Author(s): Lehto, Martti

Title: APT Cyber-attack Modelling : Building a General Model

Year: 2022

Version: Published version

Please cite the original version:

Lehto, M. (2022). APT Cyber-attack Modelling : Building a General Model. In R. P. Griffin, U. Tatarand, & B. Yankson (Eds.), ICCWS 2022 : Proceedings of the 17th International Conference on Cyber Warfare and Security (17, pp. 121-129). Academic Conferences International Ltd. The proceedings of the 17th international conference on cyber warfare and security. https://doi.org/10.34190/iccws.17.1.36

APT cyber-attack modelling - building a general model

Martti Lehto
University of Jyväskylä, Finland
martti.j.lehto@jyu.fi

Abstract: The global community continues to experience an increase in the scale, sophistication, and successful perpetration of cyber-attacks. As the quantity and value of electronic information have increased, so too have the efforts of criminals and other malicious actors who have embraced the Internet as a more anonymous, convenient, and profitable way of carrying out their activities. The systems are attacked more and more by single or multiple hacktivists, state sponsored hackers, cyber criminals, cyber terrorists, cyber spies, or cyber warfare warfighters. The cyber security approach requires a balance of cyber threat intelligence, real time cyber-attack detection and especially the cyber early warning ability. Threats in cyberspace are difficult to define, as it is hard to identify the source of attacks and the motives that drive them, or even to foresee the course of an attack as it unfolds. The identification of cyber threats is further complicated by the difficulty in defining the boundaries between national, international, public, and private interests. Because threats in cyberspace are global in nature and involve rapid technological developments, the struggle to respond them is ever-changing and increasingly complicated. Cyber-attack models describe the structure of an attack in different phases. They provide a means to conceptualize the different aspects and elements of an attack. However, it is important to understand that not all attacks must complete all phases to be successful, and the objective of the attack defines the structure of the attack. Different actors have built different cyber-attack models. Modeling is used to understand the different goals of cyber attackers. Attack models are based on attack targets and attack objectives. This paper analyzes different APT cyber-attack models and presents a general cyber-attack model.

Keywords: cyber security, cyber-attack model, ATP attack

1. Introduction

Attack models describe the structure of an attack in different phases. They provide a means to conceptualize the different aspects of an attack. However, it is important to understand that not all attacks must complete all phases to be successful. In fact, many attacks iterate recursively through the phases of an attack model.

The models have been developed based on the motives and objectives of various cyber-attacks. Cyber-attacks are often divided four categories based on the attack objective and target: APT-attack, Cyber-Physical Attack against Critical Infrastructure, Data breach attack, and Military Cyberspace Operations.

The objective of this paper is to define the general cyber-attack model in an APT-threat context. Section 2 explains into ATP attack essence and in Section 3 is describing existing ATP attack models. Section 4 addresses general cyber-attack modeling., followed by a discussion of the relevance of the modelling of the cyber-attacks.

2. APT attack essence

An Advanced Persistent Threat (APT) is a stealthy computer network threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. In recent times, the term may also refer to non-state sponsored groups conducting large-scale targeted intrusions for specific goals. APT is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time. Normally APT attacks are initiated to steal data rather than cause damage to the target organization's network (Fire Eye, 2021).

The goal of most APT attacks is to achieve and maintain ongoing access to the targeted network rather than to get in and out as quickly as possible. The attackers use a great deal of effort and resources to carry out APT attacks, and they typically select high-value targets. The targets of APT attack include large organizational networks that contain valuable secret information. APT attacks can be defined as action aimed at acquiring secret information (sensitive, proprietary, or classified) from competitors, groups, governments, and adversaries for political, military, or financial gain by using special methods on the Internet, in networks, programs or computers (Liaropoulos 2010); Segal, 2019).

Executing an APT attack requires a higher degree of customization and sophistication than a traditional attack. APT groups are a nation state or state-sponsored who have advanced devices and are already financially

covered. Several effective APT groups have been identified from Russia and China. Advanced APT attack operations will remain secret for several years. Table 1 illustrates this detection problem with a few examples.

