniquely among the groups APT29 has used supply chain attacks as a delivery method multiple times (F-Secure, 2015a; Lehtiö, 2014; Ramakrishna, 2021). Though Turla and APT28 have also been identified using legitimate software that has been infected with their malware. It is however not clear if the malicious software was delivered to a victim in a way to fit the supply chain attack method or if it was delivered by another method (ESET, 2016; Kaspersky Labs, 2019; Symantec, 2016). Turla has also been known to use some unique delivery methods, the group has taken over the infrastructure of another APT group and used it to gain access to their victims and in another attack registered an expired command & control domain name of a commodity malware to take control of victims of the malware (Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023; National Security Agency & National Cyber Security Centre UK, 2019)

5.1.4 Social Engineering

Social engineering techniques were reported among all groups, as the groups used various social engineering techniques in many attacks and in very similar ways. The groups all used social engineering techniques to trick their victims into opening malicious documents, links, emails, or as a decoy after a malicious file has been opened or delivered (Faou, 2020c; F-Secure, 2015a; Hirvonen, 2014; Huss, 2017; Kharouni et al., 2014). Turla also used social engineering to trick victims into downloading and running a malicious installer that was masquerading as legitimate software (Kaspersky Labs, 2014a).

5.1.5 Exploitation

Exploitation techniques varied noticeably between the groups, with APT28 being identified using the most exploits, followed by APT29, and Turla having been connected to only a few exploits. APT28 has been connected to the exploitation of many zero-day vulnerabilities, using as many as six in one year alone (ESET, 2016). The use of exploits with various malicious documents is the most common way of exploitation among the groups. All groups have used various vulnerabilities with Adobe and Word documents to achieve code execution. (ESET, 2014a, 2016; F-Secure, 2015a; Jiang et al., 2017; Kaspersky Labs, 2014a) All of the groups have also exploited various Windows vulnerabilities to perform privilege escalation (ESET, 2016, 2022; Kaspersky Labs, 2014a).

Some overlap can also be identified between individual groups. APT28 and Turla were both identified using two similar zero-day vulnerabilities with malicious Microsoft Office documents (Jiang et al., 2017). The groups have also used watering hole attacks in similar types of attacks with malicious websites exploiting browser or other web-based vulnerabilities to achieve their initial compromise. However, the specific vulnerabilities the groups have used were different. (ESET, 2016; FireEye, 2017; Kaspersky Labs, 2014a) APT28 and Turla have both also used different vulnerabilities to avoid operating system defense features (BAE Systems, 2014; Ilascu, 2018).

APT28 and APT29 have also shown some similarities in exploitation. The groups have exploited the same Microsoft Word code execution vulnerability by using malicious documents and exploited the same Microsoft Exchange vulnerability (Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; ESET, 2014a, 2014b; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021). One overlap was also identified between Turla and APT29, both have used the same privilege escalation vulnerability in Windows operating systems (F-Secure, 2015a; Symantec, 2016).

As APT28 exploited the most vulnerabilities, the group also has exploited some unique vulnerabilities. The group was the only one to exploit a Firefox vulnerability, as well as a Java privilege escalation vulnerability, and a UEFI vulnerability (ESET, 2016; Hacquebord, 2017; Ilascu, 2018).

Other unique findings among the groups were found from APT29, the only group to have exploited a vulnerability in Apple iPhones. The group used a malicious website that hosted an exploit to a vulnerability in iPhones (Microsoft Threat Intelligence Center, 2021b). Additionally, APT29 exploited a wide selection of network devices and network software mostly unique among the group, with Microsoft Exchange exploitation being in common with APT28 (Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; National Cyber Security Centre UK, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Security Agency, 2021).

5.1.6 Persistence

The use of persistence techniques was mostly similar between the groups, still some variance could be identified. All groups employed some similar persistence techniques like abusing start up folders, making registry modifications, creating or modifying services, and creating scheduled tasks (ESET, 2016; Hacquebord & Remorin, 2020; Hirvonen, 2014; Huss, 2017; Levene, Falcone, & Halfpop, 2017; Microsoft Threat Intelligence Center, 2021d; Raiu, Soumenkov, Baumgartner, & Kamluk, 2013; Unterbrink, 2021). However, not all persistence techniques were found among all the groups. For example, APT29 and Turla both have used WMI and account creation for persistence, while APT28 has not (Crowdstrike, 2022c; Faou, 2020a; Faou & Dumont, 2019; Faou, Tartare, & Dupuy, 2019). APT28 and Turla share the use of rootkits for persistence, while APT29 has not been identified using them (BAE Systems, 2014; ESET, 2016; Ilascu, 2018).

5.1.7 Defense evasion

Defense evasion techniques showed some notable differences between the groups. All the groups used some common defense evasion techniques, such as checking for antivirus products, using code obfuscation, encrypted or encoded payloads, encrypted or encoded communication, and using legitimate seeming names for their tools or files to blend into the compromised environment (Baumgartner & Raiu, 2015; Crowdstrike, 2022; ESET, 2014, 2016; Faou, 2020; Faou & Dumont, 2019; Federal Bureau of Investigation et al., 2023; FireEye, 2014; Lee & Falcone, 2018; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021; Raiu, Soumenkov, Baumgartner, & Kamluk, 2013; Symantec, 2017; Telsy, 2020). Additional similarity can be seen in the use of legitimate online services, such as Twitter, Dropbox, Google Drive, or Instagram to act as a command & control server, or a proxy to the command & control servers. It should however be noted that APT29 was identified using this technique as early as 2011, has used this technique often, and has been identified using multiple different services while APT28 and Turla have only been identified using the technique in individual cases. (Boutin, 2017; FireEye, 2015b; Hacquebord & Remorin, 2020; Harbison & Renals, 2022)

Beyond these similarities, APT29 stands out from the other groups as APT29 has a very wide range of techniques they have used for defense evasion that neither APT28 nor Turla have been identified using. For example: using IP addresses and hostnames that match the victim network, disabling security software, using domain generation algorithms (DGA), using domain fronting, using

HTML smuggling, using unique folder and file names for each compromise, and using multiple user accounts for different stages of a compromise (Dunwoody, 2017b; FireEye, 2020; Mandiant, 2022b; Microsoft Threat Intelligence Center, 2020b, 2021c; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022).

Despite APT29 having used many unique defense evasion techniques, some overlap can be seen. APT29 and Turla have both have signed some of the malicious files the groups have used (Faou, Tartare, & Dupuy, 2019; Kaspersky Labs, 2014a). APT29 and Turla have both also used a technique called "timestomping" to falsify or obfuscate timestamps that have been created and steganography to obfuscate the communications between their malware and their command & control servers (Faou, 2019; Faou & Dumont, 2019; FireEye, 2015b; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). Turla also has used some unique techniques: they have used their Snake rootkit to hide files and to capture network traffic, as well as operating some of their malware only during local office hours (BAE Systems, 2014; Faou, 2020a; Faou & Dumont, 2019).

APT28 and Turla also have some technique overlap, both groups have employed process injection techniques to allow their malware to connect to the command & control server through browsers used by the victim. Both groups have also exploited vulnerabilities to avoid defense features (BAE Systems, 2014; ESET, 2016; Ilascu, 2018). APT28 and APT29 also share two techniques, both groups have been known to disable logging and clear logs to avoid detection (Mandiant, 2022b; Mehta, Leonard, & Huntley, 2014; Mueller, 2018).

5.1.8 Command & control

All the groups use some similar command & control communication techniques. Each group has been known to often use the HTTP protocol for communications between their malware and the command & control servers, often encrypting or encoding their communications (ESET, 2014b; Faou, 2020a; Lee, Harbison, & Falcone, 2018). The groups have all also been identified using systems that have likely been compromised, as well as legitimate services like Google Drive, Instagram, Dropbox, and Twitter as their command & control servers or proxies to their command & control servers (Boutin, 2017; Crowdstrike, 2022c; FireEye, 2015b; Hacquebord & Remorin, 2020; Levene, Falcone, & Halfpop, 2017; SecurityScorecard, 2022). All three groups also have the capability for communicating to their command & control servers by using the FTP protocol (F-Secure, 2015a; Hacquebord & Mercês, 2015; Levene, Falcone, & Halfpop, 2017). APT28 and Turla both have capabilities for communicating with the SMTP protocol which APT29 has not shown to have (ESET, 2016; G Data SecurityLabs, 2014). APT29 and Turla both have the capability to use DNS for their command & control communication and have used named pipes to forward communication inside local networks (Accenture, 2020; ESET, 2017b; Faou, Tartare, & Dupuy, 2019; Federal Bureau of Investigation et al., 2023; PwC, 2020).

Some unique aspects can be identified between the groups. APT28, for example, has their Xtunnel malware specifically designed to act as a tunnel between the command & control server (ESET, 2016). The group also has the capability to communicate over the POP3 protocol (Anthe et al., 2015). Uniquely APT29's CosmicDuke malware has the capability to use the WebDav protocol for its command & control communication and the group has also used TOR for their command & control communication (Dunwoody, 2017b; F-Secure, 2015a). Turla has the widest selection of network protocols that the group has used for its command & control communication. For Turla's Snake malware they have built their own communication method that can be transferred over TCP, UDP, and ICMP as well as more common protocols used by other groups, HTTP, DNS, and SMTP (Federal Bureau of Investigation et al., 2023). Turla is also unique in their use of satellite communications for command & control and multiple Turla malware have the capability to communicate between each other in a peer-to-peer manner to reach the command & control server (Accenture, 2020; ESET, 2017b; Federal Bureau of Investigation et al., 2023; Tanase, 2015).

5.1.9 Pivoting

Not many different pivoting techniques were identified among the groups, though all groups were found to have used some. APT28 has been identified using Xtunnel for pivoting on multiple occasions (Guarnieri, 2015; Mueller, 2019; Secureworks, 2017). APT29 has used pivoting techniques that do not rely on its own malware: the group has been identified using SSH tunneling on a compromised device and cobalt strike beacons for pivoting purposes (Barnett, 2021; Crowdstrike, 2022c). Turla on the other hand has not been identified using any specific pivoting techniques, though the group has been known to perform pivoting via some unspecified methods (GovCERT.ch, 2016; Guerrero-Saade, Raiu, & Rid, 2018; Kaspersky Labs, 2014a).

The groups all had some pivoting capabilities built into their malware. The main purpose of APT28's Xtunnel is to allow for pivoting (ESET, 2016). Multiple Turla malware also have the capability for tunnelling command & control traffic through them to allow for pivoting (Accenture, 2020; ESET, 2017b; Federal Bureau of Investigation et al., 2023). APT29's FatDuke and MiniDuke malware have some pivoting features (Faou, Tartare, & Dupuy, 2019).

5.1.10 Discovery

All groups have performed various discovery techniques and certain overlap is found. Often the discovery techniques identified from the groups were performed using each group's own malware. The groups all have malware that can perform discovery through built-in commands or specific features (Bitdefender, 2015b; ESET, 2016; Tivadar, BALÁZS, & Istrate, 2013). Some overlap can be identified as APT28 and Turla malware also perform discovery through invoking operating system commands with cmd.exe, which was not identified from APT29 (Bartholomew, 2017; ESET, 2018a). Another similarity between APT28 and Turla can be seen, both groups have used malicious Javascript embedded into websites multiple times to perform discovery (Anthe et al., 2015; Boutin, 2017; ESET, 2014a; Faou, 2020c).

More similarities can be identified between Turla and APT29: both groups have used living off the land methods to perform discovery, though APT29 has often specifically used Powershell commands which Turla has not used for discovery purposes (Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; Crowdstrike, 2022c). Turla has instead often used native operating system commands and tools for discovery, which APT29 has also done (Crowdstrike, 2022c; Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023; Kaspersky Labs, 2014a).

Both APT29 and Turla have also been known to use a variety of additional tools to perform discovery, though there is no overlap on the actual tools used. APT29 has been identified using AdFind, BloodHound, SharpView and Cobalt strike for discovery purposes (ANSSI, 2021; ESET, 2022). Turla on the other hand has used tools like ShareEnum as well as some unknown custom tools for discovery (GovCERT.ch, 2016; Symantec, 2016). Turla has been known to also use batch scripts and VBScript scripts that contain operating system commands to perform discovery (GovCERT.ch, 2016; Kaspersky Labs, 2014b; Symantec, 2016).

5.1.11 Privilege escalation

Privilege escalation techniques showed some differences between the groups. Clear similarities between all the groups were limited to all groups using Mimikatz to steal privileged credentials as well as other methods for stealing privileged credentials (Anthe et al., 2015; GovCERT.ch, 2016; Microsoft 365 Defender Team, 2020). A less specific similarity was also identified between the groups as each group also used their own, though unspecified, tools specifically for privilege escalation (Benchea, Vatamanu, Maximciuc, & Luncaşu, 2015; ESET, 2022; Symantec, 2016). Another similarity was that each group also exploited various vulnerabilities for privilege escalation, however only one vulnerability was found that was common between Turla and APT29 (F-Secure, 2015a; Symantec, 2016).

Unique privilege escalation techniques from APT28 were the use of Responder to steal privileged credentials, DLL search order hijacking, process injection, malicious document which had a privilege escalation exploit built-in, a Java privilege escalation vulnerability, and the creation of new privileged accounts (ESET, 2016; Hacquebord, 2017; Kaspersky Labs, 2018a; Lee, Harbison, & Falcone, 2018; Smith & Read, 2017; Suiche, 2017).

APT29 could be identified using some unique living off the land techniques that use built-in features and tools. These include abusing shortcut modification, path interception by search order hijacking, exploiting the "sticky keys" feature, dumping LSASS process memory by using the task manager to steal credentials, and forging tokens with a stolen certificate (Dunwoody, 2017b; Jenkins, Sarah, Parnian, & Bienstock, 2021; Mandiant, 2022b). One of these living off the land techniques used by APT29 was also in common with APT28: both groups achieved privilege escalation by creating scheduled task (ESET, 2019; Jenkins, Sarah, Parnian, & Bienstock, 2021).

