Juuso Itkonen

HOW ORGANIZATIONS CAN PREPARE FOR EMERGING THREATS FROM THE DARK WEB

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2022

ABSTRACT

Itkonen, Juuso
How organizations can prepare for emerging threats from the dark web
Jyväskylä: University of Jyväskylä, 2022, 65 pp.
Information Technology, Master's Thesis
Supervisor(s): Lehto, Martti; Niemelä, Mikko S.

This study examines the dark web and emerging threats to organizations from there. It is possible to acquire cyber threat intelligence and a greater understanding of cybercriminal practices by conducting research on the dark web. The objective was to determine what kind of threats emerge from the dark web and how organizations can prepare for them. The possibly available intelligence on cyber threats could be used for more proactive preparation against various cyber threats and attacks.

Because Tor is the most used technology, it is used to represent the darknet. The research methodology consisted of a case study. The issue involved Nasdaq Helsinki and the associated surface exposures that were discovered using the domain names of the listed companies. It was attempted to answer the research question of how organizations may prepare for increasing threats from the dark web. In order to address this issue, mapping began to determine if the discovered information on the organizations may be used in cyberattacks or if the discoveries directly indicate the existence of ongoing threatening activities. In addition, mitigation actions for the identified threats were identified. Whenever possible, attack techniques and patterns as well as mitigation measures were mapped to the MITRE ATT&CK and MITRE CAPEC frameworks. When applicable, CIS Controls were also mapped to identified cyber-attack techniques.

In the instance of Nasdaq Helsinki, findings relating to password leaks were very prominent. If the username and target system are known, these can be used to gain unauthorized access to the services. On the basis of this investigation, it is possible to conclude that cyber threat intelligence collected from the dark web is significant. This information would allow for more proactive defense against cybercrime. Therefore, organizations should utilize cyber threat intelligence to protect themselves from future cyberattacks. If you are unaware of the threats you face, it can be difficult to protect yourself from them.

Keywords: cyber threat intelligence, the dark web, Tor-network, attack techniques, mitigations

TIIVISTELMÄ

Itkonen, Juuso
Kuinka organisaatiot voivat varautua pimeästä verkosta nouseviin uhkiin
Jyväskylä: Jyväskylän yliopisto, 2022, 65 s.
Tietotekniikka, pro gradu -tutkielma
Ohjaaja(t): Lehto, Martti; Niemelä, Mikko S.

Tämä tutkielma käsittelee pimeää verkkoa ja sieltä organisaatioille nousevia uhkia. Pimeän verkon tutkimisella voidaan kasvattaa ymmärrystä kyberrikollisten toimintatavoista ja saada kyberuhkatietoa. Tavoitteena oli selvittää, millaisia uhkia pimeästä verkosta nousee organisaatioille ja miten niihin voisi varautua. Mahdollisesti saatavalla kyberuhkatiedolla voitaisiin varautua ennakoivammin erilaisiin kyberuhkiin ja hyökkäyksiin.

Pimeän verkon teknologiaksi rajattiin Tor-verkko, koska se on käytetyin teknologia. Tutkimusstrategiana oli tapaustutkimus ja tapauksena Nasdaq Helsinki listatut yhtiöt sekä niihin liittyvien verkkotunnuksien perusteella löydetyt uhkaavat asiat pimeästä verkosta. Tutkimuskysymykseen siitä, miten organisaatiot voivat varautua pimeästä verkosta nouseviin uhkiin, pyrittiin hakemaan vastausta. Tähän kysymykseen vastaamiseksi lähdettiin kartoittamaan, mitä organisaatioista löytyneistä tiedoista voitaisiin hyödyntää kyberhyökkäyksissä tai kertovatko löydökset suoraan meneillään olevasta uhkaavasta toiminnasta. Lisäksi kartoitettiin lievennyskeinoja löydöksiin liittyviin uhkiin. Hyökkäystekniikoita ja -kuvioita sekä lievennyskeinoja kartoitettiin MITRE ATT&CK viitekehystä ja MITRE CAPEC katalogia vasten siellä missä se oli mahdollista. Myös CIS Controls kontrollit kartoitettiin tunnistettuihin kyberhyökkäysmenetelmiin soveltuvin osin.

Erityisesti vuodettuihin salasanoihin liittyviä löydöksiä ilmeni Nasdaq Helsinki tapauksessa. Näitä voidaan käyttää valtuuttamattomaan pääsyyn palveluihin, jos myös käyttäjätunnus ja kohdejärjestelmä tunnetaan. Tämän tutkimuksen pohjalta voidaan todeta, että pimeästä verkosta saatavalla kyberuhkatiedolla on merkitystä. Näillä tiedoilla olisi mahdollista suojautua ennakoivammin kyberrikollisuutta vastaan. Organisaatioiden tulisikin hyödyntää kyberuhkatietoja suojautuakseen paremmin mahdollisilta kyberuhkilta ja -hyökkäyksiltä. Jos ei tiedä mille uhkille altistuu, niin niiltä voi olla hankala suojautua.

Asiasanat: kyberuhkatieto, pimeä verkko, Tor-verkko, hyökkäystekniikat, lievennykset

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

It can be claimed that cybersecurity technology has two sides, with both the defensive and offensive sides employing similar advancements (Huang, Siegel, & Madnick, 2018). The offensive side has had the upper hand thus far. Cybercrime is no longer a pastime, but rather a business or perhaps a job. There are hacking "as a service" models, and this innovation boosts and accelerates the expansion of the cybercrime ecosystem. If the direction and evolution of the cybercrime ecosystem are unknown and inaccessible, it will be difficult to defend against cyberattacks.

The dark web can serve as a conduit for numerous types of criminal behavior (Finklea, 2017). In forums, chat rooms, and other communication systems, criminal planning and coordination may take place through talks. A case in point involves talks on the dark web concerning tax-refund fraud schemes. Additionally, another expression of negative behavior on the dark web is the sale of unlawful or stolen products by criminals.

Multiple threat actors, including criminals, terrorists, and state-sponsored spies, utilize cyberspace to conduct destructive operations (Finklea, 2017). They utilize the dark web in particular because it reduces the chance of detection. The dark web is the most difficult and undetectable platform utilized by the actors previously stated (Nazah, Huda, Abawajy, & Hassan, 2020). Similar to crimes that occur in the physical world, dark web crimes occur in cyberspace. Because of the scale, obscurity, and unpredictability of the dark web's ecosystem, the ability to track down offenders is limited. To obtain potential solutions for evaluating cybercrimes, it is essential to identify dangers that emerge from the dark web.

It is now simpler to conduct sophisticated cybercriminal activities, which can result in interruptions and monetary losses for businesses (Benjamin, Valacich, & Chen, 2019). This is because the availability of sophisticated cybercriminal methods has expanded dramatically. You don't need all talents to commit cybercrimes because you can find cybercriminal materials such as tutorials, source code examples, malware, hacking tools, and more on the Internet. When society's reliance on cyber infrastructure grows, vulnerabilities to that infrastructure pose difficult challenges not only for society but also for cyber industry professionals and researchers.

Darknet or the dark web are not typically discussed in business literature, despite the fact that cyber-based risks can cause unexpectedly huge disruptions for enterprises and put company continuity and operations at risk (Benjamin, Valacich, & Chen, 2019). Research into cyber threat intelligence can assist not only businesses but also security practitioners and researchers. With cyber threat intelligence, the capability to detect emerging threats grows, and there is a greater chance of identifying or deducing future attack targets or identifying victims of prior assaults. Accordingly, it may be asserted that comprehending darknet or the dark web is more important than ever. By researching the markets and communities of the dark web, it may be able to gather understanding about these growing concerns.

The dark web can bring both digital and physical harm (Jardine, 2019). Shadow Brokers' release of stolen NSA zero-day exploits into the dark web is a digital example. The 2015 terrorist attacks in Paris, where the weapons used were obtained on the dark web, are an example of physical harm. Dark web attack vectors are multiplying at an alarming rate, necessitating accurate threat intelligence.

Darknet marketplaces are a promising source of threat intelligence (Ebrahimi, Nunamaker Jr, & Chen, 2020). Identifying cyber threats from darknet marketplaces in a timely and efficient manner can help enterprises and individuals avoid major financial losses. This can make it possible to forecast and prevent darknet-based criminal activity (UNODC, 2020).

Cybercrime is an expanding aspect of international criminal activity (UNODC, 2020). In the actual world, there are state borders for criminal activity, but the cyber world has no such boundaries. Therefore, criminals and victims may be from different countries and continents. Darknets are being utilized by cybercriminals since the technology enables the anonymization of illicit activity. Darknets can be used to conduct traditional cyberattacks, thereby serving as anonymizing bridges. In addition, the dark web provides a venue for illicit content and services. Due to the anonymity afforded by darknet technology, the work of crime detectives becomes increasingly difficult.

Every light has its shadows, and darknet technologies are no exception. Darknets are utilized for both good and evil in the same manner as the Internet. Darknets can also be used for good, such as to improve privacy against intrusive advertising and data collecting by various businesses. During internet investigations, law enforcement can also profit from this privacy. Censorship and attribution are challenging on the dark web, which is the primary distinction between the dark web and the traditional Internet (surface web). (UNODC, 2020)

By examining the material of the dark web, we can gain valuable insights that can help us comprehend criminal thoughts and so prevent cybercrimes (Basheer & Alkhatib, 2021). The identification of important actors and the transformation of cyberattack detection from reactive to proactive are both attainable goals. It has been demonstrated that exploring the dark web is a vital step in the battle against cybercrime, regardless of whether other sources from the deep web and surface web are included.