Table 1: Apt attack operations

APT operation	Targets	Year of detection	In operational use since
Operation Aura	Dozens of IT organizations (Google among others) specially in US.	2010	2009
Operation Shady RAT	More than 70 companies and government entities around the world.	2011	2007
Duqu	Information from industrial control systems.	2011	2007
sKyWIper/Flame	The Middle East governmental organizations, educational institutions, and individuals.	2012	2008
NetTraveler	More than 350 organizations in 40 countries	2013	2004
Regin	Several organizations at least 14 countries like small businesses and telecom companies.	2014	2008, first sample 2003
Remsec (Project Sauron)	More than 30 organizations in Russia, Iran, China: government, scientific research centers, military, telecommunication providers and finance.	2016	2011

3. ATP-attack models

The APTs are flexible and sophisticated. Skilled and determined cyber attacker can use multiple vectors and entry points to navigate around defenses, breach the network in minutes and evade detection for months or even years. The process by which sophisticated cyber-attacks are conducted can be described as a lifecycle. Due to the diversity of APT attacks, several models have been developed:

1. MITRE ATT&CK
2. Mandiant Attack Lifecycle Model
3. LM Cyber Kill Chain, CKC
4. Unified Kill Chain, UKC
5. Hybrid Cyber Kill Chain, HCKC

3.1 MITRE ATT&CK

MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. The aim of the framework is to improve post-compromise detection of adversaries in enterprises by illustrating the actions an attacker may have taken (MITRE, 2021).

The model has two main phases. Pre-phase covering preparatory techniques: reconnaissance and weaponization. Adversary pre-phase activities are largely executed outside the organizations' field of view, making them more difficult to detect. In the second phase, the attack phase itself is modeled. The framework consists of 11 tactics and one objective of the mission (MITRE, 2021).

1. Initial Access: The adversary is trying to get into your network.
2. Execution: The adversary is trying to run malicious code.
3. Persistence: The adversary is trying to maintain their foothold.
4. Privilege Escalation: The adversary is trying to gain higher-level permissions.
5. Defense Evasion: The adversary is trying to avoid being detected.
6. Credential Access: The adversary is trying to steal account names and passwords.
7. Discovery: The adversary is trying to figure out your environment.
8. Lateral Movement: The adversary is trying to move through your environment.
9. Collection: The adversary is trying to gather data of interest to their goal.
10. Command and Control: The adversary is trying to communicate with compromised systems to control them.
11. Exfiltration: The adversary is trying to steal data.
12. Impact: The adversary is trying to manipulate, interrupt, or destroy your systems and data.

MITRE ATT&CK was created in 2013 to improve post-compromise detection of threats through telemetry sensing and behavioral analysis. ATT&CK is also used as a tool to categorize adversary behavior (McAfee, 2021).

3.2 Mandiant Attack Lifecycle Model

APT attacks fit into a cyclic pattern of activities that the framework of Mandiant's Attack Lifecycle model describes. The stages between "Establish Foothold" and "Complete Mission" do not have to occur in this order every time. In fact, once established within a network, APT groups will continually repeat the cycle of conducting reconnaissance, identifying data of interest, moving laterally to access that data, and "completing mission" by stealing the data. This will generally continue indefinitely until they are removed entirely from the network (IACP, 2021; Parrend et al, 2018).

The model consists of eight stages:

1. Initial Reconnaissance: The attacker conducts research on a target. The attacker identifies targets (both systems and people) and determines his attack methodology.
2. Initial Compromise: The attacker successfully executes malicious code on one or more systems. This most likely occurs through social engineering.
3. Establish Foothold: The attacker ensures he maintains continued control over a recently compromised system. Typically, the attacker establishes a foothold by installing a persistent backdoor or downloading additional utilities or malware to the victim system.
4. Escalate Privileges: The attacker obtains greater access to systems and data. Attackers often escalate their privileges through using vulnerabilities in software and/or hardware.
5. Internal Reconnaissance: The attacker explores the victim's environment to gain a better understanding of the environment, the roles, and responsibilities of key individuals, and to determine where an organization stores information of interest.
6. Move Laterally: The attacker uses his access to move from system to system within the compromised environment.
7. Maintain Presence: The attacker ensures continued access to the environment. Common methods of maintaining a presence include installing multiple variants of malware backdoors or by gaining access to remote access services.
8. Complete Mission: The attacker accomplishes the goal. Once the mission has been completed, most targeted attackers do not leave the environment, but maintain access in case a new mission is directed.