Turla was the group with least privilege escalation techniques identified. The group did, however, have some unique aspects: the group used the Metasploit tool and service creation for privilege escalation (Accenture, 2020; ESET, 2018c).

5.1.12 Execution

All groups performed some similar execution techniques to achieve their initial code execution. The use of malicious documents with exploits or social engineering techniques were common among all of the groups (Bitdefender, 2015b; Falcone, 2018; Harbison & Renals, 2022; Kaspersky Labs, 2014a; Lee & Falcone, 2016; Raiu, Soumenkov, Baumgartner, & Kamluk, 2013). The groups have also similarly used their malware to execute additional payloads or commands sent from command & control server, often the malware execute these with built-in programs like rundll32.exe or cmd.exe (ESET, 2019; Faou, Tartare, & Dupuy, 2019; Shevchenko, 2008; Trend Micro, 2015; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). Similarly, the groups have all used malicious Powershell commands, specifically by embedding Powershell into shortcut files in order to perform the initial code execution, as well as through other ways to perform additional code execution after a compromise (Dunwoody, 2017a; Dunwoody et al., 2018; Falcone, 2018; Faou, 2020a; Hacquebord & Remorin, 2020; Kaspersky Labs, 2018b). Interestingly, APT28 and Turla have been identified using almost identical Powershell code in these shortcut files (Kaspersky Labs, 2018b). Similarity can also be seen in the use of additional tools to perform code execution on remote machines. The tools however do not match between the groups: APT28 has used Winexe and Remcom, APT29 has used Sharp-SMBExec while Turla has used Winrs.exe and IntelliAdmin (Anthe et al., 2015; ESET, 2022; Kaspersky Labs, 2014a; Secureworks, 2017; Symantec, 2019).

Beyond these similarities in tactics and techniques by all groups, some additional similarities can also be seen between individual groups. Turla and APT28 have both used regsvr32.exe to get their malicious code to run (ESET, 2018b, 2019). Both groups have also used malicious Javascript and exploits embedded into websites to perform some code execution (Anthe et al., 2015; Kaspersky Labs, 2014a).

APT29 and Turla have both used PsExec and WMI to execute commands at later stages of a compromise and wscript.exe to run malicious scripts or code (Bartholomew, 2017; Crowdstrike, 2022c; Faou, Tartare, & Dupuy, 2019; GovCERT.ch, 2016). APT29 and Turla have both also used DLL side loading and DLL search order hijacking techniques to execute their malicious DLLs (Faou, 2020b; Federal Bureau of Investigation et al., 2023; Harbison & Renals, 2022; Nafisi, 2021).

APT29 has the most unique execution techniques among the groups. These are mostly various living off the land techniques that the group has used after the initial execution phase. These include using SMB tools, remote WMI, local and remote task creation, and a built-in "Run command" feature in Azure (Jenkins, Sarah, Parnian, & Bienstock, 2021; Nafisi, 2021). The Solarwinds compromise also included two unique code execution methods by APT29. The group inserted their code into legitimate parts of the Solarwinds product, which loaded the malicious code along with the legitimate code (Microsoft Threat Intelligence Center, 2020b). Another unique method was the creation of an "Image File Execution Options Debugger" value for dllhost.exe, which was executed occasionally during normal operations, which caused APT29's malicious code to run (Microsoft Threat Intelligence Center, 2021c).

Turla also has unique code execution techniques, as the group has used the Linux shell and Python interpreter to execute commands through their malware (Baumgartner & Raiu, 2014; Faou, 2020c).

5.1.13 Credential Access

Techniques and methods used for credential access had only limited similarities between the groups. All groups have used various keyloggers to steal passwords and the Mimikatz tool to steal various passwords or password hashes (Anthe et al., 2015; Crowdstrike, 2022c; ESET, 2014a; GovCERT.ch, 2016; Hirvonen, 2014). Beyond these, only similarities between individual groups can be identified. Malware used by both APT28 and APT29 have been used to steal passwords and cookies. Both groups have also used Responder, tried to bruteforce accounts, added or modified accounts, and used various living off the land methods to gain password hashes from the LSASS process. (Bitdefender, 2015a; Crowdstrike, 2022c; F-Secure, 2015a; Jazi & Santos, 2022; Jenkins, Sarah, Parnian, & Bienstock, 2021; Microsoft, 2020; Microsoft Security Response Center, 2021; Microsoft Threat Intelligence Center, 2021d; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021; Smith & Read, 2017; Trend Micro, 2020) Both APT28 and APT29 have also been identified stealing information from internal repositories, though only APT28 has been known to steal passwords specifically (Crowdstrike, 2022c; Suiche, 2017). Only one similarity can be identified between Turla and another group: both Turla and APT29 have used some unspecified custom password stealing tools (Mandiant, 2022b; Symantec, 2016).

Beyond these techniques, APT29 has used multiple techniques unique among the groups. These include kerberoasting, forging tokens, precomputing cookies, and stealing passwords from email boxes or directly from the filesystem of a compromised device (Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; Microsoft, 2020; Microsoft Threat Intelligence Center, 2021c; National Cyber Security Centre UK, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Security Agency, 2021; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). APT29 has used some unique tools for credential access. The group has used a tool called DSInternals and the group's own custom tools, one for stealing credentials from Solarwinds Orion databases and another tool for stealing ADFS certificates (Crowdstrike, 2022c; Mandiant, 2022b; Symantec, 2021b). In one instance, APT29 has been suspected of purchasing stolen credentials from a third party (Jenkins, Sarah, Parnian, & Bienstock, 2021).

Unique technique could also be identified from APT28 as the group has been phishing specifically for credential access (Trend Micro, 2020). Turla on the other hand has been unique in using Powershell, batch scripts, and shell scripts for credential access (Guerrero-Saade, Raiu, & Rid, 2018; Symantec, 2016, 2019).

5.1.14 Lateral Movement

Lateral movement methods used by the groups are mostly similar. All groups have been known to use stolen credentials to allow them to move laterally (Anthe et al., 2015; Crowdstrike, 2022c; GovCERT.ch, 2016). However, APT29 has been noted as using a unique technique of employing multiple sets of stolen credentials for different stages or purposes during a compromise (Crowdstrike, 2022c). The groups have also all used some living off the land methods for lateral movement. For APT28 this means adding new accounts as well as using the Windows native command "net use" to map network shares, the latter of which is a technique that is in common with Turla (GovCERT.ch, 2016; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021; Suiche, 2017). APT29 and Turla also have one common living off the land lateral movement technique, the use of WMI (GovCERT.ch, 2016; Microsoft Threat Intelligence Center, 2021c). In addition to these techniques, APT29 has used many other living off the land techniques that are unique among the groups. APT29 has been known to use SSH tunneling, remote scheduled task creation, RDP tools, SMB tools, and the creation of new certificates for lateral movement (Crowdstrike, 2022c; Jenkins, Sarah, Parnian, & Bienstock, 2021; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022).

In addition to living off the land methods, all groups have some lateral movement features in their own malware. These features differ between the groups. For example, APT28's Xtunnel is an independent proxy tool, which creates a tunnel between infected machines to allow for easier lateral movement, a similar feature is also included in APT29's FatDuke (ESET, 2016; Faou, Tartare, & Dupuy, 2019). For Turla, many of their malware have peer-to-peer functionality, which allows infected instances to communicate with each other allowing for further lateral movement (ESET, 2017b; Federal Bureau of Investigation et al., 2023). The groups also have in common the use of various tools that are used for lateral movement. However, the used tools themselves mostly differ. APT29 has used PsExec, Mimikatz and SMB beacon from Cobalt Strike for lateral movement (Crowdstrike, 2020; Faou, Tartare, & Dupuy, 2019; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022). Turla has also used PsExec for lateral movement, similar to APT29, and the legitimate remote execution tools winrs.exe and IntelliAdmin (Kaspersky Labs, 2014a; Symantec, 2019). APT28 has used legitimate remote execution tools Winexe and Remcom, as well as the password stealing tool

Mimikatz, the latter of which is a tool also used by APT29 in terms of lateral movement (Anthe et al., 2015; Guarnieri, 2015; Secureworks, 2017).

A unique technique among the groups was identified from APT28 as they have used an exploit for lateral movement (Smith & Read, 2017).

5.1.15 Collection

The techniques for data collection are largely similar across the groups. The malware used by all of the groups have features that support various ways of collecting data. The malware mostly has overlapping collection features, such as the ability to list directory contents, take screenshots, search for files with specific file extensions, and collect files from removable drives (Calvert, 2014; ESET, 2016; Faou, 2020; FireEye, 2014; F-Secure, 2015a; Hirvonen, 2014; Kaspersky Labs, 2015; Levene, Falcone, & Halfpop, 2017). There are, however, some differences to be seen in the features. APT28 and APT29 have capabilities for logging keystrokes, automatically searching for files with specific filenames, as well as stealing browser data in their malware (Calvert, 2014; Hirvonen, 2014; Jazi & Santos, 2022). Turla and APT29 malware both have the capability to steal Wi-Fi passwords (Hirvonen, 2014; Kaspersky Labs, 2018). Malware used by Turla has unique capabilities specifically for stealing emails and taking pictures with the webcam of an infected device (ESET, 2018b; Faou, 2019; Levene, Falcone, & Halfpop, 2017). ATP29 has a custom malware designed to steal a specific type of ADFS token signing certificates (Mandiant, 2022b).

More similarity can be seen, as the groups use a common technique of creating archived files to stage the collected information for exfiltration. Interestingly, the groups seem to prefer different tools for this purpose. APT28 has been known to use WinRAR, APT29 has used 7-Zip, and Turla has used rar as well as tar tools (Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; Guerrero-Saade, Raiu, & Rid, 2018; Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021).

All of the groups are also known for performing some manual data collection, though the techniques between the groups differ somewhat. APT28 and APT29 share the technique of manual data collection from shared network drives, internal information repositories, and email inboxes of their victims (Bienstock, 2022; Crowdstrike, 2022c; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021; Suiche, 2017). Uniquely, APT29 has also collected data from cloud storage and code repositories (Mandiant, 2022b).

All the groups have used some living off the land methods for collection purposes. APT28 and Turla have executed operating system commands with the use of scripts to perform various data collection tasks (Guarnieri, 2015; Symantec, 2016). Turla has also been known to run some of the same commands manually (Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023). APT29 has used Powershell, browser features, as well as operating system tools like ntdsutil and

Procdump to perform data collection on its victims (Crowdstrike, 2022c; Jenkins, Sarah, Parnian, & Bienstock, 2021).

Uniquely, Turla has also used multiple standalone custom tools to perform collection. As Turla's malware does not have capabilities to log keystrokes the group has relied on separate tools for that purpose (Federal Bureau of Investigation et al., 2023). Additionally, the group has used a separate custom tool to steal data from a victims database (Faou, 2020a).

5.1.16 Exfiltration

The exfiltration techniques used were largely similar between the groups. All of the groups have malware with capabilities for exfiltrating individual files as well as multiple files (Calvert, 2014; ESET, 2016; Huss, 2017; Levene, Falcone, & Wartell, 2015; Tivadar, BALÁZS, & Istrate, 2013). The different malware from the groups have the use of the HTTP protocol for exfiltration in common (F-Secure, 2015; Hacquebord & Mercês, 2015; Huss, 2017). In addition to the HTTP exfiltration capabilities, APT28 malware have the capability to exfiltrate via the IMAP protocol, APT29 malware have the capabilities to use FTP and WebDav protocols, and Turla malware can use TCP, UDP, ICMP, and DNS protocols, as well as named pipes for exfiltration (Federal Bureau of Investigation et al., 2023; F-Secure, 2015a; G Data SecurityLabs, 2014; Jazi & Santos, 2022). Each group also has malware which include some method of encrypting the stolen data or the exfiltration traffic (Bitdefender, 2015b; ESET, 2018; Hirvonen, 2014).

Individual groups also have some exfiltration techniques in common. Both APT28 and Turla have used emails as an exfiltration method and both groups have taken advantage of a victim's email server to send the exfiltrated data onward (ESET, 2018b; Faou, 2019; FireEye, 2014). Both groups have also used proxy servers for data exfiltration (Mueller, 2019; Symantec, 2016). APT29 and Turla have both used shared network drives and existing APIs offered by legitimate services to exfiltrate data out (Faou, 2020a, 2020b; Microsoft 365 Defender Team, 2020; Microsoft Threat Intelligence Center, 2021c). APT28 and APT29 also use some similar exfiltration techniques. Both groups have staged stolen data on a victim's internet facing email server, where it has been exfiltrated from with simple web requests. Both groups have also used innocuous file names and extensions for data that has been prepared for exfiltration, most likely as a way to avoid detection. (Cash, Meltzer, Koessel, Adair, & Lancaster, 2020; Microsoft Threat Intelligence Center, 2021; National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK, 2021)

More similarities can be identified in the use of legitimate services to assist in exfiltration: the groups have all used various legitimate services as a place to exfiltrate their data to. However, the services used are not similar between the groups. APT29 and Turla have both used OneDrive while APT28 has used Google Drive to exfiltrate their data to (Faou, 2020a; Hacquebord & Remorin, 2020; Microsoft Threat Intelligence Center, 2021c). Turla has also used Dropbox,

Box, and Gmail email boxes for data exfiltration (Faou, 2020a, 2020b; Symantec, 2019). APT29 on the other hand has uniquely taken advantage of services like Trello, Notion, Firebase, and Twitter (Raiu, Soumenkov, Baumgartner, & Kamluk, 2013; Recorded Future, 2023).

Some unique methods can also be identified. Turla has used various exfiltration methods to avoid detection. The group has done automatic exfiltration at specific times of day to avoid attention and has used steganography to hide exfiltrated data into files (Faou, 2019). Turla has also used a unique method of storing data into browsers local cache before its exfiltrated by the browser (Bitdefender, 2017).