Cybersecurity is an increasing social concern (Samtani, Chinn, Chen, & Nunamaker Jr, 2017). Traditionally, cyber threat intelligence has concentrated on analyzing previously hacked systems. Despite the difficulties associated with proactive cyber threat intelligence, the cyber security community and practitioners have made efforts to advance it. One way to approach more proactive cyber threat intelligence is to do research and attempt to comprehend emerging risks straight from hacker communities.

The following chapter covers the fundamental concepts associated with this topic, such as the dark web and the onion router. This study's scope is also mentioned at the beginning of that chapter. The methodology section explains how the research was conducted. The results of this study are presented in the results chapter with one chart. In the chapter on surface exposure, potential surface exposures and cyberattacks associated with those exposures are outlined briefly. In the chapter on remediation of surface exposures, pertinent data have been mapped to potential hazards and mitigations and discussed. The conclusion chapter concludes the study, while the limitations and future work chapter analyzes the study's shortcomings and what more could have been done or what could be done in the future.

2 DARK WEB AND TOR

The focus of this thesis is limited to the dark web and the onion router (Tor) technology as one of the darknet technologies. In addition, there are more darknet technologies, such as the Invisible Internet Project (I2P) and Freenet, but Tor is chosen since it is the most popular (UNODC, 2020) (Nazah, Huda, Abawajy, & Hassan, 2020) (Akhgar, Gercke, Vrochidis, & Gibson, 2021). Due to the necessity for specialist software to operate on the Tor network and the difficulty involved, the dark web was chosen as the subject of this study's definition (The Tor Project, n.d.). The subsequent section briefly discusses the internet and web hierarchy. This provides insight into the dark web. The following section provides an overview of the Tor network.

2.1 Layers of the internet

Despite the fact that de facto Internet layers do not exist, discussing these abstract layers assists in comprehending the various types of Internet usage. In relation to this, the focus is typically on the end consumer, but in this instance it is on content generation.

There may be misconceptions that the internet and World Wide Web (the web) are synonymous, but they are not (Akhgar, Gercke, Vrochidis, & Gibson, 2021). The internet is a worldwide network of networks that connects millions of computers. One would believe that computers can communicate with one another if they are connected to the internet. The web is a model for sharing information built on the internet and a method for accessing and sharing information through the internet. There are numerous languages spoken on the internet, but the web employs hypertext markup language (HTTP). If the internet is a superset, then the web is a subset. There are three distinct areas of the Internet: the surface web, the deep web, and the dark web.

The surface web is the initial layer of the web (Akhgar, Gercke, Vrochidis, & Gibson, 2021). It is a publicly accessible portion of the web that is indexed by search engines such as Google and Bing. Consequently, search engines can retrieve information from the surface web. The surface web has existed since the web's inception.

The deep web is the second layer of the Internet (Akhgar, Gercke, Vrochidis, & Gibson, 2021). The primary distinction between the surface web and the deep web is that search engines cannot index deep web material; hence, the deep web is not searchable. Similar to the surface web, the deep web is accessible to the public in concept; nevertheless, there are multiple ways to reach the deep web. To access the deep web, for instance, a login page and credentials are necessary. In addition, there are secret and prohibited websites, as well as networks with restricted access. The deep web contains sensitive information, such as social media data, medical records, and financial records.

The dark web, which is part of the deep web, is the third and deepest layer of the Internet (Akhgar, Gercke, Vrochidis, & Gibson, 2021). Accessing the dark web requires specialist software, which is a major distinction from other levels of the Internet. With a Tor browser, the dark web is accessible, but just the Tor network, a subset of the dark web. There are numerous darknet technologies, such as Tor and I2P, however they just provide the network and not the content, unlike the Tor browser-accessible dark web. Similar distinction as that between the internet and the web. Darknets are not designed to facilitate illicit conduct, but data encryption and anonymity make it possible. Some lawful uses of darknets include circumvention of censorship, protection against identity theft, and protection against marketing tracking.

2.2 The Onion Router (Tor)

The Tor Project is a non-profit organization responsible for the development and maintenance of the Tor software (The Tor Project, n.d.). Tor is an installable computer application that secures its users by routing their communications through a distributed network of relays. Volunteers from all across the world participate in these relays. Tor lets users remain secure online. If a Tor user's network traffic is sniffed, the sites visited cannot be determined. Neither the visited sites nor the Tor user's geographical location can be determined. The collective name for this network of relays is the Tor network. Tor is typically accessed with a Tor Browser. This web browser is based on Mozilla's Firefox. Nonetheless, Tor Browser addresses numerous privacy issues.

Each packet in internet communication (TCP/IP) has a source and a destination IP address (The Tor Project, n.d.). When a packet is sent from its source to its destination, it may pass via many routers. Each of these routers examines the target address and forwards the packet to the next router until it reaches its final destination. Thus, the communication between the sender and receiver is transparent to the routers, and the communication participants are identified. Particularly the user's internet service provider (ISP) might create an accurate profile of the user's online activity. The same is true for internet servers, which can profile user behavior. There are three privacy-related objectives that Tor aims to achieve.

The first has to do with the user's location, which Tor conceals from web sites and services (The Tor Project, n.d.). The habits and interests of users could be determined from this data. This is disabled by default, so users can choose which information to disclose.

The second has to do with internet filtering and protecting network communications from prying eyes (The Tor Project, n.d.). Tor prohibits ISPs and any malicious actors from viewing the content of sent data and the origin from which it was retrieved. Even if a threat actor gained access to a user's home router, the details and destinations of network traffic cannot be ascertained. If this information cannot be determined, censorship can be circumvented because any website on the internet is available via the Tor network.

The third is connected to routing, which differs from the conventional proxy strategy in which a single proxy server relays network traffic (The Tor Project, n.d.). Tor routes traffic through a minimum of three relays; hence, a single relay cannot determine what is occurring. In addition, these relays are operated by organizations and individuals, which increases security via distributed trust compared to conventional proxy methods.

In addition to allowing users to browse the web anonymously, Tor also allows users to post material anonymously via Onion services (The Tor Project, n.d.). These Onion services are exclusively available via the Tor network and utilize the ".onion" top-level domain (TLD). Additionally, Onion services are utilized for file sharing, metadata-free communication, and safer software updates. As Facebook does, some prominent websites also publish their services as Onion services to enable more secure access to their services.

3 METHODOLOGY

The following subsections describe the methodology and design of this investigation. The research question, relevant sub-questions, and primary research strategy are described. The case under consideration and associated frameworks are then given.

3.1 Research question

Initially, there was a plan to investigate what may be found on the dark web that affects cyber security. Additionally, it was intriguing to investigate whether discovered information may be utilized to improve cyber security. After a period of preliminary study, the primary research question was formulated. After the idea that potential indicators of threats may be linked to industry-approved frameworks for cyberattacks and how to defend against them, two sub-questions arose. In the following bulleted list, the primary research question and sub-questions are offered.

- RQ1: How can organizations prepare for emerging threats from the dark web?
  - RQ1a: How can threat actors exploit the dark web information for cyber-attacks?
  - RQ1b: How can targets mitigate threats or remediate the situation of being exposed to cyber-attacks?

3.2 Research method

After searching for acceptable research methodologies or strategies based on the research topics, the case study was discovered and seemed adequate.

> In general, case studies are the preferred strategy when "how" or "why" questions are being posed, when the investigator has little control over events, and when the focus is on a contemporary phenomenon within some real-life context. (Yin, 2003)

On the basis of these three "requirements" for which the case study would be the preferred research technique, the case study has been selected. Previously mentioned research questions begin with the appropriate question "how." Existing data analysis involves no event control, thus the second criteria is likewise satisfied. The third condition of focusing on contemporary phenomena within a real-world context will also be met because the topic is timely and cyber-attacks occur frequently, thus there is the required real-world context.

Single-case and multiple-case studies are the two forms of case studies (Yin, 2003). Both may contain single-unit or multiple-unit analyses. Considering the scope of the effort, a single-case, single-unit analysis seemed suitable for this study. It was proposed that corporations listed on a stock exchange may be the focus of this investigation. So, one stock market would be the single case, and if all organizations in that stock market were processed as a single unit without disaggregating the results of each firm, this case would be a single case with single-unit analysis.

The dark web data utilized in this study was given by Cyber Intelligence House and was crawled from the Tor network with a 10-year history. This study's case is provided in the next section. When the data were collected, they were analyzed, and the results are presented in the chapter titled "Results." Following the results are chapters on surface exposures and their remediations, followed by a conclusion that addresses the research questions. Overall, the chapters from result to conclusion report the investigated case.

3.3 The case Nasdaq Helsinki

The Nasdaq Helsinki stock market is based in Helsinki, Finland. The website of Nasdaq Nordic was scoured for information regarding the companies listed on Nasdaq Helsinki (Nasdaq, Inc., n.d.). The names of organizations and their related top-level domains were compiled. Morningstar provided the fact sheets for the Nasdaq Helsinki listed companies table, which included information about the homepages of each company. For instance, if "www.example.com" is reported as a homepage, then "example.com" is the main domain name. The same homepage information may be found on the Morningstar website under the organization's contact information. At the time of data collection on 19 March 2022, there were 133 identified organizations with distinct primary domain names. If many stocks of the same company were reported with the same primary domain name, then only one stock was included in the case.