3.3 LM Cyber Kill Chain (CKC)

The Cyber Kill Chain framework is developed by Lockheed Martin for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete to achieve their objective. The seven steps of the Cyber Kill Chain enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques, and procedures (LM, 2021).

1. Reconnaissance: Identify the Targets: The adversaries are in the planning phase of their operation. They conduct research to understand which targets will enable them to meet their objectives.
2. Weaponization: Prepare the Operation: The adversaries are in the preparation and staging phase of their operation. A "weaponizer" couples malware and exploit into a deliverable payload.
3. Delivery: Launch the Operation: The adversaries convey the malware to the target. They have launched their operation: Adversary controlled delivery or adversary released delivery.
4. Exploitation: Gain Access to Victim: The adversaries must exploit a vulnerability to gain access. Zero-day vulnerabilities are exploited in this step.
5. Installation: Establish Beachhead at the Victim: Typically, the adversaries install a persistent backdoor or implant in the victim environment to maintain access for an extended period.
6. Command & Control (C^2): Remotely Control the Implants: Malware opens a command channel to enable the adversary to control the operation.
7. Actions on Objectives: Achieve the Mission's Goal: The attacker accomplishes the mission's goal, like collect and exfiltrate data, destroy systems, overwrite, or corrupt data.

3.4 Unified Kill Chain, UKC

The Unified Kill Chain (UKC) was proposed in 2017 by Paul Pols. Combining elements from both the Cyber Kill Chain and ATT&CK (along with several other models), it divides an attack into 18 separate stages. Its aim is to expand the scope of the Cyber Kill Chain and to represent an improvement over the time-agnostic nature of ATT&CK. UKC model is developed that focuses on the tactics that form the consecutive phases of cyber-attacks. The resulting UKC is a meta model that supports the development of end-to-end attack specific kill chains and actor specific kill chains, that can subsequently be analyzed, compared, and defended against (Pols, 2017; Pols, 2019).

The 18 steps are broadly grouped into three overarching areas. First, the *Initial Foothold* must be gained. This phase covers the steps taken to compromise a single system within a target and includes steps 1-8. In *Network Propagation* the attacker attempts to pivot from their compromised system to other, more important parts of the target's environment. It comprises the steps 9-14. The *Action on Objectives* describes a situation in which the attacker, having found the goal, gains privileged access to a part of critical infrastructure, and performs initially planned task. This could be the exfiltration of sensitive data or its manipulation. It comprises the steps 15-18. (Pols, 2017; Pols, 2019)

The 18 stages of the Unified Kill Chain are (Pols, 2019):

1. Reconnaissance: Researching, identifying, and selecting targets using active or passive reconnaissance.
2. Weaponization: Preparatory activities aimed at setting up the infrastructure required for the attack.
3. Delivery: Techniques resulting in the transmission of a weaponized object to the targeted environment.
4. Social Engineering: Techniques aimed at the manipulation of people to perform unsafe actions.
5. Exploitation: Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
6. Persistence: Any access, action or change to a system that gives an attacker persistent presence on the system.
7. Defense Evasion: Techniques an attacker may specifically use for evading detection or avoiding other defenses.
8. Command & Control: Techniques that allow attackers to communicate with controlled systems within a target network.
9. Pivoting: Tunneling traffic through a controlled system to other systems that are not directly accessible.
10. Discovery: Techniques that allow an attacker to gain knowledge about a system and its network environment.
11. Privilege Escalation: The result of techniques that provide an attacker with higher permissions on a system or network.
12. Execution: Techniques that result in execution of attacker-controlled code on a local or remote system.
13. Credential Access: Techniques resulting in the access of, or control over, system, service or domain credentials.
14. Lateral Movement: Techniques that enable an adversary to horizontally access and control other remote systems.
15. Collection: Techniques used to identify and gather data from a target network prior to exfiltration.
16. Exfiltration: Techniques that result or aid in an attacker removing data from a target network.
17. Impact: Techniques aimed at manipulating, interrupting or destroying the target system or data.
18. Objectives: Socio-technical objectives of an attack that are intended to achieve a strategic goal.