5.1.17 Impact

No clear similarity can be seen in the use of impact techniques among the groups. APT28 is the only group that has been identified performing overt impact techniques, such as denial-of-service, defacement, and sabotage attacks (FireEye, 2017; Suiche, 2017). APT29 was also identified using one impact technique; however, it was more covert and designed to stay hidden, as the group inserted malicious code into their victim's systems (Microsoft Threat Intelligence Center, 2020b). Turla was not identified performing any impact techniques.

5.1.18 Objectives

The objectives identified for each group were mostly similar. All of the groups have the stealing of sensitive information as their most common objective (ESET, 2018a; National Cyber Security Centre UK, 2017; Polish Military Counterintelligence Service & CERT-PL, 2023). All groups have been identified attempting to steal broadly similar information, they all target similar targets and appear to be mainly interested in politically relevant and sensitive information (Federal Bureau of Investigation et al., 2023; FireEye, 2017; Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022).

Uniquely among the groups, APT28 has been known to purposefully leak some of the information stolen by the group to achieve their strategic goals (FireEye, 2017). Another unique aspect from APT28 is them performing some sabotage-type operations where the objective has been to destroy data, possibly also to cause alarm in the victims (FireEye, 2017; Suiche, 2017). In one instance, APT28 has also been suspected of attempting to assist the Russian military with the help of their malware (Meyers, 2016).

5.2 Kill chain analysis

The kill chains that were identified are broadly similar across the groups. Most kill chains begin with similar steps, include similar TTPs, progress in broadly similar ways, and end in similar ways. However, some overarching themes and notable findings can be identified from the whole kill chains as well as some specific parts of the kill chains. When analysing the kill chains as a whole, several findings and themes could be seen. For example, APT28 kill chains are slightly shorter than APT29 and Turla kill chains. APT29 kill chains appear to have more variance in which TTPs were used and in which order, as well as including more occurrences of defense evasion techniques than in APT28 and Turla kill chains. Additionally, in Turla kill chains more discovery steps can be identified than in APT28 and APT29 kill chains. Most identified kill chains from all groups end with collection and exfiltration, however in only one kill chain from the ones that were studied was the objective of the attack identified.

5.2.1 Initial attack paths

Many of the attacks identified had similar initial attack paths. The most common initial attack path was spear phishing using malicious documents with the second most common initial attack path being various watering hole attacks. APT28's identified initial attack paths can be divided into three categories: spear phishing to deliver malicious documents (C1-1, C1-2, C1-4, C1-6, C1-7, C1-10, C1-11, C1-13), spear phishing to direct victims into a watering hole site (C1-8, C1-12), and spear phishing for credentials (C1-9) with the remaining two kill chains having an unknown delivery method (C1-3, C1-5). For APT29, the initial attack paths consisted of almost entirely of spear phishing to deliver malicious documents in various ways (C2-1, C2-2, C2-3, C2-4, C2-5, C2-7, C2-8, C2-9, C2-10, C2-11, C2-12, C2-13) with supply chain attack being identified in one kill chain (C2-6). Turla on the other hand, used watering hole attacks (C3-3, C3-4, C3-6, C3-7, C3-8, C3-9, C3-11, C3-13), spear phishing to deliver malicious documents (C3-1, C3-2, C3-5), and initial attack methods similar to supply chain attacks (C3-10, C3-12) as initial attack paths.

5.2.2 Compromise phase

The beginning of the initial compromise phase is mostly similar for each group, besides some individual kill chains. Each group has been known to perform some initial reconnaissance, though Turla has been identified using reconnaissance in more kill chains than the other groups. Notably for Turla kill chains, reconnaissance was only found in the group's watering hole attacks: in these watering hole attacks unknown reconnaissance methods were used to identify ranges of IP addresses which they considered interesting. Almost all remaining kill chains begin with resource development followed by delivery. In the cases where reconnaissance steps were found, the following steps were resource development and delivery. All APT28 kill chains and almost all APT29 kill chains include social engineering after the initial delivery step, while in Turla kill chains the delivery phase is often followed by discovery, though in some Turla kill chains social engineering can also be seen. The only outlier to the trend of kill chains beginning with reconnaissance or resource development was Turla's C3-12 kill chain: the kill chain begins with delivery and only includes resource development later in the kill chain. In this attack, Turla registered an expired domain name used by a common malware after the victims were already infected by the malware.

After these initial steps, further differences can be identified. In APT28 kill chains, the attacks move quickly to execution, often with the help of social engineering or exploitation. APT28 attacks use exploitation more than the other groups, though the group also uses social engineering even where exploitation is taken advantage of. APT29 appears to compensate for the relative lack of exploitation techniques with more occurrences of social engineering, with multiple kill chains including two or three occurrences of social engineering. Turla kill chains only include exploitation or social engineering, not both. This could be at least partly due to APT28 and APT29 favouring malicious documents whereas Turla uses watering hole attacks more often.

With APT28's relatively short kill chains, additional techniques such as persistence or defense evasion are not seen in many kill chains before execution is reached. APT29 kill chains, on the other hand, include more steps before execution. These commonly include additional delivery, social engineering, defense evasion, or persistence techniques. Notably in multiple kill chains, APT29 has multiple occurrences of defense evasion techniques before execution and before command & control server is contacted. Turla kill chains, on the other hand, commonly include discovery techniques before execution. This can be seen most clearly in the watering hole attacks where initial discover is performed with Javascript as a potential victim first visits a malicious website.

After execution has been reached, the kill chains are again more similar across the groups: defense evasion and persistence are the most common techniques before reaching out to the command & control server.

5.2.3 Actions after the compromise

After the initial compromise stage, not many clear similarities can be identified from the kill chains of the groups. Instead, the kill chains for all groups appear to be more unique, even when only comparing within the groups. Some limited similarities can still be identified. All groups can be identified performing additional delivery, as the groups send additional tools or malware to the compromised environment. APT28 and APT29 show some similarity, as the groups only rarely perform the additional steps at this point that can often be seen from Turla, such as discovery, privilege escalation, credential access, or lateral movement. However, some individual APT28 and APT29 kill chains do include additional steps at this stage, such as the ones mentioned earlier, but also defense evasion, persistence, and command & control connections. APT28 and APT29 kill chains instead generally reach their final steps quickly after reaching the first connection to the command & control server. APT28 and APT29 have in common the final steps being collection and exfiltration in most cases. APT29 kill chains also in some instances end their kill chain with execution.

Turla kill chains differ slightly from APT28 and APT29 as noted above. In all Turla kill chains, discovery can be identified after the command & control is reached, even in the cases where discovery has already been performed in an earlier stage. Turla kill chains also include more occurrences of credential access and lateral movement than APT28 and APT29. In addition, Turla kill chains often include multiple occurrences of delivery, even at this stage, with some kill chains even ending with the delivery of a final payload. Though, in most cases, Turla kill chains also end with the same steps of collection and exfiltration, similar to APT28 and APT29 kill chains.

6 RESULTS

In this chapter the results will be discussed. The findings from the earlier chapters will be used to answer the research questions that were specified for this thesis.

6.1 Modus operandi of Russian connected APT groups

The APT groups studied for this thesis operate by using a wide selection of tactics, techniques, and procedures. The groups are persistent and capable of breaching even major organizations. The groups are also capable of many types of attacks. Though, when the objective of attacks could be identified, it was almost always the collection of various forms of sensitive information. As an exception to this, APT28 has been known to also perform some individual sabotage operations and to purposefully leak some information they have stolen in order to reach their objectives. These outlier attacks could not be identified in kill chain form. APT29 and Turla have only been known to perform operations where the apparent objective has been to covertly steal information. From the reports describing the groups and their operations, almost all phases of the Unified Kill Chain were covered by the TTPs used by all of the groups. APT28 and APT29 both have used various TTPs from all the different phases of the Unified Kill Chain; from Turla's attacks no impact TTPs were identified.

The analysis made it possible for typical kill chains and techniques used by each group to be identified. These were described in further detail in Chapter 5. In typical attacks, APT28 develops a malicious office document that is delivered via email to the victims. The email message or the malicious document typically uses some social engineering techniques, such as an embedded decoy document that is shown to a victim. The document also commonly includes an exploit that often targets a vulnerability in an office application, which then allows the group to execute their malware. This is often followed by the malware performing defense evasion, such as hiding files related to the malware, or persistence techniques, such as adding registry keys, before it connects to the group's command

& control server. Then APT28 typically sends additional payloads to the compromised system. These payloads are often more sophisticated custom malware. Sometimes at this stage, the group performs privilege escalation, which is often done via credential access techniques by using tools like Mimikatz, followed by lateral movement to expand their access. The typical APT28 kill chain ends with execution of additional code, collection of data, and exfiltration of the collected data.

Typical APT29 attacks begin with the development of a malicious document that is then emailed to their victims. The malicious document is often an HTML file that contains an ISO file, which actually contains the malware files. The embedding of malicious files into other files is a common defense evasion technique used by APT29. In some cases, the malicious document has also been an office document with a decoy and an exploit. The malicious files usually employ some social engineering tricks, such as a shortcut file masquerading as a document that the user is tricked into opening. This then allows the group to have their malware be executed. At this point the malware typically performs persistence techniques, such as adding registry keys, and sometimes additional defense evasion techniques, like checking for the existence of antivirus software, before connecting to the command & control server. From the command & control server, APT29 often delivers additional payloads, which are generally additional custom malware or even commercial tools like a Cobalt Strike beacon. The additional payloads are sometimes used to execute additional commands at this stage. After this phase, the group sometimes performs credential access, often with living off the land methods or in some cases with tools like Mimikatz. The group sometimes uses the gained credentials to escalate privileges. The attacks then often end with APT29 collecting and exfiltrating data.

Turla attacks typically include reconnaissance of the desired victims before a watering hole website is prepared. As the victims browse to the watering hole site, malicious Javascript is delivered to the victim's browser, which performs some initial discovery, attempting to identify the victim's device. If the victim is deemed interesting and suitable, an exploit can be used to execute Turla malware, or the victim can be convinced to download and execute a malicious installer with social engineering techniques. This could be, for example, showing the victim a message telling them an update is required. These techniques then allow the execution of the group's malware. The malware then often performs defense evasion like checking for antivirus software. After these steps, the malware connects to the command & control server. From the command & control server, Turla often commands the malware to perform additional discovery techniques, often with a set of predetermined operating system commands, in order to identify the victim device and their network further before more payloads are sent or additional actions are taken. If additional payloads are sent, they are often more advanced custom malware or additional tools to perform further steps, which are commonly credential access and lateral movement. Generally, after credential access and lateral movement are performed, the final steps in the attack are the collection and exfiltration of data. Sometimes one final additional payload is sent, in the form of a final malware to maintain persistence in the victim environment.

6.2 Similarity of Russian connected APT groups

The groups that were studied operate in broadly similar ways, though some differences were identified. The groups share a large portion of the TTPs they use, but each group has also used some unique TTPs. For example, similarity can easily be seen among all the groups in the use of some common and freely available tools, such as Mimikatz and Powershell. In addition to tools, similarities can be found in tool-independent techniques, such as taking advantage of scheduled tasks or startup folders to gain persistence, or using code obfuscation and encrypted communications for defense evasion.

Some specific differences between the TTPs used by the groups can be seen by noting some of the tools the groups use. Each of the groups has their own set of custom malware and tools, each with specific and different capabilities, technologies, and identifying artifacts. Interestingly, even beyond their own custom tools, the groups favour some different tools to perform the same tasks: APT28 using WinRAR, APT29 using 7-Zip, and Turla using rar and tar tools to create archived files before exfiltration. Beyond the use of different tools, the clearest differences in TTPs between the groups can be seen in delivery techniques and exploitation.

The different delivery methods show that APT28 and Turla have more variance in their delivery methods, whereas APT29 relies almost completely on email as their delivery method. APT29 has only performed individual attacks where they take advantage of the supply chain attack method as an alternative to email. Both APT28 and Turla have used watering hole attacks multiple times. APT28 has also been known to use stolen credentials as a delivery method and Turla has used the infrastructure of another APT group as a delivery method. In another attack, Turla registered an expired command & control domain name for a commodity malware to take control of its victims.

The supply chain attacks of APT29 appear to be a unique aspect of the group. While both APT28 and Turla have performed some attacks that have some aspects of supply chain attacks, only APT29 has been confirmed performing multiple attacks that are clearly supply chain attacks. However, despite these differences in the delivery techniques, a clear trend can be seen as all the groups rely heavily on email as their delivery method of malicious objects to the victim and as an initial attack method.

The differences identified in exploitation techniques show that out of the studied groups APT28 is the most willing and able to use a wide variety of exploits, even using multiple zero-day exploits in a relatively short period of time. While all groups exploited some vulnerabilities, APT28 was identified as having abused most exploits and in the largest variety of products.

In addition to specific tools and TTPs from single UKC phases, some differences can be identified from the totality of the kill chain phases. During multiple kill chain phases, APT29 was identified as using many living off the land methods for various purposes, such as discovery, privilege escalation, execution, credential access, and lateral movement. While these living off the land techniques used by APT29 were not all or even mostly unique to the group, APT29 can be identified using these methods the most.

A similar trend can be identified in the way Turla has differentiated itself. The group has used some innovative techniques, such as employing the unique delivery methods described earlier, using satellite connections for command & control traffic, using steganography to perform particularly stealthy exfiltration, and targeting email servers and clients with custom malware made to target these software specifically.

The kill chains that were created from the reports show that the operations these groups perform mostly have a similar structure. The attacks typically begin, progress, and end in a broadly similar manner and they mostly follow the phases of the Unified Kill Chain. However, as with the TTPs there are some differences and themes that can be identified.

Most of APT28's kill chains are slightly shorter than the other groups and they reach execution in fewer steps than other groups. This is often done by using exploitation techniques, of which there are more occurrences of, than in APT29 or Turla kill chains.

APT29 kill chains show that the group, possibly as a compensation for the relative lack of exploitation techniques, performs more social engineering techniques than either APT28 or Turla. APT29's kill chains also include more defense evasion techniques than the other groups, as most kill chains include two occurrences of the techniques and even up to four occurrences in one kill chain. The kill chains from APT29 also appear less uniform than APT28 and Turla.