When searching for threatening things (later surface exposure) using dark web data, the primary domain names were employed as keywords. Since the data analysis was completed on 29 March 2022, the results do not include time after this date. The findings were considered as a single mass and presented in an acceptable manner in the results section, without being divided down by organization.

After identifying the pertinent findings, an attempt was made to map them to the various frameworks and knowledge offered in the following sections. In addition, a literature review was conducted. Two viewpoints exist on mappings. Possible attack strategies employed by threat actors and the countermeasures, controls, or safeguards that should be implemented to defend an organization's information systems against cyberattacks related to the mapped attacks.

3.4 MITRE ATT&CK

MITRE ATT&CK is a network-oriented enterprise framework and model that describes the actions of threat actors working within target networks (Strom, et al., 2017). ATT&CK is the acronym for Adversarial Tactics, Techniques, and Common Knowledge. The ATT&CK framework is based on real-world scenarios collected from watching APT attacks and public reporting of those intrusions. This framework enables a better understanding of the steps threat actors may take to achieve their objectives. This may aid in identifying weaknesses in the security of target networks.

ATT&CK refers to the phases of a cyberattack as tactics. These include, in descending order, reconnaissance, resource creation, initial access, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact. Each tactic includes attack techniques and possible sub-techniques. Techniques include instances of conducted attack operations, potential countermeasures against specific techniques, and detection methods for that type of attack.

In this thesis, dark web findings were mapped to ATT&CK framework attack methodologies where applicable. The purpose of the mapping was to determine what destructive activities threat actors can take with the material discovered on the dark web or what can be anticipated regarding the discoveries. Version 11 of the ATT&CK framework was released on April 25, 2022, during the completion of this thesis, and this most recent version was reviewed and adopted.

3.5 MITRE CAPEC

MITRE CAPEC is a catalog of common attack patterns that is available to the public (The MITRE Corporation, 2019a). Attack Pattern Enumeration and Classification are the abbreviations for CAPEC. These patterns may assist in comprehending how threat actors exploit vulnerabilities or holes in applications and other cyber capabilities. With this information, the CAPEC can be utilized to create and deploy improved information system defensive mechanisms.

Comparing CAPEC and ATT&CK from a cyber security perspective, they have distinct focuses (The MITRE Corporation, 2019b). CAPEC is focused on application security, whereas ATT&CK is focused on network security. CAPEC lists attacks against susceptible systems, including supply chain and social engineering, and is related to the enumeration of common weaknesses (CWE). The ATT&CK methodology is founded on cyber threat information and red team research. In addition, ATT&CK provides a contextual knowledge of harmful activity as well as an analysis of available defenses and testing support.

The two primary classes of CAPEC attack patterns are based on attack mechanisms and attack domains. There are also numerous useful views and external mappings, such as ATT&CK and OWASP-related patterns. In this thesis, the findings of the dark web were mapped to CAPEC, if applicable, using the same logic as the preceding section. Possible attack patterns and countermeasures are described in the threats and countermeasures sections for each type of finding.

3.6 CIS Controls

The CIS Critical Security Controls (CIS Controls) are the result of the pooled experience of numerous information technology specialists (The Center for Internet Security, Inc., 2021). This undertaking was directed by the Center for Internet Security (CIS). This investigation began by determining the most prevalent and significant cyber-attacks from actual cases that are continuously impacting enterprises. By turning this knowledge into an advantage for defenders and then sharing it with the public, it is believed that businesses and individuals will be better able to defend their information systems against cyber-attacks by focusing on the essentials.

The most recent version of the CIS Controls (v8) has 18 distinct controls that are further subdivided into 153 more specific safeguards. The safeguards are classified into three implementation groups (IGs), IG1 through IG3. The purpose of IGs is to enable businesses of varying sizes and types to prioritize and concentrate their defensive efforts on the most vital threats. Every organization should adopt the IG1's precautions, which is known as "essential cyber hygiene." (The Center for Internet Security, Inc., 2021). IG2 incorporates all IG1 precautions and provides extra safeguards for businesses with varying risk profiles. The same holds true for IG3, which incorporates all IG1 and IG2 precautions and adds the remaining protections, so incorporating all CIS Controls safeguards. Different types of organizations should choose which IG group best fits their environments and implement the corresponding controls and protections. The CIS Controls (v8) and associated safeguards are available in Appendix 1.

The CIS Controls are already mapped to MITRE ATT&CK v8.2, although ATT&CK v11 was used in this thesis. This previously completed mapping by CIS served as a guide for mapping pertinent ATT&CK tactics and CAPEC attack patterns to CIS Controls. Mapping was only performed at a high level, at the level of control.

4 RESULTS

In the case of Nasdaq Helsinki, a number of dark web results were found. As stated in the chapter on methodology, the primary domain names of the organizations were utilized as keywords during the search process. For instance, if it is determined that a page on the dark web is a marketplace and there is a hit, this discovery is regarded as a marketplace associated with the concerned company. In the instance of Nasdaq Helsinki, the results are not published per organization, but rather as a sum of all organizations' conclusions.

Next, the results of the case study are provided in Figure 1. This graph sorts and displays the results by the total number of hits across all Nasdaq Helsinki-listed companies. In addition, the mean of each discovery across all organizations in the case study is displayed on each bar. The chart's top value is the maximum number of occurrences of a certain finding type for a single organization. In addition, the median of each discovery across all organizations is shown. The hits value indicates the number of organizations with hits for a certain finding.

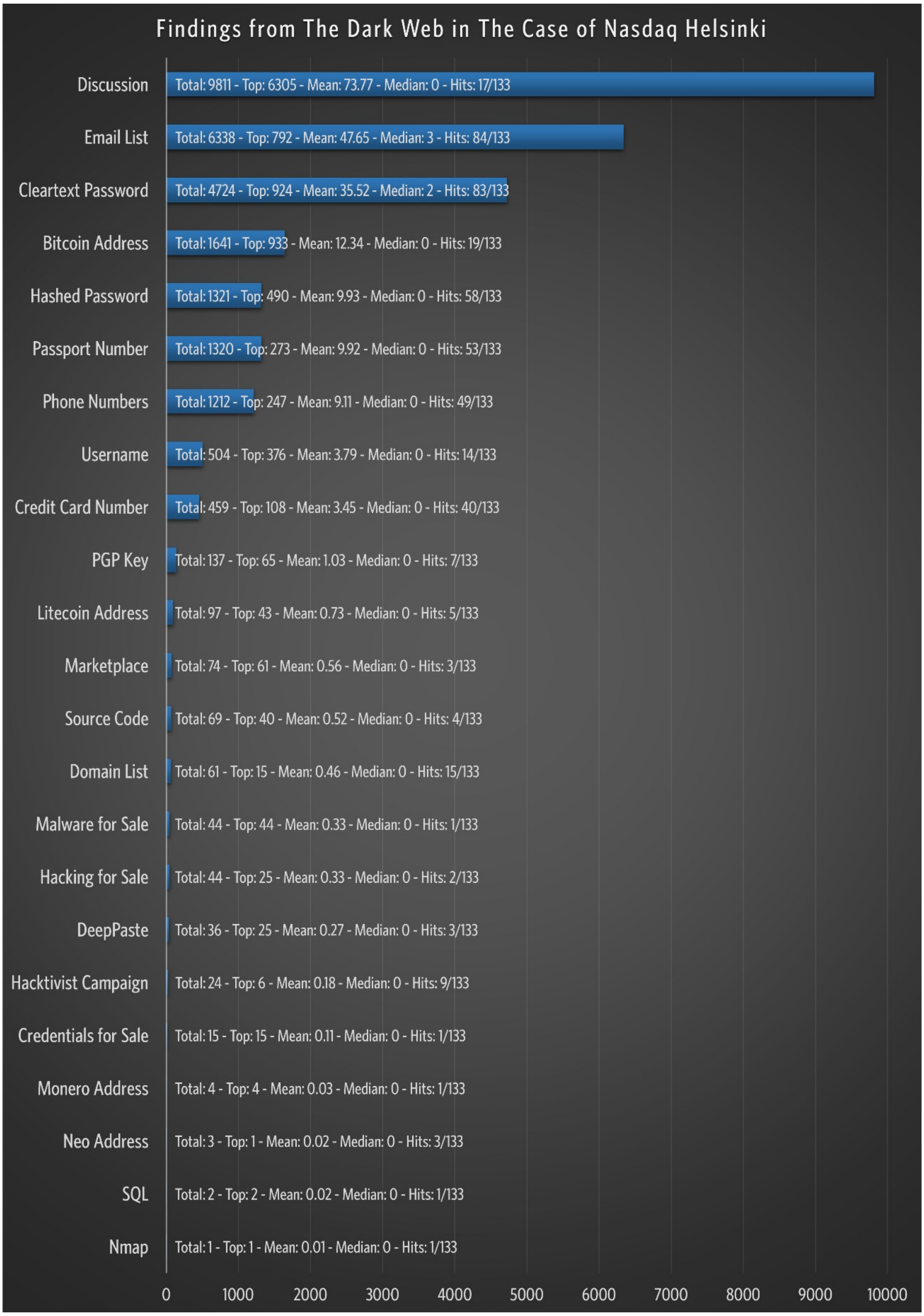

FIGURE 1 Findings from the dark web

As shown in Figure 1, there were numerous hits pertaining to conversations, email lists, and cleartext passwords. Only two types of results had a median value greater than zero. These discovery kinds pertained to email lists and cleartext passwords. As indicated by the hits value, these two sorts of findings were the most prevalent across all organizations.