The main advantage of the way the Unified Kill Chain is laid out is in the use of repetition. Whereas the Cyber Kill Chain suggests a step 1, 2, 3 approach to attacking, the Initial Foothold, Network Propagation and Action on Objectives stages of UKC are presented as loops that may, eventually, move on to the next stage. This better captures the actual behavior of an attacker, who is likely to spend a lot of time attempting to gain that initial foothold and comparatively less actually doing what he comes to do (Pols, 2019).

3.5 Hybrid Cyber Kill Chain, HCKC

Zeng and Germanos (2019) constructed a Hybrid Cyber Kill Chain (HCKC) framework. Although LM Cyber Kill Chain has been widely adopted by organizations since it has been published, it has been criticized for its weakness in handling insider threats, because it is too focused on the perimeter and malware prevention. For example, shows that the stages of CKC do not capture all possible attack vectors and are not expressive enough to model internal actions within the target network. Consequently, based on these facts, improvements, and amendments to CKC have been proposed. Some of these proposed extensions try to address the insider's perspective (Zeng and Germanos, 2019).

HCKC framework aims to provide a holistic approach by considering the factors, like the persistence and the lateral movement of the attacker, the defence actions of the defender, and the strength level both attacker and defender. The third factor is embedded in each stage of HCKC after the weaponization. That is because the two first stages are not under the control of the defender. According to this rule, the attacker's strength level must be greater than the one of the defenders to proceed to the next stage in the kill chain (Zeng and Germanos, 2019).

Stage 1 - Reconnaissance: The attackers would gather as much information as possible about target organization. For example: names of the employers, their positions, email addresses and IP addresses.

Stage 2 - Weaponization: The attackers develop exploitation and malware. The attackers might create websites that contain malware and develop malicious software for a specific platform or purpose, which designed according to the vulnerabilities discovered during reconnaissance.

Stage 3 - Delivery: The attackers transmit the malicious code to the target information system. The attacker might use a spear-phishing attack targeting an internal employee of the organization, social engineering, or some vulnerability of the system to deliver the malware.

Stage 4 - Persistence: This stage denotes the attacker's persistence to accomplish an action.

Stage 5 - Exploitation: The attacker utilizing the discovered vulnerabilities, is executing the malicious code on the target network using remote or local mechanisms. The aim is to gain admin access to the target's information system.

Stage 6 - Installation: After the exploitation, the malicious code will install itself onto the target's information system. Then, the malicious code will start downloading additional software when there is available network access.

Stage 7 - Command & Control: The attacker has set up the management and communication code onto the target network. Now, the attacker can fully manage the malicious code and move further into the network, and exfiltrate data.

Stage 8 - Lateral Movement: This stage expresses the move of the attacker to bigger targets using the target network after some of its systems has been compromised.

Stage 9 - Action on Objectives: The actions and objectives of the attacks are dependent on their specific mission (e.g., exfiltrate or conduct disruption or destruction of the data).

Zeng and Germanos (2019) states that HCKC is useful for post-incident analysis of attacks. A formal model of the HCKC can also provide security metrics that can be utilized by system architects to make trade-off decisions involving system security. There is a growing need for efficient and timely incident response. In many cases, the period between detection and response can be months long and can allow adversaries to attain their goals (Zeng and Germanos, 2019).

4. General cyber-attack modelling

Cyber-attack models provide us with a means of decomposing an attack into discrete phases. These in turn can be used to conduct post-intrusion analysis to better predict and avoid future attacks. By understanding the tactics, techniques, and procedures (TTPs) of an attacker, we learn how threat actors operate and have the means to evaluate our defensive posture and develop strategic courses of action to eliminate gaps.

APT cyber-attack models presented above have common elements. The main differences in cyber-attack patterns are due to the level of detail of the attack operation. Some models include only the main components of the attack, while others describe the attack components accurately.

Based on the different ATP attack models, the general model has been developed. Other models do not present an early attack phase, i.e., strategic decision-making, that precedes the actual preparation for an APT attack. Cyber-attack can thus be divided into three main stages: early-attack, pre-attack, and the actual attack operation. Most models recognize pre-attack and attack phases. While most models recognize pre-attack and attack phases, other attack models do not describe very clear the end state phase, i.e., termination of the attack, which addresses the issues such as how the attacker completes the mission and how he covers his tracks. Different cyber-attack models use different terms to describe different stages of an attack.