Turla kill chains show that the group uses discovery techniques more than APT28 and APT29. Most Turla kill chains notably include occurrences of discovery techniques not only before, but also after the command & control server is contacted. This could be partly due to the way Turla uses watering hole attacks, but a similar pattern can be seen in some spear phishing attacks. Turla kill chains also showed more occurrences of reconnaissance techniques at the beginning of the kill chains. More occurrences of credential access and lateral movement can also be seen in Turla kill chains than in APT28 or APT29 kill chains.

Beyond the aspects found from TTPs and kill chains, more findings can be gleaned directly from the data that was studied. The groups have attacked some of the same victims. In the most notable case, APT28 and APT29 both having compromised the DNC networks simultaneously, apparently unaware of each other (Crowdstrike, 2020). In separate incidents, Turla has also been known to have attacked some of the same victims as APT29 and targeted some of the same victims as APT28 (Faou, 2020b; Kaspersky Labs, 2018c). Interestingly, in one case, researchers have even identified all three groups to have compromised the same devices (Faou, Tartare, & Dupuy, 2019). Additionally, some technical similarities were found in the code of some custom malware used by APT29 and Turla. The similarities were identified in Sunburst, which has been connected to APT29, and Kazuar, which has been connected to Turla. (Kucherin, Kuznetsov, & Raiu, 2021) Turla has also used Powershell embedded into shortcut files in an almost identical way to APT28 (Kaspersky Labs, 2018b).

7 CONCLUSION

The goal of this thesis was to study the way APT groups operate. More specifically the thesis was meant to broaden the understanding of how APT groups operate on a technical and tactical level, as well as to compare the way these groups operate. There exists a large amount of information about APT groups that has been published by the cyber security industry, but this has not yet been taken advantage of in peer-reviewed cyber security research. Three APT groups that have been connected to Russia were chosen to be studied because APT groups connected to Russia have been identified as particularly active, they have been connected to some of the most high-profile attacks, and additionally, there is a lot of information available on these APT groups (Council on Foreign Relations, 2022; Greenberg, 2019). To reach the goal of this study, two research questions were chosen with additional sub-questions for each:

1. How do APT groups connected to Russia operate?
   - What tactics, techniques, and procedures do Russian connected APT groups use?
   - How are these tactics, techniques, and procedures used by the groups (in attacks/operations)?

2. Do APT groups connected to Russia operate in a similar manner?

   - Are the tactics, techniques, and procedures used by Russian connected APT groups similar between the groups?
   - Are the tactics, techniques, and procedures used by Russian connected APT groups used in a similar way between the groups?

To answer these research questions, qualitative content analysis research method was chosen. Content analysis was performed by breaking down the research and analysis process into five steps. First an initial reading of the available data was done to get familiar with the data and to identify what will be the units of meaning. Following this, the units of meaning, which in this case were descriptions of

TTPs used by the groups, were found, noted, and highlighted from the data. After this the units of meaning were coded. This meant that the identified TTPs were categorized into the kill chain phases described in the UKC. Following this step, the data was then further categorized by organizing the found TTPs into kill chains to add additional context and structure to the data. For this modelling phase, the kill chain phases described in UKC were used. Each of these kill chains signifies specific attacks identified from each group, their capabilities, or tendencies. The final step of the analysis consisted of using the kill chains and TTPs which were identified and created using the data, to find relationships, themes, patterns, differences, and similarities between the groups and the ways the operate. This analysis then allowed the research questions to be answered.

The data that was used for the thesis was collected from public sources and mostly consisted of various reports, whitepapers, and articles from various cyber security vendors, industry researchers, governmental organizations, and some limited academic sources. The data was collected by searching for literature regarding the specific APT groups from search engines such as Google, Google Scholar, and JYKDOK as well as taking searching from industry information repositories such as Malpedia, MITRE ATT&CK knowledge base, and VX-Underground.

Before analysing the data, the concept of Advanced Persistent Threats (APTs) was discussed, described, and defined. The process of APT attribution and problems relating to it were also discussed during this section. Additionally, various models and frameworks that have been used to model APT groups and APT attacks were studied to identify a suitable model that could be used to study the chosen APT groups. Ultimately, the Unified Kill Chain (UKC) was chosen for the analysis stage of this thesis.

Following this, the coding and categorization of the data was conducted. The collected data was coded and categorized following the steps outlined in the research methodology. Using this coded and categorized data, each APT group was described before describing the TTPs that were identified for each group. The kill chains that were created for each group following the Unified Kill Chain framework were also described at this stage.

The next step was analysis of the data that was now coded and categorized into TTPs and kill chains. The analysis of TTPs was done by comparing TTPs used by each group which had been categorized into the phases of the Unified Kill Chain. The kill chains were analysed by comparing kill chains from the groups as wholes and as individual parts divided into separate stages of the kill chains. Finally, the analysis that was performed was used to produce the findings of the study and answer the research questions that were set for this thesis.

7.1 Discussion of the results

The findings of this study show that the APT groups that were studied use a wide selection of tactics, techniques, and procedures during their operations which were described at length. The groups are not limited to only a single type of attack and are capable of using different TTPs when necessary. The identified objectives from the groups suggest that the groups focus almost entirely on the stealing of sensitive data from their chosen victims. Out of the studied groups, only APT28 has performed individual attacks that appear to have had objectives other than stealing sensitive data. This could indicate that APT28 is slightly more aggressive or less careful in their operations than APT29 or Turla, as sabotage operations or attacks where stolen information is leaked are bound to be noticed by the victim. It could also simply suggest that APT28 has different tasking than APT29 and Turla.

The typical attacks for each APT group were described using the kill chains and the TTPs. APT28 and APT29 generally relying on spear phishing attacks via email, which use different types of malicious documents, while Turla typically uses watering hole attacks, which take advantage of social engineering or exploits. The kill chains from all the groups typically culminate in the collection and exfiltration of data. This coincides with finding of the objectives that were identified from the TTPs and the attributions of the APT groups to various intelligence services.

The findings from both the kill chains and TTPs show that the groups operate in broadly similar ways. The groups share many TTPs, and the kill chains were seen as mostly similar. There are also similarities outside the TTP and kill chain analysis, as the groups have been identified targeting and successfully attacking the same victims in multiple cases. This could suggest that the groups share interests, or the groups have been tasked with similar goals in mind. Additionally, similarities in the code of their custom tools have been found. This could suggest that the groups share at least some developers. This has all but been confirmed as each of the specific Russian state organizations that these APT groups have been connected to — Russian military intelligence agency GRU, Russian Foreign Intelligence Service SVR, and the Russian Federal Security Service FSB — have been known to have worked with and have contracts with the same company, “NTC Vulkan” (Antoniadis et al., 2023).

Despite these similarities, some differences as well as some general themes could be identified from the TTPs and kill chains. The clearest differences in TTPs could be identified in the delivery and exploitation techniques.

The differences in exploitation techniques showed that APT28 was the most prolific user of exploits. The group used exploits in most of its attacks and was also connected to exploits that targeted the widest selection of products. This could be identified from both the TTPs and kill chains. Another finding showing that APT28 kill chains are slightly shorter than the other groups could also be related to this finding. If the use of exploits allows APT28 to skip some steps in their kill chains, it could mean that APT28 kill chains are shorter specifically due to the use of exploits. As exploits to vulnerabilities are sometimes sold on the black market, the heavy use of exploits by APT28 could suggest they access to the biggest budget of the groups. It could also suggest that APT28 has the most expertise regarding exploitation of vulnerabilities or lacks expertise in other areas.

The delivery method analysis showed that APT28 and Turla both had more variety in their delivery methods while APT29 relied almost exclusively on spear phishing via email. However, in the remaining kill chain, APT29 was identified using supply chain attack as a delivery method, unique among the groups. This same delivery method was also seen in the TTPs of more APT29 attacks, showing it is not a one-off. Turla was also identified using some unique and innovative delivery methods not seen elsewhere. Turla took over the infrastructure of another APT group and in another attack registered an expired domain name used for the command & control of a commodity malware, using both methods to gain access to new victims. Despite the differences, a trend within delivery methods could be identified across the groups. The use of malicious emails is a method that all of the groups use heavily and one that some groups would almost certainly be struggling without. This could be a potentially sensible point of focus for defenders.

Some differences and themes were also seen in TTPs across multiple phases of the UKC. In what can be seen as a theme, APT29 used various living off the land techniques in multiple kill chain phases much more than the other groups. This could suggest that APT29 values staying undetected more than the other groups, as additional tools could increase the risk of being detected. This suggestion is strengthened by the reports that often note that APT29 is particularly stealthy and has a high level of operations security. This is also supported by a similar finding that APT29 also uses defense evasion techniques more than APT28 and Turla.

A general theme could also be seen regarding Turla. The group has used some techniques that have been described as particularly innovative and are unique among the groups. These techniques include the unique delivery techniques described earlier, the innovative way of using satellite connections for command & control infrastructure, using steganography to perform particularly stealthy exfiltration, and using custom malware that specifical targets email servers and client software.

Additional findings regarding Turla from the kill chains show that they include more use of discovery techniques than other groups that were studied. Turla could also be seen performing more initial reconnaissance in their kill chains. These findings could suggest that Turla is very specific when it is selecting its victims. This is supported by some reports noting that Turla is indeed particularly careful and selective in its targeting. Turla kill chains also include more credential access and lateral movement techniques. This could suggest that Turla is not only after specific victims, but also after very specific information, instead of stealing whatever is available, which could require additional lateral movement.

These findings show that organizations looking to defend against specifically Russian connected APT groups must be able to defend against many techniques. This can also be seen as possible opportunities to detect attacks by these groups. However, focusing on email security should be a top priority for these organizations, as this covers a very important delivery method for both APT28 and APT29, with Turla also using emails in at least some of their attacks. For defenders looking to defend against Turla attacks, particular focus could be put into updating web browsers as soon as updates are available and training the end users to be vary of watering hole attacks, as some of the watering hole attacks use social engineering.

All of the groups also often employ various social engineering techniques. This could be another potential area of focus by training the members of organizations extensively to look out for, and to be aware of, social engineering techniques. As all of the groups also focus largely on stealing sensitive information, the most valuable information inside these organizations should be secured with extraordinary care.

7.2 Limitations of the research

The main limitation in this research is the data that was collected and analysed. The data used for this thesis could possibly disproportionately highlight certain tactics, techniques, or procedures, or alternatively understate or miss certain tactics, techniques, or procedure which are harder to identify. The data could also include a disproportionately small or large amount of information regarding a certain group, when compared to the other groups.

As peer-reviewed research about APT groups is not readily available, it was necessary to largely rely on data provided by vendors of various cyber security products and other industry organizations. The cyber security vendors have their own commercial interests and motives that might not coincide with publishing their findings accurately and without biases. The various information sources used for this thesis also might have differing views on what constitutes a specific tactic, technique, or procedure, and in these aspects the reports and the data might not be entirely comparable. Additionally, the different naming conventions used by various information sources are possible sources of misunderstandings or mistakes. For this study, it was assumed that the naming conventions used by different sources are accounted for in the collation of data in MITRE ATT&CK knowledge base and Malpedia. Should there be some misattribution, unintended overlap, or other mistakes in the names, some findings in the study will possibly have been faulty.

Another possible limitation of the research was the interpretative analysis that was necessary for the analysis of the TTPs and kill chains. This makes exact replication of the research difficult. To aid any replication studies, further descriptions and references to the kill chains can be found in the appendix.

The thesis also did not take into account the time when the various techniques were used or when attacks were performed. This could lead to certain tactics, techniques, procedures, or types of attacks being attributed to groups which are no longer in the repertoire of said groups. This might also cause the results of the research to not give an accurate representation of the current capabilities of the groups that were studied, or the tactics, techniques, procedures, or types of attacks currently favoured by the groups.

7.3 Suggestions for future research

Future research could be directed to studying APT groups that have been attributed to multiple different countries to identify possible similarities or differences between the groups attributed to different countries. Future research could also be conducted with different and possibly some more standardized set of data, if such data becomes available at a later date. Another possible avenue for future research could be creating a model or framework specifically for comparing APT groups. Future research could also be done on how the TTPs used by certain APT groups or types of attacks performed by the groups have evolved as time goes by or if they remain the same.