5 SURFACE EXPOSURE

Surface exposure refers to variables that amplify the probability of compromising vectors (Woods & Böhme, 2021). The previously disclosed facts from the dark web regarding the matter of Nasdaq Helsinki can be deemed to be surface exposures. These surface exposures will be given on a general level in this chapter, along with a number of Nasdaq Helsinki case study findings.

5.1 Cleartext passwords

Cleartext passwords are passwords that are human-readable. Therefore, they are not encrypted. A threat actor may utilize cleartext passwords to gain unauthorized access to a system if the target system and a potentially required username are known. Numerous Internet services, for instance, merely require a username and password for login. In the case of Nasdaq Helsinki, a total of 4,724 such surface exposures were discovered.

5.2 Hashed passwords

Cleartext passwords are input to a hashing algorithm, which produces hashed passwords. Typically, hashed passwords can be retrieved from a database of software or a service that requires user authentication, where the user's password is saved in hashed form for comparison reasons during authentication. Threat actors may attempt to decrypt hashed passwords to recover the cleartext passwords. If successful, the threat actor may employ cracked passwords, such as the previously mentioned cleartext passwords. In the case of Nasdaq Helsinki, a total of 1,321 such surface exposures were discovered.

5.3 PGP keys

It is possible to employ Pretty Good Privacy (PGP) keys for asymmetric encryption. There are both private and public keys, and as the names of the keys suggest, the private ones should be kept secure. Asymmetric in this context means that only a private key can decode data encrypted with a public key, and vice versa. If a public key is used to encrypt a message that should remain confidential and only a private key holder should be able to decrypt the message, then the confidentiality is compromised if a threat actor obtains the private key. When a private key is used to verify the validity of a message and a threat actor obtains the private key, the authenticity of messages associated with that private key can no longer be trusted. 137 surface exposures of this type were discovered in the instance of Nasdaq Helsinki.

5.4 Hacktivist campaigns

Cyber activism occurs just as it does in the real world. These cyber activists may be referred to as hacktivists. They can post online their plans to assault certain information systems for whatever cause. 24 surface exposures of this type were discovered in the case of Nasdaq Helsinki.

5.5 Domain list

In this study, "domain list" refers to a list of domain names such as "www.example.com, host.example.com, etc." If a threat actor wishes to attack the information systems of an organization, a list of targets is required. This may be a list of domains, for instance. 61 surface exposures of this type were discovered in the instance of Nasdaq Helsinki.

5.6 IP list

In this study, IP list refers to a list of IP addresses. This situation is identical to the domain list discussed above. A threat actor may exploit a list of an organization's IP addresses for attack purposes. In the instance of Nasdaq Helsinki, there were no discoveries connected to this surface exposure, yet it is nonetheless included in our analysis.

5.7 Email list

An email list is of course a list of email addresses. This kind of list may be used by a threat actor to send fraudulent messages to get valuable information or get someone to do something the threat actor wants. Total number of found surface exposures of this kind in the case of Nasdaq Helsinki was 6338.

5.8 Phone numbers

In this study, phone numbers refer to a collection or list of telephone numbers. These can be used to call the numbers in the means to obtain vital information or to get the individual to do what the caller desires. 1212 surface exposures of this type were discovered in the instance of Nasdaq Helsinki.

5.9 Credit card numbers

In this study, credit card number refers to the specific type of payment card numbers. These may be used for fraud, or the unauthorized use of another person's money. In the case of Nasdaq Helsinki, a total of 459 such surface exposures were identified.

5.10 Passport numbers

Passport numbers are unique identification numbers utilized in passports. These may be used to commit identity theft. In the case of Nasdaq Helsinki, a total of 1,320 such surface exposures were discovered.

5.11 Access for sale

Access for sale indicates that an information system's access is for sale. It does not necessarily indicate that some credentials that grant access to certain systems are for sale, but it can also mean other things. Threat actors can simply acquire access to an organization's systems and go on to the subsequent phases of their destructive activities. 15 surface exposures of this type were discovered in the case of Nasdaq Helsinki (credentials for sale).

5.12 Obtainable capabilities

This study identifies malware, tools, and exploits as capabilities that can be utilized to execute cyberattacks. Attempts may be made to infect the systems of the target organization with malware that steals data, for instance. For attacks, industry-standard tools that are not necessary meant for this kind of activity but rather for testing purposes may be utilized. Exploits are software programs that can be used to exploit flaws and vulnerabilities in the target information systems. 44 surface exposures of this type were discovered in the case of Nasdaq Helsinki (malware for sale).

5.13 Source code

Source code refers to a recognizable code format, such as HTML, Python, Java, or C. There may be numerous instances in which such findings pose a threat to companies. The source code of a commercial program may be leaked. This could potentially be associated with accessible capabilities and be more specific to exploit code. 69 surface exposures of this type were discovered in the instance of Nasdaq Helsinki.

5.14 Cryptocurrency addresses

In this study, cryptocurrency addresses refer to cryptocurrency-related addresses such as Bitcoin wallet addresses. These may include Bitcoin, Monero, Neo, and Litecoin addresses, as seen in the instance of Nasdaq Helsinki. These addresses may indicate trade activity on the site where the findings are discovered. In the case of the Nasdaq Helsinki, several surface exposures were discovered. In the case of Nasdaq Helsinki, a total of 1,745 surface exposures of this type were discovered (Bitcoin + Litecoin + Monero + Neo).

5.15 Black markets

In this study, "black markets" refers to online marketplaces on the dark web. On these platforms, companies' stolen intellectual property may be for sale. In the instance of Nasdaq Helsinki, a total of 74 surface exposures of this type were identified.

5.16 Discussion forums

Discussion forums on the dark web are online meeting places for individuals to converse. There may have been plans for harmful action or the dissemination of stolen information. In the instance of Nasdaq Helsinki, a total of 9811 surface exposures of this type were uncovered.

5.17 DeepPaste

DeepPaste is a 'pastebin' website on the dark web. People can anonymously copy and paste text on this website and share it with others. Texts that have been copied and pasted may include sensitive information for organizations, such as password lists. In the instance of Nasdaq Helsinki, a total of 36 such surface exposures were discovered.

6 REMEDIATIONS TO SURFACE EXPOSURES

In this chapter, previously stated surface exposures have been mapped to associated cyber-attack techniques and patterns, and potential mitigations have been mapped accordingly. Against MITRE ATT&CK, MITRE CAPEC, and CIS Controls, mappings were performed. However, all surface exposures were not successfully mapped.

6.1 Remediation to Cleartext passwords

When cleartext passwords are combined with a legitimate username and the system to which the tokens are assigned, it is evident that there is a chance of gaining access to that system, and threat actors can use this vulnerability for harmful reasons. In addition, these cleartext passwords may be associated with attacks such as password policy discovery, password spraying, and credential stuffing. In Tables 1 and 2, I provide potential cyberattack tactics pertaining to cleartext passwords, whereas Tables 3, 4, and 5 present mitigations.

TABLE 1 MITRE ATT&CK attack techniques (cleartext passwords)

ID	Name
T1021	Remote Services
T1078	Valid Accounts
T1110.003	Password Spraying
T1110.004	Credential Stuffing
T1111	Multi-Factor Authentication Interception
T1201	Password Policy Discovery
T1621	Multi-Factor Authentication Request Generation

TABLE 2 MITRE CAPEC attack patterns (cleartext passwords)

ID	Name
555	Remote Services with Stole Credentials
560	Use of Known Domain Credentials
565	Password Spraying
600	Credential Stuffing

TABLE 3 MITRE ATT&CK mitigations (cleartext passwords)

ID	Name
M1013	Application Developer Guidance
M1017	User Training
M1018	User Account Management
M1026	Privileged Account Management
M1027	Password Policies
M1032	Multi-Factor Authentication
M1036	Account Use Policies

TABLE 4 MITRE CAPEC mitigations (cleartext passwords)

Related mitigations from MITRE CAPEC
- Create a strong password policy and ensure that your system enforces this policy.
- Deny remote use of local admin credentials to log into domain systems.
- Disable RDP, telnet, SSH and enable firewall rules to block such traffic. Limit users and accounts that have remote interactive login access. Remove the Local Administrators group from the list of groups allowed to login through RDP. Limit remote user permissions. Use remote desktop gateways and multifactor authentication for remote logins.
- Do not allow accounts to be a local administrator on more than one system.
- Do not reuse local administrator account credentials across systems.
- Ensure users are not reusing username/password combinations for multiple systems, applications, or services.
- Implement an intelligent password throttling mechanism. Care must be taken to assure that these mechanisms do not excessively enable account lockout attacks such as CAPEC-2.
- Leverage multi-factor authentication for all authentication services and prior to granting an entity access to the domain network.
- Monitor system and domain logs for abnormal credential access.