In the early attack phase the attacker will made the strategic decision of the target and attack objectives. Strategic decisions involve a political problem of reconciling divergent interests as well as a technical problem of attempting to calculate the best decision given several parameters (Child, Elbanna and Rodrigues, 2010). Figure 1 illustrates the general cyber-attack model.

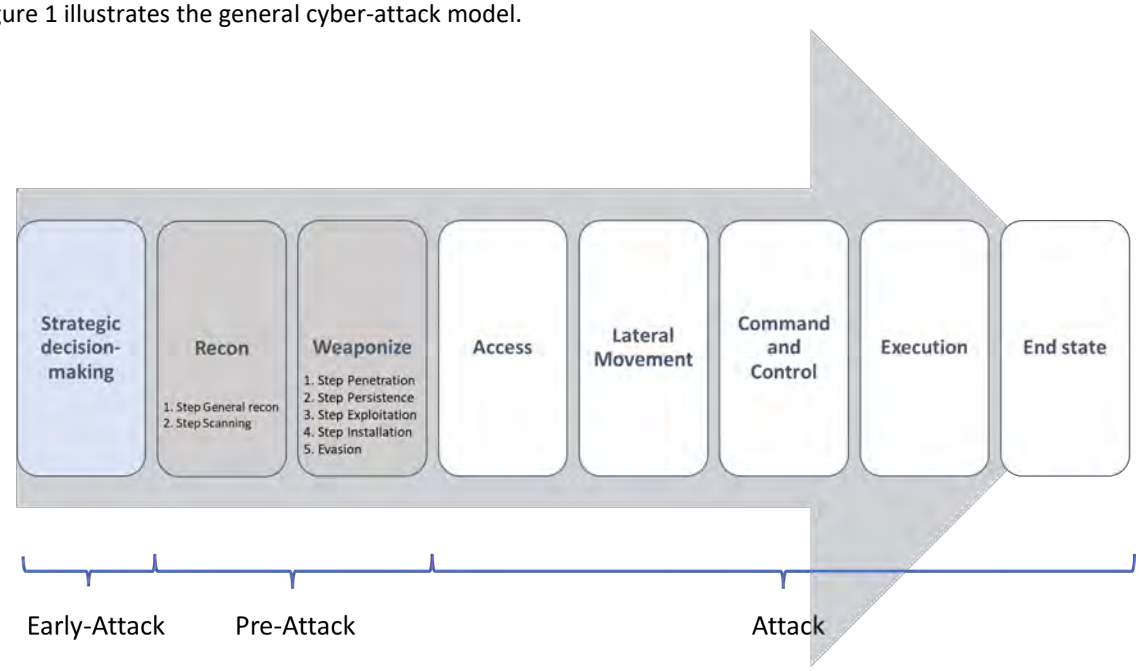

Figure 1: General Cyber-attack model

The table 2 illustrates the phases and steps of the general APT cyber-attack model.

Table 2: General APT cyber-attack model

General APT cyber-attack model	
Early-Attack phase	
Strategic decision-making	In state-sponsored APT attacks, a decision is made at the strategic level on the target of the attack and the objectives of the attack, and how it relates to other strategic objectives.
Pre-Attack phase	
Reconnaissance - target identification - target location - target characteristics	**1st step: General reconnaissance**: attack planners create the situational awareness from the target organization. They conduct research to understand which targets will enable them to meet their objectives. In reconnaissance phase the attacker want to gather as much information as possible about target organization. **2nd step: Scanning**: attacker will be closely examining the system for potential vulnerabilities. The attacker will be scanning for further detailed information from applications, and more specific information from the operating system. The attacker focuses on finding an exposed application that might be particularly interesting in terms of entry.
Weaponize - operation preparing and malware production	In weaponization phase the attackers develop exploitation and malware. The attackers might create websites that contain malware or develop malicious software which designed according to the vulnerabilities discovered during reconnaissance. A weapon designer compiles malware and exploit into a deliverable payload (in-house production). Weapons are also available on the Dark web. For the file-based exploits the designer develops a dropper to hide the real payload. Also, the designer selects backdoor implant and appropriate command and control infrastructure for operation.
Attack phase	
Access - entry to target network - penetration - persistence - exploitation	The access phase represents the methods that attacker uses to penetrate a target organization's network and take it over to execute the operation. The attacker seeks to achieve a main admin authority. This phase is divided five steps. **1st step: Penetration**: Attacker frequently targets individual users within a victim environment. As such, the most observed method of initial compromise is spear phishing. The attacker might