REFERENCES

Accenture. (2020, October 28). Turla uses HyperStack, Carbon, and Kazuar to compromise government entity. Retrieved 5 July 2023, from https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity

Adair, S. (2016). *PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs*. Retrieved from https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

Agarwal, A., Walia, H., & Gupta, H. (2021). Cyber Security Model for Threat Hunting. *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1–8. https://doi.org/10.1109/ICRITO51393.2021.9596199

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, *86*, 402–418. https://doi.org/10.1016/j.cose.2019.07.001

Aimé, F. (2022). *NOBELIUM's EnvyScout infection chain goes in the registry, targeting embassies*. Retrieved from https://blog.sekoia.io/nobeliums-envyscout-infection-chain-goes-in-the-registry-targeting-embassies/

Aldridge, J. (2012). Remediating Targeted-threat Intrusions (p. 10). Retrieved from https://media.blackhat.com/ad-12/Aldridge/bh-ad-12-remediating-Aldridge-WP.pdf

Alert Logic. (2023). Penetration Testing Tool, Responder. Retrieved 1 October 2023, from https://support.alertlogic.com/hc/en-us/articles/360004707492-Penetration-Testing-Tool-Responder

Al-Matarneh, eras M. (2020). ADVANCED PERSISTENT THREATS AND ITS ROLE IN NETWORK SECURITY VULNERABILITIES. *International Journal of Advanced Research in Computer Science*, *11*(1), 11–20. https://doi.org/10.26483/ijarcs.v11i1.6502

Al-Mohannadi, H., Awan, I., & Hamar, J. (2020). Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence. *Service Oriented Computing and Applications*, *14*. https://doi.org/10.1007/s11761-019-00285-7

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and

Research Opportunities. *IEEE Communications Surveys & Tutorials*, *PP*, 1–1. https://doi.org/10.1109/COMST.2019.2891891

ANSSI. (2021). *PHISHING CAMPAIGNS BY THE NOBELIUM INTRUSION SET*. Retrieved from https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-011.pdf

Anthe, C., Jones, J., Penta, A., Chrzan, P., Ng, N., Ragragio, I., … Henry, P. (2015). *Microsoft Security Intelligence Report – Volume 19*. Retrieved from https://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf

Antoniadis, N., Baumann, S., Buschek, C., Christoph, M., Diehl, J., Epp, A., … Widmann-Schmidt, W. (2023, March 30). The 'Vulkan Files' -A Look Inside Putin's Secret Plans for Cyber-Warfare. *Der Spiegel*. Retrieved from https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236

Ashcraft, A., Sharkey, K., Coulter, D., Batchelor, D., & Satran, M. (2021, January 7). Microsoft SMB Protocol and CIFS Protocol Overview—Win32 apps. Retrieved 1 October 2023, from https://learn.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview

Asher-Dotan, L. (2023). What are Supply Chain Attacks? Retrieved 1 October 2023, from https://www.cybereason.com/blog/what-are-supply-chain-attacks

Aspers, P., & Corte, U. (2019). What is Qualitative in Qualitative Research. *Qualitative Sociology*, *42*(2), 139–160. https://doi.org/10.1007/s11133-019-9413-7

BAE Systems. (2014). *SNAKE CAMPAIGN & CYBER ESPIONAGE TOOLKIT*. Retrieved from https://artemonsecurity.com/snake_whitepaper.pdf

Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K.-K. R., & Javadi, H. H. S. (2019). Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures. *Journal of Information Processing Systems*, *15*(4), 865–889. https://doi.org/10.3745/JIPS.03.0126

Barnett, J. (2021). *NOBELIUM Campaigns and Malware*. Retrieved from https://blogs.infoblox.com/cyber-threat-intelligence/nobelium-campaigns-and-malware/

Bartholomew, B. (2017). *KopiLuwak: A New JavaScript Payload from Turla*. Retrieved from https://securelist.com/kopiluwak-a-new-javascript-payload-from-turla/77429/

Baumgartner, K., & Raiu, C. (2014). *The 'Penquin' Turla*. Retrieved from https://securelist.com/the-penquin-turla-2/67962/

Baumgartner, K., & Raiu, C. (2015). *The CozyDuke APT*. Retrieved from https://securelist.com/the-cozyduke-apt/69731/

Benchea, R., Vatamanu, C., Maximciuc, A., & Luncaşu, V. (2015). *APT28 Under the Scope – A Journey into Exfiltrating Intelligence and Government Information*. Retrieved from https://cdn2.hubspot.net/hubfs/341979/PDFs/Bitdefender_In-depth_analysis_of_APT28The_Political_Cyber-Espionage_Mal....pdf?__hstc=&__hssc=&hsCtaTracking=3c039578-15a3-4838-ac8a-f34ef1105a51%7Cd97a753a-8552-4f88-b6e0-2610ffc3f133

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, *2*, 8–14. https://doi.org/10.1016/j.npls.2016.01.001

Betz, D. J., & Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Routledge.

Bianco, D. J. (2013, March 1). Enterprise Detection & Response: The Pyramid of Pain. Retrieved 18 December 2022, from http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Bienstock, D. (2022). *You Can't Audit Me: APT29 Continues Targeting Microsoft 365*. Retrieved from https://www.mandiant.com/resources/blog/apt29-continues-targeting-microsoft

Bitdefender. (2015a). *Dissecting the APT28 Mac OS X Payload*. Retrieved from https://download.bitdefender.com/resources/files/News/CaseStudies/study/143/Bitdefender-Whitepaper-APT-Mac-A4-en-EN-web.pdf

Bitdefender. (2015b). *Pacifier APT*. Retrieved from https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender-Whitepaper-PAC-A4-en_EN1.pdf

Bitdefender. (2017). New Pacifier APT Components Point to Russian-Linked Turla Group. Retrieved from https://download.bitdefender.com/resources/files/News/CaseStudies/study/170/Bitdefender-Whitepaper-Pacifier2-A4-en-EN.pdf

Bodeau, D., Fox, D. B., & McCollum, C. D. (2018). Cyber Threat Modeling: Survey, Assessment, and Representative Framework (p. 119). Retrieved from https://www.mitre.org/sites/default/files/2021-11/prs-18-1174-ngci-cyber-threat-modeling.pdf

Boebert, W. E. (2010). *A Survey of Challenges in Attribution*. Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. https://doi.org/10.17226/12997

Boutin, J.-I. (2017, June 6). Turla's watering hole campaign: An updated Firefox extension abusing Instagram. Retrieved 30 June 2023, from https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Bunda, J. (2020). *APT28: Tapaustutkimus Venäjään yhdistettyjen kyberoperaatioiden kehittymisestä vuosina 2007 - 2016*. Retrieved from https://jyx.jyu.fi/handle/123456789/67845

Burita, L., & Le, D. T. (2021). Cyber Security and APT Groups. *2021 Communication and Information Technologies (KIT)*, 1–7. https://doi.org/10.1109/KIT52904.2021.9583744

Burt, T. (2021, October 25). New activity from Russian actor Nobelium. Retrieved 17 May 2023, from https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium/

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The Diamond Model of Intrusion Analysis*. 62. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

Calvert, J. (2014, November 11). Sednit Espionage Group Attacking Air-Gapped Networks. Retrieved 8 January 2023, from https://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/

Cash, D., Grunzweig, J., Meltzer, M., Koessel, S., Adair, S., & Lancaster, T. (2021). *Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns*. Retrieved from https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/

Cash, D., Meltzer, M., Koessel, S., Adair, S., & Lancaster, T. (2020). *Dark Halo Leverages SolarWinds Compromise to Breach Organizations*. Retrieved from https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/

Cisco. (2023). What Is an Exploit? Retrieved 1 October 2023, from https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html

Clark, D. D., & Landau, S. (2010). Untangling Attribution. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Retrieved from https://www.nap.edu/read/12997/chapter/4

Cloudflare. (2023). What is a domain name? Retrieved 1 October 2023, from https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/

Couchard, G., & Arquillière, M. (2022, May 23). TURLA's new phishing-based reconnaissance campaign in Eastern Europe. Retrieved 30 June 2023, from https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/

Council on Foreign Relations. (2022). Tracking State-Sponsored Cyberattacks Around the World. Retrieved 2 November 2022, from https://www.cfr.org/cyber-operations

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (4th ed). Boston: Pearson.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed). Thousand Oaks: SAGE Publications.

Creus, D., Halfpop, T., & Falcone, R. (2016, September 26). Sofacy's 'Komplex' OS X Trojan. Retrieved from https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/

Crowdstrike. (2019, February 12). Who is FANCY BEAR (APT28)? Retrieved 11 January 2023, from https://www.crowdstrike.com/blog/who-is-fancy-bear/

Crowdstrike. (2020, June 5). CrowdStrike's work with the Democratic National Committee: Setting the record straight. Retrieved 3 January 2023, from https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Crowdstrike. (2022a, June 15). What is an Advanced Persistent Threat (APT)? | CrowdStrike. Retrieved 8 November 2022, from https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

Crowdstrike. (2022b). Adversary: Fancy Bear - Threat Actor. Retrieved 11 December 2022, from https://adversary.crowdstrike.com/en-US/adversary/fancy-bear/?L=75/

Crowdstrike. (2022c). *Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign*. Retrieved from https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

Crowdstrike. (2022d). Adversary: Venomous bear—Threat Actor. Retrieved 1 July 2023, from https://web.archive.org/web/20221220093236/https://adversary.crowdstrike.com/en-US/adversary/venomous-bear/

Cybersecurity & Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, Canadian Centre for Cyber Security, Government Communications Security Bureau, National Cyber Security Centre UK, & National Crime Agency. (2022). *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*. Retrieved from https://www.cisa.gov/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf

CyCraft Technology Corp. (2022, June 10). Threat Attribution—Chimera "Under the Radar". Retrieved 18 December 2022, from https://cycrafttechnology.medium.com/threat-attribution-chimera-under-the-radar-7c4cce390efd

Cyware. (2020, May 29). Turla Hacker Group Continues to Innovate and Stun Security Researchers. Retrieved 2 July 2023, from https://cyware.com/news/turla-hacker-group-continues-to-innovate-and-stun-security-researchers-821bdd90

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*, *15*(4), 277–305. https://doi.org/10.1007/s11416-019-00338-7

Dunwoody, M. (2017a). *Dissecting One of APT29's Fileless WMI and PowerShell Backdoors (POSHSPY)*. Retrieved from https://www.mandiant.com/resources/blog/dissecting-one-ofap

Dunwoody, M. (2017b). *APT29 Domain Fronting With TOR*. Retrieved from https://www.mandiant.com/resources/blog/apt29-domain-frontin

Dunwoody, M., Thompson, A., Withnell, B., Leathery, J., Matonis, M., & Carr, N. (2018). *Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign*. Retrieved from https://www.mandiant.com/resources/blog/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign

Eckels, S., Smith, J., & Ballenthin, W. (2020). *SUNBURST Additional Technical Details*. Retrieved from https://www.mandiant.com/resources/blog/sunburst-additional-technical-details

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis: A Focus on Trustworthiness. *SAGE Open*, *4*(1), 215824401452263. https://doi.org/10.1177/2158244014522633

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, *62*(1), 107–115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

Engel, G. (2014, November 18). Deconstructing The Cyber Kill Chain. Retrieved 12 November 2022, from https://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain

ENISA. (2014). *Advanced persistent threat incident handling handbook*. Retrieved from https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/advanced_persistent_threat_incident_handling_handbook

ENISA. (2023a). Rootkits [Page]. Retrieved 1 October 2023, from https://www.enisa.europa.eu/topics/incident-response/glossary/rootkits

ENISA. (2023b). What is Social Engineering? [Page]. Retrieved 1 October 2023, from https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

ESET. (2014a, October 8). Sednit espionage group now using custom exploit kit. Retrieved 8 January 2023, from https://www.welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/

ESET. (2014b). *Miniduke still duking it out*. Retrieved from https://www.welivesecurity.com/2014/05/20/miniduke-still-duking/

ESET. (2016). *En Route with Sednit*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-full.pdf

ESET. (2017a). *Gazing at Gazer – Turla's new second stage backdoor*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

ESET. (2017b, March 30). Carbon Paper: Peering into Turla's second stage backdoor. Retrieved 30 June 2023, from https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/

ESET. (2018a). *Sednit update: Analysis of Zebrocy*. Retrieved from https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/

ESET. (2018b). *TURLA OUTLOOK BACKDOOR - Analysis of an unusual Turla backdoor*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf

ESET. (2018c, May 22). Turla Mosquito: A shift towards more generic tools. Retrieved 30 June 2023, from https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/

ESET. (2019, September 24). No summer vacations for Zebrocy. Retrieved 14 June 2023, from https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/

ESET. (2022). *Threat Report T3 2021*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2022/02/eset_threat_report_t32021.pdf

European Repository on Cyber Incidents. (2023). *APT28 – Exploiting Democratic Vulnerabilities in Cyberspace*. Retrieved from https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_APT_28_4856c0a0ac.pdf

Falcone, R. (2018, December 18). Sofacy Creates New 'Go' Variant of Zebrocy Tool. Retrieved 31 July 2023, from https://unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/

Falcone, R., & Lee, B. (2016, June 14). New Sofacy Attacks Against US Government Agency. Retrieved 8 January 2023, from https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agency/

Faou, M. (2019). *Turla LightNeuron: One email away from remote code execution*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

Faou, M. (2020a). *FROM AGENT.BTZ TO COMRAT V4 – A ten-year journey*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

Faou, M. (2020b, December 2). Turla Crutch: Keeping the "back door" open. Retrieved 23 September 2022, from https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

Faou, M. (2020c, March 12). Tracking Turla: New backdoor delivered via Armenian watering holes. Retrieved 30 June 2023, from https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/

Faou, M., & Dumont, R. (2019, May 29). A dive into Turla PowerShell usage. Retrieved 30 June 2023, from https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/

Faou, M., Tartare, M., & Dupuy, T. (2019). *OPERATION GHOST: The Dukes aren't back – They never left*. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

Federal Bureau of Investigation, National Security Agency, Cybersecurity & Infrastructure Security Agency, United States Cyber Command, Canadian Centre for Cyber Security, National Cyber Security Centre UK, … National Cyber Security Centr NZ. (2023). *Hunting Russian Intelligence "Snake" Malware*. Retrieved from https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_2.pdf

FireEye. (2014). *APT28: A Window Into Russia's Cyber Espionage Operations?* Retrieved from https://samples.vx-underground.org/root/Papers/ICS%20SCADA/Other/2014-10-27%20-%20APT28%20-%20A%20Window%20into%20Russias%20Cyber%20Espionage%20Ops.pdf

FireEye. (2015a). Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack. Retrieved from https://www.mandiant.com/resources/blog/probable-apt28-useo

FireEye. (2015b). *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*. Retrieved from https://www.mandiant.com/sites/default/files/2021-09/rpt-apt29-hammertoss-1-1.pdf

FireEye. (2015c). *Pinpointing Targets: Exploiting Web Analytics to Ensnare Victims*. Retrieved from https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf

FireEye. (2017). *APT28: At The Center of The Storm: Russia Strategically Evolves Its Cyber Operations*. Retrieved from https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf

FireEye. (2020). *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*. Retrieved from https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

France, N. (2023, July 12). What is a Digital Certificate? Retrieved 1 October 2023, from https://www.sectigo.com/resource-library/what-is-a-digital-certificate

F-Secure. (2015a). *The Dukes 7 – Years Of Russian Cyberespionage*. Retrieved from https://blog.f-secure.com/wp-content/uploads/2020/03/F-Secure_Dukes_Whitepaper.pdf

F-Secure. (2015b). *COZYDUKE*. Retrieved from https://blog.f-secure.com/wp-content/uploads/2019/10/CozyDuke.pdf