TABLE 5 CIS Critical Security Controls (cleartext passwords)

Control	Name

4	Secure Configuration of Enterprise Assets and Software
5	Account Management
6	Access Control Management
14	Security Awareness and Skills Training
16	Application Software Security

Threat actors may attempt to exploit valid accounts during many phases of the lifecycle of a cyberattack (The MITRE Corporation, 2022i). They can attempt to enter an organization's network or keep their current foothold. In addition, threat actors may attempt to increase rights they already possess or escape detection by utilizing these legitimate accounts. In general, valid accounts can circumvent the access controls established on various systems and resources. Because the access is legitimate and the accounts are valid, it can be difficult to discover unauthorized use of these exposed accounts. In order to remain as anonymous as possible, threat actors could avoid utilizing attack tools such as malware with valid accounts. Malicious acts may target externally accessible remote systems and services, such as the virtual private network (VPN), remote desktop, and web-based email. Different accounts' permissions overlapping across a network would be undesirable from the viewpoint of the defender, as an attacker may utilize this to pivot between computers and seize highly privileged access accounts, such as domain administrator.

Against the threat that threat actors obtain a valid account, countermeasures such as application developer guidance, password policies, privileged account management, user account management, and user training can be implemented (The MITRE Corporation, 2022i). Developers can be instructed not to save credentials in plain text in application code, linked code repositories, or storage systems. Moreover, applications should securely store credentials and other sensitive data. Default credentials should not be used, and if apps utilize secure shell (SSH) keys, they must be safeguarded and routinely updated. Periodically, privileged accounts should be audited in order to verify their presence and rights. Similarly, end user accounts should be audited to ensure that there are no unnecessary accounts and that permissions are appropriate. Users should be instructed not to accept invalid push notifications for multi-factor authentication (MFA) and to report them.

If a threat actor obtains legitimate domain credentials, they can be utilized to traverse the target network laterally (The MITRE Corporation, 2021g). Typically, domain users are permitted to log in to different systems or applications using the same credentials or through single-sign-on (SSO). This might lead to a situation in which a threat actor could access sensitive data, infect target systems with malware, assume a persona associated to the credentials and engage in social engineering.

Password policies are used to require users to employ complex passwords that are difficult to crack using brute force or guessing (The MITRE Corporation, 2022f). If a threat actor is attempting to brute-force more passwords and is aware of the target organization's password policy, this might be extremely useful knowledge during an attack. The advantage is that it is not necessary to try all possible combinations of passwords when cracking, only a subset of all passwords. If the password policy requires a minimum length of eight characters, it is not necessary to try any shorter passwords during the cracking process. The same logic applies to determining which characters must be tried, or at least it is known which characters must be tried, therefore passwords that do not contain required characters can be omitted from testing. If an attacker obtains a large number of passwords belonging to the same organization, they can extract password policy-like information from these passwords and use this information to attack other businesses' accounts that have not been compromised.

Threat actors may use password spraying to gain unauthorized access to an organization's systems (The MITRE Corporation, 2021b). It is a technique in which malicious actors utilize a single or several regularly used passwords against multiple accounts in an attempt to obtain legitimate account credentials. Using many target accounts rather than a single account helps to prevent account lockouts. Obviously, if a threat actor knows the password policy of the target system or has access to stolen passwords and can use this information to deduce the password policy, a higher success rate can be expected when better-guessed passwords are used in an attack.

Account use policies, multi-factor authentication (MFA), and password policies can help defend against password spraying attacks (The MITRE Corporation, 2021b). The account should be locked after a specified number of failed logins attempts to prevent guessing the password. However, an overly stringent policy can result in a denial-of-service attack if, for instance, all system accounts are under brute-force attack. Also recommended is the usage of multi-factor authentication whenever possible. Password policies should be implemented to prohibit the use of weak passwords. Good guidelines for designing password policies can be found in NIST guidelines, for instance.

Credential stuffing is an attack that threat actors may employ in an attempt to get access to other systems to which leaked credentials do not allow access (The MITRE Corporation, 2021a). This hack exploits the tendency of individuals to reuse passwords across several systems. If a person's compromised credentials grant access to their personal email, it is likely that they used the same password for a business system, and if there are no other protections in place, the same password grants access there as well.

With account use policies, multi-factor authentication, password policies, and user account management, credential stuffing can be minimized (The MITRE Corporation, 2021a). A policy for account lockout similar to the one described in the event of password spraying should be in place. In addition, multifactor authentication should be implemented wherever possible, and password regulations should be implemented. As part of user account management, a proactive reset must be performed promptly or after detecting assaults against credentials that are known to be compromised.

Common remote access protocols, such as SSH and RDP, facilitate remote connections between computers (The MITRE Corporation, 2022h). Through these remote access protocols, threat actors can exploit valid accounts to get unauthorized access. When a threat actor has compromised a system, he or she has the ability to perform any action permitted by the exploited account privileges. If a valid account that has been compromised is a domain account, it may be feasible to gain access to many computers inside the domain environment. If threat actors have only recently gained initial access to the IT-environment, they may like to learn more about it prior to lateral movement. Therefore, it is probable that they use discovery approaches to attempt to uncover more environmental information.

Monitoring login activity and searching for out-of-the-ordinary behavior and other suspicious activity related to remote services may aid in identifying attackers (The MITRE Corporation, 2022h). Using multifactor authentication and user account management, the threat of unauthorized access usage with valid accounts can be addressed. Accounts that can be used for remote services should be restricted based on actual need. In addition, remote usage accounts' rights should be restricted to only the actions required.

It is also possible for threat actors to attack the multi-factor authentication method itself in an attempt to acquire access to accounts protected by the MFA mechanism (The MITRE Corporation, 2022c). If one element of the MFA is a smart card, then threat actors would employ a keylogger to obtain the associated password while the end user is using the system regularly. Likewise, one-time passwords can be intercepted if the devices to which they are sent are not adequately safeguarded. However, such attacks need great skill. Interception of multifactor authentication can be mitigated through user training. Smart cards should be withdrawn from devices when they are not in use to prevent them from falling into the wrong hands.

If a threat actor possesses legitimate account credentials and the login to a target system is protected by multi-factor authentication, the threat actor may attempt to log in as many times as the real user accepts MFA push notification to access the system (The MITRE Corporation, 2022d). In this instance, instructing users not to accept MFA push notifications whose origin they are unsure about and to report such incidents may prevent an attack similar to the one described before. Additionally, location-based limits could be implemented as mitigations. If the login attempts do not occur in the same location as the MFA device, or if the login attempt itself does not occur from the permitted location, access will be refused. As an additional mitigation, the maximum number of push notifications that can be sent within a given time period can be defined. Additionally, there are alternative techniques for push notifications, such as a one-time passcode on the login screen, which mitigate the risk associated with push messages.

6.2 Remediation to Hashed passwords

As the preceding section demonstrates, passwords should not be saved in plaintext format. In the case of Nasdaq Helsinki, hashed passwords associated with the organization's primary domain names were discovered. The following tables illustrate relevant attack approaches, trends, and countermeasures against hashed passwords.

TABLE 6 MITRE ATT&CK attack techniques (hashed passwords)

ID	Name
T1110.002	Password Cracking
T1550.002	Pass the Hash

TABLE 7 MITRE CAPEC attack patterns (hashed passwords)

ID	Name
49	Password Brute Forcing
55	Rainbow Table Password Cracking
644	Use of Captured Hashes (Pass The Hash)

TABLE 8 MITRE ATT&CK mitigations (hashed passwords)

ID	Name
M1018	User Account Management
M1026	Privileged Account Management
M1027	Password Policies
M1032	Multi-factor Authentication
M1051	Update Software
M1052	User Account Control

TABLE 9 MITRE CAPEC mitigations (hashed passwords)

Related mitigations from MITRE CAPEC
- Create a strong password policy and ensure that your system enforces this policy. - Implement a password throttling mechanism. This mechanism should take into account both the IP address and the log in name of the user. - Leverage multi-factor authentication for all authentication services and prior to granting an entity access to the domain network. - Leverage system penetration testing and other defense in depth methods to determine vulnerable systems within a domain. - Monitor system and domain logs for abnormal credential access.

- Passwords need to be recycled to prevent aging, that is every once in a while a new password must be chosen.
- Prevent the use of Lan Man and NT Lan Man authentication on severs and apply patch KB2871997 to Windows 7 and higher systems.
- Put together a strong password policy and make sure that all user created passwords comply with it. Alternatively automatically generate strong passwords for users.
- Use salt when computing password hashes. That is, concatenate the salt (random bits) with the original password prior to hashing it.

TABLE 10 CIS Critical Security Controls (hashed passwords)

Control	Name
4	Secure Configuration of Enterprise Assets and Software
5	Account Management
6	Access Control Management
7	Continuous Vulnerability Management
18	Penetration Testing

Threat actors may still attempt to convert hashed passwords to cleartext format, also known as "cracking" hashed passwords, via a variety of techniques (The MITRE Corporation, 2022a). It is possible to guess passwords, feed them to suitable hashing functions, and then compare the results to leaked hashed passwords. There are even precomputed hashes for various words (rainbow tables) or password candidates, making cracking operations easier if there is a match between the password candidates and the actual cleartext password. Typically, hash cracking is performed outside of a hacked system from which password hashes have been acquired. When a cleartext password is successfully exposed, the threats are identical to those mentioned in the previous section. There are also attack methods where hashes can be utilized directly without first breaking the password, such as the pass-the-hash attack.

Multi-factor authentication and password policies can be used to mitigate password cracking (The MITRE Corporation, 2022a). By utilizing MFA, threat actors cannot get access to systems using stolen credentials alone. Using password policies, such as requiring strong passwords, may make password cracking significantly more difficult for attackers.