General APT cyber-attack model	
- installation - evasion	use a spear-phishing attack targeting an internal employee of the organization, social engineering, or some vulnerability of the system to deliver the malware. **2nd step: Persistence**: the attacker transmits the malicious code to the target information system and establishes a foothold ensures that APT attack groups can access and control one or more computers within the victim organization from outside the network. Typically, the attacker installs a persistent backdoor or implant in the victim environment to maintain access for an extended period. **3rd step: Exploitation**: the attacker utilizes the discovered vulnerabilities to gain access, executes the malicious code on the target network. The aim is to get administrator rights to the target's information system. Vulnerabilities be found from people, technologies, or processes. The most effective are the zero-day vulnerabilities. **4th step: Installation**: As soon as the exploitation is successful, the malicious code will install itself onto the target's information system. The attacker can maintain continuity of access to the target system by a remote access trojan or creating a backdoor to penetrate further into the target network. **5th step: Evasion**: The attacker is trying to avoid being detected. The attacker tries to stay hidden by carrying out a stealth attack. State-Sponsored Attackers appear to be successful in this regard, as an average APT malware is found after five years of attack.
Lateral Movement - surveillance - environment expanding	In the lateral movement phase the attacker is trying to figure out ICT environment. Also, the attacker tries enlarging attack surface using the target network after some of its systems has been compromised. The attacker tries escalating privileges involves acquiring items that will allow access to more resources within the victim environment.
Command and Control - attack management - maintain presence	In the command and control (C^2) phase the attacker will set up the management and communication code onto the target network. Then the attacker can manage the malware and move further into the network and execute the operation. In this phase, the attacker takes actions to ensure continued control over key systems in the network environment from outside of the network.
Execution - data collection - data exfiltration - data manipulation	In the execution phase the attacker executes the mission = action on objectives. The actions and objectives of the attacks are dependent on their specific mission: data collection and exfiltration, data manipulation (corruption) or data overwriting. The main goal of APT attack is to steal data, including intellectual property, business contracts or negotiations, secret policy and military papers and information etc. Today, data manipulation is considered one of the most dangerous attacks.
End state - termination of the attack	When the attack objectives are accomplished, the attacker disappears unnoticed. The attacker tries to clean-up all traces from the "visiting" in the ICT system. "Mission accomplished in stealth." If the APT attack involved a silent data exfiltration which was not detected, attackers will remain inside the network and wait for additional attack opportunities. Over time they may collect additional sensitive data and repeat the process. They will also aim to create backdoors that are difficult to detect, so even if they are caught, they can regain access to the system in the future.

Different cyber-attack models use different terms to describe different stages of an attack. At a high level of abstraction, different cyber-attack models contain almost identical steps. But there are also differences in definitions and descriptions of steps. Table 3 shows five APT attack models combined in a general model.

Table 3: APT-attack models versus general model

General Modell	MITRE ATT&CK	Mandiant Attack Lifecycle Model	LM Cyber Kill Chain, CKC	Unified Kill Chain, UKC	Hybrid Cyber Kill Chain, HCKC
Early Attack					
Strategic decision-making					
Pre-Attack					
Reconnaissance - target identification - target location - target characteristics	1. Reconnaissance	1. Initial reconnaissance	1. Reconnaissance	1. Reconnaissance	1. Reconnaissance
Weaponize - operation preparing and malwares	2. Weaponization		2. Weaponization	2. Weaponization	2. Weaponization
Attack					
Access - entry to target network - penetration - persistence - exploitation - installation - evasion	3. Initial access 4. Execution 5. Persistence 6. Privilege escalation 7. Defense evasion 8. Credential access 9. Discovery	2. Initial compromise 3. Establish foothold 4. Escalate privileges 5. Internal reconnaissance	3. Delivery 4. Exploitation 5. Installation	3. Delivery 4. Social engineering 5. Exploitation 6. Persistence 7. Defence evasion 8. Pivoting 9. Privilege scalation 10. Credential access 11. Discovery	3. Delivery 4. Persistence 5. Exploitation 6. Installation
Lateral Movement - surveillance - environment expanding	10. Lateral movement	6. Lateral movement		12. Lateral Movement	7. Lateral movement
Command and Control - attack management - maintain presence	11. Command and Control	7. Maintain presence	6. Command & Control	13. Command & Control	8. Command & Control
Execution - data collection - data exfiltration, - data manipulation	12. Collection 13. Exfiltration 14. Impact	8. Complete mission	7. Actions on objectives	14. Execution 15. Collection 16. Exfiltration 17. Target manipulation 18. Objectives	9. Action on objectives
End state - termination of the attack					