G Data SecurityLabs. (2014). *Uroburos – Highly complex espionage software with Russian roots*. Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2014/08/20082353/GData_Uroburos_RedPaper_EN_v1.pdf

Google Threat Analysis Group. (2023). *Fog of War – How the Ukraine Conflict Transformed the Cyber Threat Landscape*. Retrieved from https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

Gossi, C. (2020). IDENTIFYING ATTACKERS BY USING MACHINE LEARNING ON UNSTRUCTURED CYBER THREAT INTELLIGENCE. Retrieved from https://www.goescy.ch/identifying_attackers/goessi2020attackers.pdf

Gostev, A. (2014). *Agent.btz: A Source of Inspiration?* Retrieved from https://securelist.com/agent-btz-a-source-of-inspiration/58551/

GovCERT.ch. (2016). *APT Case RUAG - Technical Report*. Retrieved from https://www.govcert.ch/downloads/whitepapers/Report_Ruag-Espionage-Case.pdf

Graneheim, U. H., Lindgren, B.-M., & Lundman, B. (2017). Methodological challenges in qualitative content analysis: A discussion paper. *Nurse Education Today*, *56*, 29–34. https://doi.org/10.1016/j.nedt.2017.06.002

Greenberg, A. (2017, September 11). How the Mimikatz Hacker Tool Stole the World's Passwords | WIRED. Retrieved 1 October 2023, from https://web.archive.org/web/20171109151816/https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Greenberg, A. (2023, May 20). The Underground History of Russia's Most Ingenious Hacker Group. *Wired*. Retrieved from https://www.wired.com/story/turla-history-russia-fsb-hackers/

Guarnieri, C. (2015, June 19). Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag. Retrieved 1 February 2023, from https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

Guerrero-Saade, J. A., Raiu, C., & Rid, T. (2018). *PENQUIN'S MOONLIT MAZE - The Dawn of Nation-State Digital Espionage*. Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf

Guibernau, F., Towne, K., & Wells, J. (2022, September 21). Emulating the Sophisticated Russian Adversary APT28. Retrieved 15 January 2023, from https://www.attackiq.com/2022/09/21/emulating-the-sophisticated-russian-adversary-apt28/

Haaster, J. V., Gevers, R., & Sprengers, M. (2016). *Cyber Guerilla*. Syngress.

Hacquebord, F. (2017). *Two Years of Pawn Storm Examining an Increasingly Relevant Threat*. Retrieved from https://resources.trendmicro.com/rs/945-CXD-062/images/2017-Q2-EMEA-EN-wp-two-years-of-pawn-storm.pdf

Hacquebord, F. (2018, January 12). Update on Pawn Storm: New Targets and Politically Motivated Campaigns. Retrieved from https://www.trendmicro.com/en_us/research/18/a/update-pawn-storm-new-targets-politically-motivated-campaigns.html

Hacquebord, F., & Mercês, F. (2015, February 4). Pawn Storm Update: iOS Espionage App Found. Retrieved 8 January 2023, from https://www.trendmicro.com/en_us/research/15/b/pawn-storm-update-ios-espionage-app-found.html

Hacquebord, F., & Remorin, A. (2020, December 17). Pawn Storm's Lack of Sophistication as a Strategy. Retrieved 8 January 2023, from https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html

Harbison, M., & Renals, P. (2022). *Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive*. Retrieved from https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/

Hasan, K., Shetty, S., Islam, T., & Ahmed, I. (2022). Predictive Cyber Defense Remediation against Advanced Persistent Threat in Cyber-Physical Systems. *2022 International Conference on Computer Communications and Networks (ICCCN)*, 1–10. https://doi.org/10.1109/ICCCN54977.2022.9868886

Hawley, S., Roncone, G., McLellan, T., Mattos, E., & Wolfram, J. (2023, January 5). Turla: A Galaxy of Opportunity. Retrieved 30 June 2023, from https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

Hirvonen, T. (2014). *COSMICDUKE Cosmu with a twist of MiniDuke*. Retrieved from https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf

Hsieh, H.-F., & Shannon, S. E. (2005). *Three Approaches to Qualitative Content Analysis | Scinapse*. https://doi.org/10.1177/1049732305276687

Huhta, R. (2021). *Venäjän federaation tavat suorittaa hyökkäyksellisiä kyberoperaatioita vuosina 2007–2020*. Retrieved from https://jyx.jyu.fi/handle/123456789/76232

Huss, D. (2017, August 17). Turla APT actor refreshes KopiLuwak JavaScript backdoor for use in G20-themed attack. Retrieved 30 June 2023, from https://www.proofpoint.com/us/threat-insight/post/turla-apt-actor-refreshes-kopiluwak-javascript-backdoor-use-g20-themed-attack

Hussain, S., Ahmad, M. B., & Ghouri, S. S. U. (2021). Advance Persistent Threat—A Systematic Review of Literature and Meta-Analysis of Threat Vectors. In S. K. Bhatia, S. Tiwari, S. Ruidan, M. C. Trivedi, & K. K. Mishra (Eds.), *Advances in Computer, Communication and Computational Sciences* (pp. 161–178). Singapore: Springer. https://doi.org/10.1007/978-981-15-4409-5_15

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. 14. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Ilascu, I. (2018, September 27). APT28 Uses LoJax, First UEFI Rootkit Seen in the Wild. Retrieved from https://www.bleepingcomputer.com/news/security/apt28-uses-lojax-first-uefi-rootkit-seen-in-the-wild/

Jansen, W. (2021, January 12). Abusing cloud services to fly under the radar. Retrieved 18 December 2022, from https://research.nccgroup.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/

Jansson, K., & Von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929X.2011.632650

Jazi, H., & Santos, R. (2022, June 13). Russia's APT28 uses fear of nuclear war to spread Follina docs in Ukraine. Retrieved from https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine

Jenkins, L., Sarah, H., Parnian, N., & Bienstock, D. (2021). *Suspected Russian Activity Targeting Government and Business Entities Around the Globe*. Retrieved from https://www.mandiant.com/resources/blog/russian-targeting-gov-business

Jiang, G., Lanstein, A., Berry, A., Read, B., Kizhakkinan, D., & McManus, G. (2017, May 9). EPS Processing Zero-Days Exploited by Multiple Threat Actors. Retrieved 4 July 2023, https://www.mandiant.com/resources/blog/eps-processing-zero-days

Johansson, M. (2021). *Venäjän ja Kiinan sotilastiedusteluorganisaatioiden kybermenetelmien kehitys vuosina 2004–2021*. Retrieved from https://jyx.jyu.fi/handle/123456789/75923

Jung, J. (2021, May 7). What is Password Hashing and Salting? Retrieved 1 October 2023, from https://www.okta.com/uk/blog/2019/03/what-are-salted-passwords-and-password-hashing/

Juurvee, I., & Mattiisen, M. (2020). *Revisiting an early case of hybrid Conflict*. 55. Retrieved from https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf

Karsikas, J. (2021). *Monitapaustutkimus valikoiduista Kiinaan ja Venäjään liitetyistä kyberhyökkäysryhmistä: Kohdennetut haittaohjelmahyökkäykset*. Retrieved from https://jyx.jyu.fi/handle/123456789/75892

Kaspersky. (2023a). What are Cookies? Retrieved 1 October 2023, from https://www.kaspersky.com/resource-center/definitions/cookies

Kaspersky. (2023b). What is a Living off the Land (LotL) attack? Retrieved 1 October 2023, from https://encyclopedia.kaspersky.com/glossary/lotl-living-off-the-land/

Kaspersky. (2023c, April 19). The Epic Turla (snake/Uroburos) attacks. Retrieved 30 June 2023, from https://www.kaspersky.com/resource-center/threats/epic-turla-snake-malware-attacks

Kaspersky Labs, G. R. & A. T. (2014a). *The Epic Turla Operation*. Retrieved from https://securelist.com/the-epic-turla-operation/65545/

Kaspersky Labs, G. R. & A. T. (2014b). *The Epic Turla Operation: Solving some of the mysteries of Snake/Uroboros*. Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080105/KL_Epic_Turla_Technical_Appendix_20140806.pdf

Kaspersky Labs, G. R. & A. T. (2015, December 4). Sofacy APT hits high profile targets with updated toolset. Retrieved 8 January 2023, from https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/

Kaspersky Labs, G. R. & A. T. (2017). *Introducing WhiteBear*. Retrieved from https://securelist.com/introducing-whitebear/81638/

Kaspersky Labs, G. R. & A. T. (2018a, February 20). A Slice of 2017 Sofacy Activity. Retrieved 8 January 2023, from https://securelist.com/a-slice-of-2017-sofacy-activity/83930/

Kaspersky Labs, G. R. & A. T. (2018b). *Shedding Skin – Turla's Fresh Faces*. Retrieved from https://securelist.com/shedding-skin-turlas-fresh-faces/88069/

Kaspersky Labs, G. R. & A. T. (2018c, March 9). Masha and these Bears. Retrieved from https://securelist.com/masha-and-these-bears/84311/

Kaspersky Labs, G. R. & A. T. (2019). *Turla renews its arsenal with Topinambour*. Retrieved from https://securelist.com/turla-renews-its-arsenal-with-topinambour/91687/

Kharouni, L., Hacquebord, F., Huq, N., Gogolinski, J., Mercês, F., Remorin, A., & Otis, D. (2014). *Operation Pawn Storm: Using Decoys to Evade Detection*. Retrieved from https://documents.trendmicro.com/assets/wp/wp-operation-pawn-storm.pdf

Kleinheksel, A. J., Rockich-Winston, N., Tawfik, H., & Wyatt, T. R. (2020). Demystifying Content Analysis. *American Journal of Pharmaceutical Education*, 11. https://doi.org/10.5688%2Fajpe7113

Korolov, M., & Myers, L. (2022, April 14). What is the cyber kill chain? A model for tracing cyberattacks. Retrieved 12 November 2022, from https://www.csoonline.com/article/2134037/what-is-the-cyber-kill-chain-a-model-for-tracing-cyberattacks.html

Kucherin, G., Kuznetsov, I., & Raiu, C. (2021). *Sunburst backdoor – code overlaps with Kazuar*. Retrieved from https://securelist.com/sunburst-backdoor-kazuar/99981/

Landler, M., & Markoff, J. (2007, May 28). In Estonia, what may be the first war in cyberspace. Retrieved 23 September 2023, from https://archive.ph/FDb95

Lee, B., & Falcone, R. (2016, October 17). 'DealersChoice' is Sofacy's Flash Player Exploit Platform. Retrieved 8 January 2023, from https://unit42.paloaltonetworks.com/unit42-dealerschoice-sofacys-flash-player-exploit-platform/

Lee, B., & Falcone, R. (2018, June 6). Sofacy Group's Parallel Attacks. Retrieved from https://unit42.paloaltonetworks.com/unit42-sofacy-groups-parallel-attacks/

Lee, B., Harbison, M., & Falcone, R. (2018, February 28). Sofacy Attacks Multiple Government Entities. Retrieved from https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/

Lehtiö, A. (2014). *OnionDuke: APT Attacks Via the Tor Network*. Retrieved from https://archive.f-secure.com/weblog/archives/00002764.html

Lehto, M. (2022). APT Cyber-attack Modelling: Building a General Model. *International Conference on Cyber Warfare and Security*, *17*(1), 121–129. https://doi.org/10.34190/iccws.17.1.36

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, *72*, 26–59. https://doi.org/10.1016/j.cose.2017.08.005

Leonard, B. (2022, July 19). Continued cyber activity in Eastern Europe observed by TAG. Retrieved 8 January 2023, from https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/

Leonardo. (2020). *MALWARE TECHNICAL INSIGHT - TURLA "Penquin_x64"*. Retrieved from https://www.leonardo.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf

Levene, B., Falcone, R., & Halfpop, T. (2017, May 3). Kazuar: Multiplatform Espionage Backdoor with API Access. Retrieved 30 June 2023, from https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Levene, B., Falcone, R., & Wartell, R. (2015). *Tracking MiniDionis: CozyCar's New Ride Is Related to Seaduke*. Retrieved from https://unit42.paloaltonetworks.com/tracking-minidionis-cozycars-new-ride-is-related-to-seaduke/

Liang, H., Li, A., Rugerio, D., Chen, L., & Xu, S. (2023, April 29). What is a DLL. Retrieved 1 October 2023, from https://learn.microsoft.com/en-us/troubleshoot/windows-client/deployment/dynamic-link-library

Malpedia. (2023). Malpedia (Fraunhofer FKIE). Retrieved 11 December 2022, from https://malpedia.caad.fkie.fraunhofer.de/

Malwarebytes. (2023a). Malware. Retrieved 1 October 2023, from https://www.malwarebytes.com/malware

Malwarebytes. (2023b). What is a Keylogger? Retrieved 1 October 2023, from https://www.malwarebytes.com/keylogger

Mandia, K. (2017, March). *Prepared Statement of Kevin Mandia, CEO of FireEye, Inc. Before the United States Senate Select Committee on Intelligence*. Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/os-kmandia-033017.pdf

Mandiant. (2013). *APT1 – Exposing One of China's Cyber Espionage Units*. Retrieved from https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

Mandiant. (2022a). Targeted Attack Lifecycle. Retrieved 1 January 2023, from https://www.mandiant.com/resources/insights/targeted-attack-lifecycle

Mandiant. (2022b). *Assembling the Russian Nesting Doll: UNC2452 Merged into APT29*. Retrieved from https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29

Mehta, N., Leonard, B., & Huntley, S. (2014). *Peering Into the Aquarium: Analysis of a Sophisticated Multi-Stage Malware Family*. Retrieved from https://s3.documentcloud.org/documents/3461560/Google-Aquarium-Clean.pdf

Mell, P., Scarfone, K., & Romanosky, S. (2007). *The common vulnerability scoring system (CVSS) and its applicability to federal agency systems* (No. NIST IR 7435; p. NIST IR 7435). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7435.pdf