The brute-force attack on a password is a technique in which all potential passwords are tested to discover the correct one (The MITRE Corporation, 2021e). This strategy will always be successful in the end, although the length of time required will vary. If the password is sufficiently lengthy and the character set employed is intricate, brute force computing may take too long to be effective.

A password rainbow table is a list of cleartext passwords and their associated hashes that have been precomputed (The MITRE Corporation, 2021f). A threat actor can find a match of the hash from a rainbow table, and if there is a match, the password is retrieved and can be utilized in the same manner as mentioned in the section titled "cleartext password." Salting can be utilized to reduce the likelihood that a password can be cracked using a rainbow table. A salt is a string of random characters appended to a password before it is hashed. When storing salted password hashes, the salt is saved alongside the password hash in cleartext. Salt essentially renders rainbow tables ineffective against salted password hashes.

In certain situations, password hashes can be utilized directly without first being decrypted into plaintext passwords (The MITRE Corporation, 2021n). If so, lateral movement within the target network and bypassing of access controls may be possible. Pass-the-hash bypasses the standard authentication phase that requires the cleartext password, proceeding directly to the authentication step that uses the password hash. There is also an overpass-the-hash assault, which is similar to the pass-the-hash attack, but that it allows a valid Kerberos ticket to be generated using a valid password hash. Then, a legitimate Kerberos ticket might be utilized in a pass-the-ticket attack.

The potential of a pass-the-hash attack can be minimized via privileged account management, software updates, user account control, and user account management (The MITRE Corporation, 2021n). In the case of a privileged account, efforts should be taken to limit credential overlap between systems and reduce the impact of a successful attack by reducing the likelihood of lateral movement between systems. Software should be routinely updated to eliminate vulnerabilities related to pass-the-hash, such as a patch that restricts the access of local administrator group accounts. There are registry mitigations against pass-the-hash attacks in Microsoft Windows operating systems. Additionally, domain users should not be members of numerous local administrative groups.

6.3 Remediation to PGP keys

In the instance of Nasdaq Helsinki, findings regarding pretty good privacy (PGP) keys or OpenPGP keys were discovered. OpenPGP is an open format for encrypting or authenticating data (OpenPGP, 2020). It is based on the original PGP software. OpenPGP utilizes public-key cryptography. Private keys should be kept private, as their name suggests, and if they are exposed, the confidentiality and integrity of all data encrypted with them are compromised. Findings are not always private keys, however the following attacks and mitigations could be employed in the event that private keys are discovered.

TABLE 11 MITRE ATT&CK attack techniques (PGP keys)

ID	Name
T1552.004	Private Keys

TABLE 12 MITRE CAPEC attack patterns (PGP keys)

ID	Name
474	Signature Spoofing by Key Theft

TABLE 13 MITRE ATT&CK mitigations (PGP keys)

ID	Name
M1022	Restrict File and Directory Permissions
M1027	Password Policies
M1041	Encrypt Sensitive Information
M1047	Audit

TABLE 14 MITRE CAPEC mitigations (PGP keys)

Related mitigations from MITRE CAPEC
- Ensure all remote methods are secured
- Ensure all services are patched and up to date
- Restrict access to administrative personnel and processes only
- Restrict access to private keys from non-supervisory accounts

TABLE 15 CIS Critical Security Controls (PGP keys)

Control	Name
3	Data Protection
5	Account Management
6	Access Control Management
11	Data Recovery
18	Penetration Testing

When a file containing a private key certificate is discovered, it is feasible to counterfeit the legitimacy of data (The MITRE Corporation, 2021d). The data signed with the compromised private key can no longer be trusted. Table 14 presents mitigations connected to CAPEC.

Additional countermeasures include restricting file and directory permissions, implementing password regulations, encrypting sensitive data, and conducting an audit (The MITRE Corporation, 2020). Regular auditing should be performed in which access lists are evaluated and it is confirmed that only authorized keys have access to vital resources. Keys should be saved on distinct instances as opposed to the local system. Private keys should also be secured using strong passphrases so that they cannot be utilized as-is. Ensuring that the permissions for the locations where the private keys are stored are configured appropriately will prevent unauthorized access.

6.4 Remediation to Hacktivist campaigns

The purpose of a cyberattack is not always to cause economic damage or profit (Nurmi & Niemelä, 2018). Similar to how activism occurs in the physical world, hacktivism occurs online. Hacktivism is performed in opposition to anything, and its motivations can be political ideas, social causes, religion, or philosophy.

A hacktivist campaign begins with the online publication of a manifesto that describes its goals and motivations (Nurmi & Niemelä, 2018). Manifestos may also be shared on social media by hacktivists. By disclosing their aims and motivations, they want to gain public support for their protest. Manifestos and other forms of hacktivist group communication typically detail the motives behind cyberattacks. Following this, the attack campaign will continue with cyberattacks, particularly DDoS (Distributed Denial of Service), whose objective is to compromise the availability of the targeted systems.

There may be publicly accessible target lists on the Internet and on social media, containing various information about the targets, such as web server-related domain names, software names, port numbers, and IP addresses (Nurmi & Niemelä, 2018). In addition, attackers may give tools for others to join the attack, such as DDoS. This will amplify the consequences of the assault, and target servers will be unable to handle the load they are subjected to and will not be functioning normally.

DDoS attack tools can be web-based, so users do not need to install them (Nurmi & Niemelä, 2018). To participate in the attack, users simply need to visit the web page and a JavaScript code will begin flooding traffic to the target systems from their computer. Users should be aware that participating in DDoS attacks is prohibited in many countries. Even if the intention is noble, such as "rescue the whales," cyberattack is not a lawful means of influencing the situation.

Although participation in these attacks is illegitimate, the attacks persist (Nurmi & Niemelä, 2018). Participating users can conceal their attack origin by utilizing the Tor network, for example. In this manner, participants conceal their true IP address. In addition, DDoS assaults may be coordinated over the anonymous communication channels of the Tor network, such as Internet relay chat (IRC). On the dark web, attack campaign coordinators might provide instructions on how to connect to the Tor network's anonymous IRC channels. Extreme difficulty exists in revealing the true names of participants on these anonymous communication channels.

Cyberattack manifestos may contain political, economic, social, technological, environmental, or legal motivations and reasoning (Nurmi & Niemelä, 2018). Motives dictate the selection of objectives. If the motivation is political, the goal of the attack is governments and businesses, and this is the most prevalent reason for attacks. In addition to economic factors and actions, societal reasons can also lead to attacks against governments and corporations. Environmental concerns are frequent justifications for hacktivism and assault campaigns, although technological incentives are uncommon and rarely the cause of an attack. In addition, several hacktivism campaigns have been motivated by the legal climate.

As previously said, DDoS attacks are typically considered as attack techniques associated with hacktivist activities. The subsequent tables map similar attack techniques, patterns, and mitigations to hacktivist campaigns.

TABLE 16 MITRE ATT&CK attack techniques (hacktivist campaigns)

ID	**Name**
T1498	Network Denial of Service
T1499	Endpoint Denial of Service

TABLE 17 MITRE CAPEC attack patterns (hacktivist campaigns)

ID	**Name**
469	HTTP DoS

TABLE 18 MITRE ATT&CK mitigations (hacktivist campaigns)

ID	**Name**
M1037	Filter Network Traffic

TABLE 19 MITRE CAPEC mitigations (hacktivist campaigns)

Related mitigations from MITRE CAPEC
- Configuration: Configure web server software to limit the waiting period on opened HTTP sessions - Design: Use load balancing mechanisms

TABLE 20 CIS Critical Security Controls (hacktivist campaigns)

Control	**Name**
4	Secure Configuration of Enterprise Assets and Software
7	Continuous Vulnerability Management

With denial of service (DoS) attacks, threat actors may attempt to compromise the system's accessibility (The MITRE Corporation, 2022e). The objective may be to reduce the accessibility of the target system or to completely prevent its use. When attack traffic against a target is generated by numerous systems deployed throughout the Internet, the attack is typically referred to as a distributed denial of service attack (DDoS). The objective of a network-level DoS is to consume so much of the target system's network connection's bandwidth that the system's availability is compromised. A web application, website, email service, or domain name system may be the target (DNS).

By filtering network traffic, network-level DoS can be avoided (The MITRE Corporation, 2022e). Internet service providers (ISPs) that host websites can distinguish malicious traffic from legitimate traffic and block it upstream of the destination. In addition, content delivery network (CDN) service providers and specialized DoS mitigation service providers can assist in mitigating these DoS attacks. In some instances where the Internet connection is not completely saturated, on-premises filtering may be a viable solution for blocking malicious data. Organizations should assess the risk of DDoS attacks against their most important assets and include these scenarios in their disaster recovery and business continuity plans.

There is also a DoS attack type at the endpoint level in which the organization's internet connection linked with the target asset is not completely overwhelmed by fraudulent traffic, but the target system becomes fatigued (The MITRE Corporation, 2022b). Another possibility is that the target system is not completely exhausted but is experiencing a continuous crash condition. Botnets are typically employed as attackers in DoS assaults of both levels.

Filtering network traffic can help defend against DoS attacks at the endpoint level (The MITRE Corporation, 2022b). Additionally, CDN and specialized DoS mitigation service providers may be utilized in this scenario. However, when the network connection is not exhausted, firewalls can filter the network boundary. The source IP addresses of the attackers can then be used to prevent DoS attack traffic, for instance.