5. Conclusion and discussion

There are a wide range of internet threats and attacks from virus propagation and worms, to distributed denial of service (DDoS) attacks and data theft and manipulation and also critical infrastructure paralysis. So far, many proactive techniques have been proposed to deal with these threats. All these techniques pursue the same goal, preventing attackers from reaching their objectives.

There is great interest in developing proactive methods of cyber security, in which future attack strategies are anticipated and cyber-attack models are used. The APT attack model is crucial for cyber early warning systems.

Early warning is a proactive approach against security attacks and threats. These systems are a complement to intrusion detection and prevention systems where the main goal of them is the early detection of the potential behavior of a system, evaluating the scope of malicious behaviors, and finally applying a suitable response against any kind of detectable security event. APT attack modelling makes it possible to build efficient early warning system which collects, correlates the heterogeneous logs from various sensors and provides timely and effective information to avoid or reduce potential risks and prepare effective response with future behavior prediction. Modern cyber-attack warning should concentrate on the identification of indicators as early as possible to augment resilience.

Also, APT attack modelling helps to develop Cyber Threat Intelligence (CTI). It refers to a dynamic, adaptive technology that leverages large-scale threat history data to proactively block and remediate future malicious attacks on a network. Cyber threat intelligence recognizes indicators of attacks as they progress and essentially puts these pieces together with shared knowledge about attack methods and processes (Shackleford, 2015).

The general APT attack model helps in different levels of the CTI. Strategic level cyber threat intelligence informs the most senior decision-makers, in the operational level CTI is aimed at making day-to-day decisions and in tactical level CTI is focused on units in need of instantaneous information. The model can be applied to the needs of each CTI level.

References

Child J., Elbanna S., and Rodrigues S. (2010) *The Political Aspects of Strategic Decision Making*, in the Handbook of Decision Making, Paul C. Nutt and David Wilson (eds.), Chichester: Wiley.

Fire Eye. (2021) *Anatomy of Advanced Persistent Threat*, https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html, retrieved 29.9.2021.

IACP. (2021) *Cyber Attack Lifecycle*, on-line information, https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/, retrieved 17.10.2021.

Liaropoulos A. (2010), *War and ethics in cyberspace: Cyber-conflict and just war theory*, in J. Demergis (ed.), Proceedings of the 9th European Conference on Information Warfare and Security, Greece.

LM. (2021) *The Cyber Kill Chain®*, on-line information, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, retrieved 17.10.2021.

McAfee. (2021) What is the MITRE ATT&CK framework? on-line information, https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html, retrieved 20.10.2021

MITRE. (2021) *MITRE ATT&CK®*, on-line information, https://attack.mitre.org/, retrieved 19.10.2021.

Parrend, P. & Navarro, J. & Guigou, F. & Deruyver, A. & Collet, P. (2018*). Foundations and Applications of Artificial Intelligence for Zero-day and Multi-Step Attack Detection*. EURASIP Journal on Information Security.

Pols P. (2017) *The Unified Kill Chain Designing a Unified Kill Chain for analyzing, comparing, and defending against cyber-attacks*, Cyber Security Academy (CSA), December 7, 2017.

Pols P. (2019) *The Unified Kill Chain – Raising Resilience against Advanced Cyber Attacks*, White Paper, https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf, retrieved 2.10.2021.

Segal E. (2019) *APT Attacks 101: What They Are and How They Work*, internet blog, Sep 27, 2019, https://medium.com/@eddies_47682/apt-attacks-101-what-they-are-and-how-they-work-393c09f55eae, retrieved 10.10.2021.

Shackleford D. (2015) *Who's Using Cyberthreat Intelligence and How?* SANS, February 2015

Zeng W. and Germanos V. (2019) *Modelling Hybrid Cyber Kill Chain*, Cyber Technology Institute, School of Computer Science and Informatics De Montfort University, Leicester.