Meyers, A. (2016, December 22). Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units. Retrieved 15 January 2023, from https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

Meyers, A. (2020, February 27). Meet The Threat Actors: List of APTs and Adversary Groups. Retrieved 2 January 2023, from https://www.outlookseries.com/A0781/Security/3511.htm

Michael, M. (2020, May 6). Deconstructing the Dukes: A Researcher's Retrospective of APT29. Retrieved 9 November 2022, from https://blog.f-secure.com/podcast-dukes-apt29/

Microsoft. (2016, March 28). Defending against persistent attackers: What we've learned. Retrieved 11 December 2022, from https://www.microsoft.com/en-us/security/blog/2016/03/28/defending-against-persistent-attackers-what-weve-learned/

Microsoft. (2021, March 2). New nation-state cyberattacks. Retrieved 2 January 2023, from: https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

Microsoft. (2023, April 20). How Microsoft names threat actors. Retrieved 15 May 2023, from https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming

Microsoft 365 Defender Team. (2020). *Using Microsoft 365 Defender to protect against Solorigate*. Retrieved from https://www.microsoft.com/en-us/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/#Tracking-the-cross-domain-Solarigate-attack

Microsoft Defender Security Research Team, M. (2018). *Analysis of cyberattack on U.S. think tanks, non-profits, public sector by unidentified attackers*. Retrieved from https://www.microsoft.com/en-us/security/blog/2018/12/03/analysis-of-cyberattack-on-u-s-think-tanks-non-profits-public-sector-by-unidentified-attackers/

Microsoft Digital Security Unit. (2022). *An overview of Russia's cyberattack activity in Ukraine*. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Microsoft, M. (2020). *Customer Guidance on Recent Nation-State Cyber Attacks*. Retrieved from https://msrc.microsoft.com/blog/2020/12/customer-guidance-on-recent-nation-state-cyber-attacks/

Microsoft Security Response Center. (2021). *New Nobelium Activity*. Retrieved from https://msrc.microsoft.com/blog/2021/06/new-nobelium-activity/

Microsoft Threat Intelligence Center. (2020a, September 10). STRONTIUM: Detecting new patterns in credential harvesting. Retrieved 14 February 2023, from https://www.microsoft.com/en-us/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/

Microsoft Threat Intelligence Center. (2020b). *Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers*. Retrieved from https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

Microsoft Threat Intelligence Center. (2021a). *NOBELIUM targeting delegated administrative privileges to facilitate broader attacks*. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/

Microsoft Threat Intelligence Center. (2021b). *New sophisticated email-based attack from NOBELIUM*. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

Microsoft Threat Intelligence Center. (2021c). *Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop*. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Microsoft Threat Intelligence Center. (2021d). *Breaking down NOBELIUM's latest early-stage toolset*. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

Microsoft Threat Intelligence Center. (2022). *MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone*. Retrieved from https://www.microsoft.com/en-us/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/

Mihaiuc, A., Kim, L., & Kasprzyk, P. (2023, March 30). PsExec. Retrieved 1 October 2023, from https://learn.microsoft.com/en-us/sysinternals/downloads/psexec

Minhas, S. (2022, April 7). What is UEFI. Retrieved 1 October 2023, from https://www.onmsft.com/how-to/what-is-uefi-and-what-is-bios/

Mite, V. (2007, May 30). Estonia: Attacks Seen As First Case Of 'Cyberwar'. *Radio Free Europe/Radio Liberty*. Retrieved from https://www.rferl.org/a/1076805.html

MITRE. (2019a, July 19). Credential Access, Tactic TA0006—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0006/

MITRE. (2019b, July 19). Initial Access, Tactic TA0001—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0001/

MITRE. (2019c, July 19). Execution, Tactic TA0002—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0002/

MITRE. (2019d, July 19). Persistence, Tactic TA0003—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0003/

MITRE. (2019e, July 19). Defense Evasion, Tactic TA0005—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0005/

MITRE. (2019f, July 19). Discovery, Tactic TA0007—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0007/

MITRE. (2019g, July 19). Lateral Movement, Tactic TA0008—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0008/

MITRE. (2019h, July 19). Collection, Tactic TA0009—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0009/

MITRE. (2019i, July 19). Command and Control, Tactic TA0011—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0011/

MITRE. (2019j, July 19). Exfiltration, Tactic TA0010—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0010/

MITRE. (2019k, July 25). Impact, Tactic TA0040—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0040/

MITRE. (2020a). Protocol Tunneling, Technique T1572—Enterprise | MITRE ATT&CK®. Retrieved 1 October 2023, from https://attack.mitre.org/techniques/T1572/

MITRE. (2020b, October 18). Reconnaissance, Tactic TA0043—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0043/

MITRE. (2020c, September 30). Resource Development, Tactic TA0042—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0042/

MITRE. (2021, January 6). Privilege Escalation, Tactic TA0004—Enterprise | MITRE ATT&CK®. Retrieved 12 November 2022, from https://attack.mitre.org/tactics/TA0004/

MITRE. (2022a). Process Injection: Dynamic-link Library Injection. Retrieved 1 October 2023, from https://attack.mitre.org/techniques/T1055/001/

MITRE. (2022b). MITRE ATT&CK®—ATT&CK Matrix. Retrieved 12 November 2022, from https://attack.mitre.org/

MITRE. (2022c). APT28, IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Group G0007 | MITRE ATT&CK®. Retrieved 11 December 2022, from https://attack.mitre.org/groups/G0007/

MITRE. (2023a). Pre-OS Boot: Bootkit. Retrieved 1 October 2023, from https://attack.mitre.org/techniques/T1542/003/

MITRE. (2023b). Brute Force, Technique T1110—Enterprise | MITRE ATT&CK®. Retrieved 1 October 2023, from https://attack.mitre.org/techniques/T1110/

MITRE. (2023c). Hijack Execution Flow: DLL Search Order Hijacking. Retrieved 1 October 2023, from https://attack.mitre.org/techniques/T1574/001/

MITRE. (2023d). Hijack Execution Flow: DLL Side-Loading. Retrieved 1 October 2023, from https://attack.mitre.org/techniques/T1574/002/

MITRE. (2023e). Steal or Forge Kerberos Tickets: Kerberoasting. Retrieved 1 October 2023, from https://attack.mitre.org/techniques/T1558/003/

MITRE. (2023f). OS Credential Dumping: LSASS Memory. Retrieved 1 October 2023, from https://attack.mitre.org/techniques/T1003/001/

MITRE. (2023g). Brute Force: Password Spraying. Retrieved 1 October 2023, from https://attack.mitre.org/techniques/T1110/003/

MITRE. (2023h). Process Injection, Technique. Retrieved 1 October 2023, from https://attack.mitre.org/techniques/T1055/

MITRE. (2023i). October 2023 (v14) ATT&CK release update | MITRE ATT&CK®. Retrieved 3 November 2023, from https://attack.mitre.org/resources/updates/updates-october-2023/

MITRE. (2023j). Who We Are. Retrieved 1 October 2023, from https://www.mitre.org/who-we-are

Modderkolk, H. (2018, January 25). Dutch agencies provide crucial intel about Russia's interference in US-elections. *de Volkskrant*. Retrieved from https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/

Morgan, R., & Kelly, D. (2019). A Novel Perspective on Cyber Attribution. *International Conference on Cyber Warfare and Security*, 609-617,XII. Reading, United Kingdom: Academic Conferences International Limited. Retrieved from https://www.proquest.com/docview/2198532101/abstract/36F1BDDD4892458APQ/1

Mozilla. (2023, October 3). What is JavaScript? - Learn web development | MDN. Retrieved 22 October 2023, from https://developer.mozilla.org/en-US/docs/Learn/JavaScript/First_steps/What_is_JavaScript

Mudrinich, E. M. (2012). Cyber 3.0: The Department of Defense strategy for operating in cyberspace and the attribution problem. *Air Force Law Review*, *68*, 167–207. Gale Academic OneFile, https://link.gale.com/apps/doc/A297309173/AONE?u=anon~ec7bfd0c&sid=googleScholar&xid=9806f9c0

Mueller, R. S. (2018). *United States of America v. Viktor Borisovich Netyksho [and 11 others]*. Retrieved from https://www.justice.gov/file/1080281/download

Mueller, R. S. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Retrieved from https://www.justice.gov/archives/sco/file/1373816/download

Nafisi, R. (2021). *FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor*. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/

Nafisi, R., & Lelli, A. (2021). *GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's layered persistence*. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

National Cyber Security Centre UK. (2017). *Turla group using Neuron and Nautilus tools alongside Snake malware*. Retrieved from https://www.ncsc.gov.uk/static-assets/documents/Turla%20group%20using%20Neuron%20and%20Nautilus%20tools%20alongside%20Snake%20malware_1.pdf

National Cyber Security Centre UK. (2018, October 3). Reckless campaign of cyber attacks by Russian military intelligence service exposed. Retrieved 30 October 2022, from https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

National Cyber Security Centre UK. (2020). *Advisory: APT29 targets COVID-19 vaccine development*. Retrieved from https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

National Cyber Security Centre UK, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Security Agency. (2021). *Advisory: Further TTPs associated with SVR cyber actors*. Retrieved from https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf

National Security Agency, Cybersecurity & Infrastructure Security Agency, & Federal Bureau of Investigation. (2021). *Russian SVR Targets U.S. and Allied Networks*. Retrieved from https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

National Security Agency, Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, & National Cyber Security Centre UK. (2021). *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*. Retrieved from https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

National Security Agency, & Federal Bureau of Investigation. (2020). *Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware*. Retrieved from https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

National Security Agency, & National Cyber Security Centre UK. (2019). *Turla Group Exploits Iranian APT To Expand Coverage Of Victims*. Retrieved from https://media.defense.gov/2019/Oct/18/2002197242/-1/-1/0/NSA_CSA_Turla_20191021%20ver%204%20-%20nsa.gov.pdf

NIST. (2011). *Managing information security risk: Organization, mission, and information system view* (No. NIST SP 800-39; p. NIST SP 800-39). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

NIST, J. T. F. T. I. (2012). *Guide for conducting risk assessments* (No. NIST SP 800-30r1; p. NIST SP 800-30r1). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Niu, W., Zhan, X., Li, K., Yang, G., & Chen, R. (2016). *Modeling Attack Process of Advanced Persistent Threat* (Vol. 10066). https://doi.org/10.1007/978-3-319-49148-6_32

Office of Information Security Securing One HHS, & Health Sector Cybersecurity Coordination Center. (2022). *Major Cyber Organizations of the Russian Intelligence Services*. Retrieved from https://www.hhs.gov/sites/default/files/major-cyber-orgs-of-russian-intelligence-services.pdf

Okta. (2023). What Is Token-Based Authentication? Retrieved 1 October 2023, from https://www.okta.com/identity-101/what-is-token-based-authentication/

Oosthoek, K., & Doerr, C. (2021). Cyber Threat Intelligence: A Product Without a Process? *International Journal of Intelligence and CounterIntelligence*, *34*(2), 300–315. https://doi.org/10.1080/08850607.2020.1780062

Pahi, T., & Skopik, F. (2019). *Cyber Attribution 2.0: Capture the False Flag*. Retrieved from https://www.semanticscholar.org/paper/Cyber-Attribution-2.0%3A-Capture-the-False-Flag-Pahi-Skopik/5e818ea9b2c7c93b04c9f41c9fab113b8035d56d

PDQ. (2023). What is a network domain? Retrieved 1 October 2023, from https://www.pdq.com/sysadmin-glossary/network-domain/

Polish Military Counterintelligence Service, & CERT-PL. (2023). *Espionage campaign linked to Russian intelligence services*. Retrieved from https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services

Pols, P. (2018). *Modeling Fancy Bear Cyber Attacks: Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks*. Retrieved from https://hdl.handle.net/1887/64569

Pols, P. (2022). *The Unified Kill Chain -Raising resilience Against Advanced Cyber Attacks*. Retrieved from https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

PwC. (2020). *How WellMess malware has been used to target COVID-19 vaccines*. Retrieved from https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html

QiAnXin Technology. (2022). *Abused Slack service: Analysis of APT29's attack activities against Italy*. Retrieved from https://ti.qianxin.com/blog/articles/analysis-of-apt29%27s-attack-activities-against-italy/

Raiu, C., Soumenkov, I., Baumgartner, K., & Kamluk, V. (2013). *The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor*. Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08083618/themysteryofthepdf0-dayassemblermicrobackdoor.pdf

Ramakrishna, S. (2021). *An Investigative Update of the Cyberattack*. Retrieved from https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000173994221000076/swi-20210507.htm

Rascagnères, P. (2014, November 11). The Uroburos case: New sophisticated RAT identified. Retrieved 30 June 2023, from https://www.gdatasoftware.com/blog/2014/11/23937-the-uroburos-case-new-sophisticated-rat-identified

Recorded Future, I. G. (2022). *SOLARDEFLECTION C2 Infrastructure Used by NOBELIUM in Company Brand Misuse*. Retrieved from https://go.recordedfuture.com/hubfs/reports/cta-2022-0503.pdf

Recorded Future, I. G. (2023). *BlueBravo Uses Ambassador Lure to Deploy GraphicalNeutrino Malware*. Retrieved from https://go.recordedfuture.com/hubfs/reports/cta-2023-0127.pdf

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Romanosky, S., & Boudreaux, B. (2019). *Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government*. 38. https://doi.org/10.1080/08850607.2020.1783877

Sadowski, J., & Hall, R. (2022, March 4). Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation. Retrieved 15 January 2023, from https://www.mandiant.com/resources/blog/russia-invasion-ukraine-retaliation

Sakaguchi, Y. (2021, May 16). Japan lashes out against alleged Chinese military cyberattacks. Retrieved 30 October 2022, from https://asia.nikkei.com/Business/Technology/Japan-lashes-out-against-alleged-Chinese-military-cyberattacks

SANS. (2022). Cyber Threat Intelligence Training | SANS FOR578. Retrieved 18 December 2022, from https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/

Satter, R. (2018, June 12). Russian hackers posed as IS to threaten military wives. *Chigago Tribune*. Retrieved from https://web.archive.org/web/20180612141330/http://www.chicagotribune.com/news/sns-bc-eu--russian-hackers-spouses-20180508-story.html

Secureworks. (2023). IRON RITUAL. Retrieved 16 May 2023, from https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/iron-ritual

Secureworks, C. T. U. (2016, June 16). Threat Group 4127 Targets Hillary Clinton Presidential Campaign. Retrieved 8 January 2023, from https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign

Secureworks, C. T. U. (2017, March 30). IRON TWILIGHT Supports Active Measures. Retrieved 8 January 2023, from https://www.secureworks.com/research/iron-twilight-supports-active-measures

SecurityScorecard. (2022, September 27). A Deep Dive Into the APT28's stealer called CredoMap. Retrieved 30 July 2023, from https://securityscorecard.com/research/apt28s-stealer-called-credomap/

Sekoia.io. (2023). APT29 aka Nobelium, Cozy Bear. Retrieved 18 May 2023, from https://www.sekoia.io/en/glossary/apt29-aka-nobelium-cozy-bear/

Sherstobitoff, R., & Rea, M. (2017). *Threat Group APT28 Slips Office Malware into Doc Citing NYC Terror Attack*. Retrieved from https://www.mcafee.com/blogs/other-blogs/mcafee-labs/apt28-threat-group-adopts-dde-technique-nyc-attack-theme-in-latest-campaign/

Shevchenko, S. (2008, November 30). Agent.btz—A Threat That Hit Pentagon. Retrieved 30 June 2023, from http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html

Singer, J. D. (1958). Threat-perception and the armament-tension dilemma. *Journal of Conflict Resolution*, *2*(1), 90–105. https://doi.org/10.1177/002200275800200110

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford ; New York: Oxford University Press.