6.5 Remediation to Domain list

Cyberattacks vary in terms of their level of complexity, as well as their scope, objective, and impact. There are numerous frameworks that divide cyberattacks into distinct phases (Mazurczyk & Caviglione, 2021). Primarily, the first step is always the collection of information on the target, often known as the reconnaissance phase. The purpose of reconnaissance is to identify the target's weak areas and formulate an attack strategy based on the obtained intelligence. The acquired information may contain information about the hardware and software utilized on the target systems, as well as their versions. In addition to technical characteristics of the target environment, the acquired information may also contain the actual location of the targeted organization, telephone numbers, employee names, and email addresses. Each and every piece of information can be used by attackers to identify vulnerabilities and even construct software exploits for vulnerable systems.

In the case of Nasdaq Helsinki, lists of domains of organizations were identified. The tables below illustrate which attack techniques and mitigations can be mapped to this type of finding.

TABLE 21 MITRE ATT&CK attack techniques (domain list)

ID	Name
T1590.001	Domain Properties

TABLE 22 MITRE ATT&CK mitigations (domain list)

ID	Name
M1056	Pre-compromise

TABLE 23 CIS Critical Security Controls (domain list)

Control	Name
18	Penetration Testing

Threat actors may attempt to obtain information about the network domain names of the target company, which can be used later in the cyber-attack preparation process (The MITRE Corporation, 2021i). Domain information may include properties and information such as the domains owned by the target organization, domain registrars, email addresses, phone numbers, physical locations, and name server addresses. Phishing and active scanning can both be used to obtain information. Information gathering may present fresh opportunities to advance in the reconnaissance phase or perhaps advance to the next phase of the cyber-attack.

Domain information collection cannot be easily mitigated. This is due to the fact that the information collection occurs outside of the organization, such as through public sources (The MITRE Corporation, 2021i). However, there is at least one thing that can be done, and that is to limit the amount of information external parties have access to, particularly sensitive information.

6.6 Remediation to IP list

In the case of Nasdaq Helsinki, IP address lists are not present, but this may be the case with more extensive data. The tables below illustrate which attack techniques and mitigations can be mapped to this type of finding.

TABLE 24 MITRE ATT&CK attack techniques (IP list)

ID	Name
T1590.005	IP Addresses

TABLE 25 MITRE ATT&CK mitigations (IP list)

ID	Name
M1056	Pre-compromise

TABLE 26 CIS Critical Security Controls (IP list)

Control	Name
18	Penetration Testing

Threat actors can use knowledge about an organization's IP addresses for attack purposes (The MITRE Corporation, 2021j). Public IP addresses are attractive from the perspective of an attacker. Organizations may be allocated a range of IP addresses, a block of IP addresses, or sequential IP addresses. Attackers can obtain useful information from these IP addresses, such as which addresses are in use, as well as organization size, Internet service provider, physical location, and hosting arrangement details for the public-facing infrastructure. As with domains, IP addresses can be acquired using techniques like as phishing, active scanning, and public databases.

The mitigation technique is the same as in the earlier domain scenario (The MITRE Corporation, 2021j). The activity of collecting IP addresses from organizations cannot be easily prevented, but the amount of information that can be collected should be minimized, especially in the case of sensitive information.

6.7 Remediation to Email list

In the case of Nasdaq Helsinki, a large number of results were discovered for lists of organizations' email addresses. The tables below illustrate which attack techniques and mitigations can be mapped to this type of result.

TABLE 27 MITRE ATT&CK attack techniques (email list)

ID	Name
T1566	Phishing
T1589.002	Email Addresses

TABLE 28 MITRE CAPEC attack patterns (email list)

ID	Name
98	Phishing

TABLE 29 MITRE ATT&CK mitigations (email list)

ID	Name
M1017	User Training
M1021	Restrict Web-Based Content
M1031	Network Intrusion Prevention
M1049	Antivirus/Antimalware
M1054	Software Configuration
M1056	Pre-compromise

TABLE 30 MITRE CAPEC mitigations (email list)

Related mitigations from MITRE CAPEC
- Do not follow any links that you receive within your e-mails and certainly do not input any login credentials on the page that they take you too. Instead, call your Bank, PayPal, eBay, etc., and inquire about the problem. A safe practice would also be to type the URL of your bank in the browser directly and only then log in. Also, never reply to any e-mails that ask you to provide sensitive information of any kind.

TABLE 31 CIS Critical Security Controls (email list)

Control	Name
2	Inventory and Control of Software Assets
9	Email and Web Browser Protections
13	Network Monitoring and Defense
14	Security Awareness and Skills Training

For usage in later phases of the cyber-attack lifecycle, threat actors may collect email addresses of the target organization (The MITRE Corporation, 2021h). Obtaining the email addresses of the target organization may be simple for attackers, as these addresses are typically available on the organization's website or through social media. Active scanning methods include systems that submit requests to authentication services and interpret answers, which may reveal the usernames of the target system. The collection of email addresses cannot be easily avoided, as was previously the case with domains and IP addresses. Even in this instance, the available information should be minimized as much as feasible.

After collecting the organization's email addresses, threat actors may move on to the next phase of their attack, which could involve phishing (The MITRE

Corporation, 2022g). Threat actors may send phishing emails to the collected email addresses in the hopes that recipients will reveal critical information, open malicious attachments, or click harmful links. On the target computer, infected attachments or links may subsequently execute malicious programs. Phishing is a sort of social engineering delivered electronically. Phishing can be a targeted assault, and so-called spear phishing or bulk phishing campaigns can be launched against all addresses. Phishing can be carried out via social networking platforms or other third-party services, and the phisher can masquerade as a trustworthy source.

Anti-malware or antivirus solutions can detect and quarantine suspicious phishing attachments automatically, thus enterprises should use this type of solution (The MITRE Corporation, 2022g). Additionally, network intrusion prevention systems (NIPS) could block suspicious files or links containing email attachments at the network level. Restrictions to web-based content should be considered by identifying websites and attachment kinds that are essential to company operations and allowing only those, particularly if network traffic cannot be properly controlled or if high-impact concerns are found. Also, organizations should use email authentication and anti-spoofing measures such as sender domain validity checks (SPF) and message integrity checks (DKIM). Adopting such methods might be accomplished, for instance, with DMARC policies. Also, user education cannot be emphasized enough in regards to phishing.

6.8 Remediation to Phone numbers

In the case of Nasdaq Helsinki, phone number-related information was found. The tables below illustrate which attack techniques and mitigations can be mapped to this type of finding.

TABLE 32 MITRE CAPEC attack patterns (phone numbers)

ID	Name
415	Pretexting via Phone

TABLE 33 CIS Critical Security Controls (phone numbers)

Control	Name
14	Security Awareness and Skills Training

Pretexting may be a sort of phone-based attack. In this attack, a threat actor may assume a trusted position with the intention of obtaining non-public information (The MITRE Corporation, 2021c). Another objective may be to convince the person who answers the phone to do what the threat actor desires. Phone pretexting is the most common sort of social engineering attack. The most popular and effective identities assumed by attackers are coworkers and computer technicians. Most usual targets are help desk staff. This threat can be reduced by educating people to spot these kind of attacks and making it clear what types of information are permissible to disclose and what kinds of actions cannot be taken when asked.

6.9 Remediation to Credit card number

The fast expansion of internet platforms has made data privacy a serious concern for society (Liu, et al., 2020). Personally identifiable information (PII) is one of the most common targets for cybercriminals and frequently finds up on the dark web hacker communities. In hacker communities, PII may be used in a variety of ways, including tax returns, medical claims, and false loan applications. These factors can result in financial losses and reputational harm. The cause of a PII leak is not always a data breach, but rather the unintended disclosure of PII over the internet. This may be occurring on a search engine or a social networking platform. This information can be exploited and used by hackers for their own benefit and goals. Leaked PII could include user information such as name, address, gender, age, education, and occupation. In 2018, Cambridge Analytica collected 87 million Facebook user profiles without their permission. Due to the fact that the elderly and children may not comprehend how to adequately protect themselves, they are a risk population that is susceptible to PII exposure.

Personal identifying information is for sale on the dark web (Liu, et al., 2020). Personal identifying information shows up on the dark web as a result of data breach attacks. PII is needed because it can be used to impersonate another person, i.e., for identity theft, and as a result, criminals can earn handsomely by submitting bogus credit applications or medical claims. In addition, it is possible to acquire a reputation as a hacker by distributing stolen PII. The exchange of PII with other hacker assets is also possible. There are three primary forms of stolen PII: social security numbers, payment card data, and online account information. This information is primarily accessible on the dark web via illegal marketplaces, carding forums, and hacker communities.

Exposed credit card information may be resold or used fraudulently (UNODC, 2020). The dark web has vast quantities of credit card information that can be sold to criminals, who can then use it to make fraudulent purchases or withdraw cash from the cards.

As the instance of Nasdaq Helsinki demonstrates, the dark web is a source for credit card numbers and other associated data. Thus, there were hits with the primary domain names of the case study organizations related with dark web content containing credit card details, such as carding forums. It is recommended to disclose discovered payment card information to the relevant parties so that these cards can be cancelled.

6.10 Remediation to Passport number

In the instance of Nasdaq Helsinki, associated results included passport numbers. It indicates that domain names of organizations were discovered on sites where these numbers occur. Additional research is required to deter potential threats. If the numbers revealed are authentic numbers from legitimate passports, a data breach may have occurred. This can lead to identity theft and unauthorized access via third parties such as banks, resulting in monetary losses.