Smith, L., Leathery, J., & Read, B. (2021). *New SUNSHUTTLE Second-Stage Backdoor Uncovered Targeting U.S. Based Entity; Possible Connection to UNC2452*. Retrieved from https://www.mandiant.com/resources/blog/sunshuttle-second-stage-backdoor-targeting-us-based-entity

Smith, L., & Read, B. (2017). *APT28 Targets Hospitality Sector, Presents Threat to Travelers*. Retrieved from https://www.mandiant.com/resources/blog/apt28-targets-hospitality-sector-presents-threat-travelers

Steffens, T. (2020). *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage*. Springer Vieweg.

Stoll, C. (1998). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Pocket Books. Retrieved from https://www.amazon.com/Cuckoos-Egg-Tracking-Computer-Espionage/dp/1416507787

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Adam G., P., & Thomas, C. B. (2020). *MITRE ATT&CK: Design and Philosophy*. Retrieved from https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Suiche, M. (2017, June 15). Lessons from TV5Monde 2015 Hack. Retrieved 8 January 2023, from https://medium.com/comae/lessons-from-tv5monde-2015-hack-c4d62f07849d

Suojelupoliisi. (2021). APT-operaatiot. Retrieved 8 November 2022, from https://supo.fi/en/apt-operations

Symantec. (2016). *The Waterbug attack group*. Retrieved from https://docs.broadcom.com/doc/waterbug-attack-group

Symantec. (2017). *'Forkmeiamfamous': Seaduke, latest weapon in the Duke armory*. Retrieved from https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/Forkmeiamfamous_SeaDuke.pdf

Symantec. (2019, June 20). Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments. Retrieved 30 June 2023, from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/waterbug-espionage-governments

Symantec, T. H. T. (2021a). *SolarWinds: How a Rare DGA Helped Attacker Communications Fly Under the Radar*. Retrieved from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-unique-dga

Symantec, T. H. T. (2021b). *Raindrop: New Malware Discovered in SolarWinds Investigation*. Retrieved from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware

Tanase, S. (2015). *Satellite Turla: APT Command and Control in the Sky*. Retrieved from https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon*, *7*(1), e05969. https://doi.org/10.1016/j.heliyon.2021.e05969

Techslang. (2019). What is a Scripting Language (Script)? Retrieved 1 October 2023, from https://www.techslang.com/definition/what-is-a-scripting-language-script/

Telsy. (2020). *Turla / Venomous Bear updates its arsenal: 'NewPass' appears on the APT threat scene*. Retrieved from https://www.telsy.com/turla-venomous-bear-updates-its-arsenal-newpass-appears-on-the-apt-threat-scene/

The Tor Project. (2023). The Tor Project | Privacy & Freedom Online. Retrieved 1 October 2023, from https://torproject.org

The United States Department of Justice. (2014, May 19). U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. Retrieved 11 December 2022, from https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

The United States Department of Justice. (2018, July 13). Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election. Retrieved 11 December 2022, from https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

Tivadar, M., BALÁZS, B., & Istrate, C. (2013). *A Closer Look at MiniDuke*. Retrieved from https://samples.vx-underground.org/root/APTs/2013/2013.04.21%20-%20A%20Closer%20Look%20at%20Miniduke/Paper/Mini%20Duke.pdf

Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. Retrieved from https://www.theguardian.com/world/2007/may/17/topstories3.russia

Trend Micro. (2015). *An In-Depth Look at How Pawn Storm's Java Zero-Day Was Used*. Retrieved from https://samples.vx-underground.org/root/APTs/2015/2015.07.14%20-%20An%20In-Depth%20Look%20at%20How%20Pawn%20Storm%E2%80%99s%20Java%20Zero-Day%20Was%20Used/Paper/How%20pawn%20storms%20java%20zero%20day%20was%20used.pdf

Trend Micro. (2020). *Pawn Storm in 2019: A Year of Scanning and Credential Phishing on High-Profile Targets*. Retrieved from https://documents.trendmicro.com/assets/white_papers/wp-pawn-storm-in-2019.pdf

Trend Micro. (2023). Trend Micro: Exploit—Definition. Retrieved 1 October 2023, from https://www.trendmicro.com/vinfo/us/security/definition/exploit

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, *17*(2), 229–244. https://doi.org/10.1093/jcsl/krs019

United States Department of Homeland Security, & Federal Bureau of Investigation. (2016). *GRIZZLY STEPPE – Russian Malicious Cyber Activity*. Retrieved from https://www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Unterbrink, H. (2021, September 21). TinyTurla—Turla deploys new malware to keep a secret backdoor on victim machines. Retrieved 30 June 2023, from https://blog.talosintelligence.com/tinyturla/

U.S General Services Administration. (2022, July). GSA's Advanced Persistent Threat (APT) Buyer's Guide. Retrieved 8 November 2022, from https://buy.gsa.gov/interact/community/138/activity-feed/post/b4d05f8f-3054-437e-9587-eccc079f1d2c/GSA_s_Advanced_Persistent_Threat_APT_Buyer_s_Guide

Välisluureamet. (2018). *International Security And Estonia 2018*. Retrieved from https://www.valisluureamet.ee/doc/raport/2018-en.pdf

Van Geluwe De Berlaere, T. (2022). *They See Me Roaming: Following APT29 by Taking a Deeper Look at Windows Credential Roaming*. Retrieved from https://www.mandiant.com/resources/blog/apt29-windows-credential-roaming

Vanderlee, K. (2020). DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors. Retrieved 2 January 2023, from https://www.mandiant.com/resources/blog/how-mandiant-tracks-uncategorized-threat-actors

Vatanen, V. (2020). *Venäjän lähialueillaan toteuttamien kyberoperaatioiden analysointi*. Retrieved from https://jyx.jyu.fi/handle/123456789/69032

Vogler, S., & Connell, M. (2016). *Russia's Approach to Cyber Warfare*. Retrieved from https://apps.dtic.mil/sti/citations/AD1019062

Warner, C. (2021, December 17). Diamond Model in Cyber Threat Intelligence. Retrieved 18 December 2022, from https://warnerchad.medium.com/diamond-model-for-cti-5aba5ba5585

Wen, S., He, N., & Yan, H. (2017). Detecting and Predicting APT Based on the Study of Cyber Kill Chain with Hierarchical Knowledge Reasoning. *Proceedings of the 2017 VI International Conference on Network, Communication and Computing*, 115–119. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3171592.3171641

Wheeler, D., & Larsen, G. (2003). *Techniques for Cyber Attack Attribution*. 82. IDA Paper P-3792. Institute for Defense Analyses, Alexandria, Virginia.

Wheeler, S., & Buck, A. (2023, June 28). What is PowerShell? - PowerShell. Retrieved 1 October 2023, from https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.3

White, S., Simpson, D., Sharkey, K., Coulter, D., Batchelor, D., Jacobs, M., & Satran, M. (2023, March 8). Windows Management Instrumentation—Win32 apps. Retrieved 1 October 2023, from https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Wiedemar, S. (2023). *NATO and Article 5 in Cyberspace*. 4 p. https://doi.org/10.3929/ETHZ-B-000610328

Williams, C. (2007). Research Methods. *Journal of Business & Economics Research (JBER)*, *5*(3). https://doi.org/10.19030/jber.v5i3.2532

Wolfram, J., Hawley, S., McLellan, T., Simonian, N., & Vejlby, A. (2022). *Trello From the Other Side: Tracking APT29 Phishing Campaigns*. Retrieved from https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown.

Zettl-Schabath, K., Bund, J., Timothy, G., & Borrett, C. (2023). *ADVANCED PERSISTENT THREAT profile: APT29 – Stealth at scale*. Retrieved from

https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_APT_29_d9cee0efa4.pdf

APPENDIX 1 ADDITIONAL KILL CHAIN REFERENCES

TABLE 4 Additional kill chain references

Kill chain	Reference	Description
C1-1	ESET, 2018a	Spear phishing attack conducted by APT28 using the Sednit malware ecosystem.
C1-2	Kharouni et al., 2014	Spear phishing campaign conducted by APT28.
C1-3	Jazi & Santos, 2022	Malicious document attributed to APT28 and the attack that was conducted with it.
C1-4	Smith & Read, 2017	Spear phishing campaign conducted by APT28 with GAMEFISH.
C1-5	Creus, Halfpop, & Falcone, 2016	Malware connected to APT28 and its capabilities.
C1-6	Lee, Harbison, & Falcone, 2018	Spear phishing campaign conducted by APT28 with SofacyCarberp.
C1-7	Lee & Falcone, 2018	Spear phishing campaign conducted by APT28 with Zebrocy.
C1-8	Anthe et al., 2015 [p.4]	Spear phishing attack conducted by APT28 leading to a watering hole attack.
C1-9	Mueller, 2018 [p.6]	Spear phishing attack conducted by APT28 leading to credential access.
C1-10	Falcone & Lee, 2016	Spear phishing campaign conducted by APT28 with Carberp.
C1-11	ESET, 2016 [p.18]	Spear phishing attack conducted by APT28 with Seuploader.
C1-12	ESET, 2016 [p.20]	Spear phishing attack conducted by APT28 leading to a watering hole attack with Seuploader.
C1-13	ESET, 2019	Spear phishing campaign conducted by APT28.
C2-1	Raiu, Soumenkov, Baumgartner, & Kamluk, 2013	Spear phishing attack conducted by APT29 using Miniduke.
C2-2	Wolfram, Hawley, McLellan, Simonian, & Vejlby, 2022	Spear phishing campaign conducted by APT29 using ROOTSAW (EnvyScout).
C2-3	Harbison & Renals, 2022	Spear phishing campaign by APT29 using EnvyScout.
C2-4	F-Secure, 2015b	Spear phishing attack conducted by APT29 using CozyDuke.
C2-5	Faou, Tartare, & Dupuy, 2019 [p. 12]	Spear phishing campaign conducted by APT29 using MiniDuke.
C2-6	Microsoft 365 Defender Team, 2020	Supply chain attack conducted by APT29 using Solorigate (SUNBURST).
C2-7	Microsoft Threat Intelligence Center, 2021d	Spear phishing attack conducted by APT29 using EnvyScout.
C2-8	Cash et al., 2021	Spear phishing campaign conducted by APT29.
C2-9	QiAnXin Technology, 2022	Spear phishing attack conducted by APT29 using EnvyScout.
C2-10	Tivadar, BALÁZS, & Istrate, 2013	Spear phishing attack conducted by APT29 using MiniDuke.

C2-11	Microsoft Defender Security Research Team, 2018	Spear phishing attack conducted by APT29 leading to malicious download.
C2-12	Microsoft Threat Intelligence Center, 2021b,	Spear phishing campaign conducted by APT29.
C2-13	ESET, 2014b	Spear phishing attack conducted by APT29 using MiniDuke.
C3-1	Kaspersky Labs, 2014a	Spear phishing campaign conducted by Turla using malicious PDF files.
C3-2	Kaspersky Labs, 2014a	Spear phishing campaign conducted by Turla using malicious installers.
C3-3	Kaspersky Labs, 2014a	Watering hole campaign conducted by Turla leading to exploits.
C3-4	Kaspersky Labs, 2014a	Watering hole campaign conducted by Turla leading to malicious installers.
C3-5	Symantec, 2016 [p. 5]	Spear phishing campaign conducted by Turla using malicious PDF files.
C3-6	Symantec, 2016 [p. 6]	Watering hole campaign conducted by Turla leading to malicious installers.
C3-7	Symantec, 2016 [p. 17]	Watering hole campaign conducted by Turla leading to exploits.
C3-8	GovCERT.ch, 2016 [p. 8]	Watering hole campaign conducted by Turla leading to malicious installers.
C3-9	GovCERT.ch, 2016 [p. 8]	Watering hole campaign conducted by Turla leading to exploits.
C3-10	Kaspersky Labs, 2019	Attack mimicking a supply chain attack by Turla with malicious installers.
C3-11	Faou, 2020c	Watering hole campaign conducted by Turla leading to malicious installers.
C3-12	Hawley, Roncone, McLellan, Mattos, & Wolfram, 2023	Turla registering a domain name used by a commodity malware to attack its victims.
C3-13	Boutin, 2017	Watering hole campaign conducted by Turla leading to malicious installers.