6.11 Remediation to Access for sale

Currently, as-a-service models for cybercrime skills are also accessible (Huang, Siegel, & Madnick, 2018). More and more brilliant hackers are drawn to careers as professional hackers, and as a result, cyberattacks are better organized. Threat actors can purchase attack services from the dark web without being required to understand the attack's execution.

In the context of "access for sale," "access" is an umbrella phrase on the dark web for any type of remote computer access (Positive Technologies, 2020). This indicates that unauthorized access to remote machines can be achieved using exploits, credentials, software, or any other means. Therefore, a hacker can, for instance, steal passwords or break into networks in some manner and sell access on the dark web.

Previously, less-skilled hackers struggled to develop attacks to the point where they could make money from attacks (Positive Technologies, 2020). Now since they may sell their services or accomplishments to other criminals, they do not have to leave without the money. For difficult tasks such as obtaining domain administrator rights or infecting high-priority servers with malware, more expert hackers can be recruited.

Large organizations will be at risk of becoming a source of easy money for less trained hackers, and external attacks will increase dramatically (Positive Technologies, 2020). Due to the prevalence of remote work from home, this threat is quite topical at present. The network perimeter is scanned by threat actors seeking for any security vulnerabilities. When software upgrades are not performed, when online applications lack the proper type of protection, when misconfiguration exists, or when administration access is poorly protected, such as with a weak password, entry points may be discovered. It is important to remember that the bigger the earnings of an attack, the larger the hacked organization and the wider the powers obtained.

It is commonly believed that larger organizations face less risk from less-skilled hackers since they have more money to spend on system security than smaller and medium-sized businesses (Positive Technologies, 2020). However, this is not the case, and even hackers without specific skills will be able to find security flaws in huge corporations. Smaller organizations are typically more vulnerable since they have fewer resources to invest in security.

Whether it's a perimeter network or a local network, organizations should safeguard their infrastructure thoroughly (Positive Technologies, 2020). All services must be adequately safeguarded and monitored to detect potential intruders in advance. In addition, it is essential to conduct routine inspections and analyses of past security events in order to discover probable missed attacks and eliminate prospective dangers before criminals act to disrupt business or steal data.

When servers have been compromised, hackers will sometimes remain unseen and keep access they have gained (UNODC, 2020). In this instance, the target will be blissfully unaware of this circumstance. This type of access is extremely valuable and comparable to currency. There are also separate groups for certain actions. One group may be skilled in acquiring unauthorized access, while another may be specialized in conducting actual operations against organizations. The group with unlawful access to organization systems will sell that information to the operations team. There are remote access credentials for sale on the dark web by international gangs specializing in unauthorized access. The buyer will receive instructions on how to remotely access the target organization when the vendor receives payment.

Access available for purchase If genuine credentials are used to provide access for sale, then surface exposure may lead to the same vulnerabilities as those stated for cleartext passwords. It is essential to explore more and see how potential access for sale is organized. This allows for the identification of potential threats and the implementation of appropriate mitigations.

6.12 Remediation to Obtainable capabilities

A substantial quantity of cyber assets, such as malicious hacking tools, can be discovered on the dark web (Samtani, Li, Benjamin, & Chen, 2021). These technologies and extensive knowledge of dark web cybercriminals have made large-scale cyberattacks possible. When the Mirai botnet was disclosed on forums, it infected millions of IoT devices and performed a denial-of-service attack against major DNS servers on the internet. Even free hacking tutorials and exploits can be obtained on dark web hacker forums.

In addition, malware that steals sensitive data has been purchased on the dark web and utilized in large data breaches (Finklea, 2017). With the assistance of this type of malware, unencrypted payment card information has been obtained. A RAM (random-access memory) scraper is one sort of malware used in this type of attack.

TABLE 34 MITRE ATT&CK attack techniques (obtainable capabilities)

ID	Name
T1588.001	Malware

T1588.002	Tool
T1588.005	Exploits

TABLE 35 MITRE CAPEC attack patterns (obtainable capabilities)

ID	Name
529	Malware-Directed Internal Reconnaissance

TABLE 36 MITRE ATT&CK mitigations (obtainable capabilities)

ID	Name
M1056	Pre-compromise

TABLE 37 MITRE CAPEC mitigations (obtainable capabilities)

Related mitigations from MITRE CAPEC
- Keep patches up to date by installing weekly or daily if possible. - Identify programs that may be used to acquire peripheral information and block them by using a software restriction policy or tools that restrict program execution by using a process allowlist.

TABLE 38 CIS Critical Security Controls (obtainable capabilities)

Control	Name
2	Inventory and Control of Software Assets
7	Continuous Vulnerability Management
10	Malware Defenses
16	Application Software Security
18	Penetration Testing

Malware may be purchased by threat actors for use in cyberattacks (The MITRE Corporation, 2021l). Malware can be used for support operations, remote machine control, defensive evasion, and post-compromise operations. Malware can also be obtained for free.

In a similar manner, threat actors may purchase or otherwise acquire attack tools (The MITRE Corporation, 2021m). These tools can be offered for free or for a fee, using closed or open source source code. The distinction between these tools and malware is that malware is designed for malevolent intentions, whereas these tools are typically not. Cobalt Strike is an example of a term designed for red teaming.

Threat actors may also obtain exploits that are ready for use. There are flaws and vulnerabilities in both computer hardware and software (The MITRE

Corporation, 2021k). Exploits can be used to exploit these flaws and vulnerabilities in order to trigger unanticipated behavior on the targets. Obtaining these exploits is identical to obtaining malware or tools. These items can be stolen, bought, or downloaded for no cost. A threat actor may monitor exploit supplier forums in order to learn about new exploits. Systems may remain vulnerable to new attacks until these exploits are made public or patches are developed and installed.

Due to factors beyond the control of organizations, preventing the acquisition of these three attack capabilities may be difficult. Mitigations and controls indicated in Tables 37 and 38 may still be effective against threats posed by these capabilities.

6.13 Remediation to Source code

As previously mentioned in the chapter on surface exposure, there may be multiple types of threats associated with this surface exposure, making it difficult to provide remediation methods. If source code is suspected to be exploit code, the preceding section 6.12 outlines a few possible solutions. As source code may be tied to a variety of factors, it is preferable to explore more to determine the nature of the threat and then take the appropriate measures.

6.14 Remediation to Cryptocurrency addresses

Bitcoin was the first cryptocurrency, and darknet merchants used it as a payment method after its inception in 2019 (UNODC, 2020). Bitcoin offers sufficient anonymity for use in these marketplaces, where trading is frequently illegal. Consequently, cryptocurrencies are the predominant payment methods on the dark web.

In addition to Bitcoin, there are numerous other cryptocurrencies nowadays. Various addresses associated with cryptocurrencies such as Bitcoin, Neo, Litecoin, and Monero were disclosed in the case of Nasdaq Helsinki. The inclusion of these Bitcoin addresses on websites where domain names of companies are mentioned may pose a threat to organizations. Further study is required to determine the nature of these potential threats, which may be associated with the sale of prohibited items.

6.15 Remediation to Black markets

The anonymous marketplaces on the dark web, often known as black markets, are the primary source of cybercriminals' cybercrime tools, as well as stolen or leaked data (Nazah, Huda, Abawajy, & Hassan, 2020). Silk Road, Sheep Market, and the Black Market Reloaded are a few instances of this type of marketplace. In addition, these markets sell drugs, pornography, firearms, financial records, credit card information, and other sensitive data.

These marketplaces can also be referred to as cryptomarkets because vendors and buyers deal using cryptocurrencies such as Bitcoin (Aldridge & Decary-Hetu, 2016). There are more approaches involved in protecting the identities of transaction participants. Tor is one of these identity protection methods, concealing the true IP-address of users and the location of marketplace servers. These marketplaces have the same look and feel as the well-known marketplaces on the surface web, such as eBay and Amazon. It is equally possible to look for and compare products and vendors.

Black markets have expanded throughout time based on numerous indications (UNODC, 2020). For instance, the number of marketplaces in 2011 was one, but in 2019 there are 118. In addition, both the variety of available products and the total number of items for sale have grown substantially. Between 2015 and 2018, the number of products for sale at the Valhalla marketplace grew from 5,000 to 13,000, illustrating an increase in product availability. In addition to hacking tools, related services are currently accessible. There are additional marketplaces specializing in certain products, such as fraudulent documents or credit card information. User interfaces have also improved from the vendor's perspective, permitting, among other things, the ordering of numerous items in the single shipment. Additionally, vendor awareness has increased regarding the possibility of authorities shutting down marketplaces, resulting in vendors operating in parallel across many platforms.

Without a context, results linked to sources such as illicit markets require further examination to determine whether or not there is a threat. Without knowledge of a threat, it is impossible to identify mitigating measures.

6.16 Remediation to Discussion forums

It has been determined that underground discussion sites share leaked personal information, and that these forums are the primary locations where such information will be distributed (Fang, Guo, Huang, & Liu, 2019). It may be claimed that these forums have strengthened their position as a source of information from data breaches since an increasing amount of stolen data is shared on them.

There are specialized hacker forums where hackers share knowledge regarding source code, hacking methods, hacking tools, and other dangerous assets (Liu, et al., 2020). These forums can provide access to previously disclosed credentials or passwords. Occasionally, this type of compromised material is even freely distributed.

Underground forums are one of the primary means via which hackers communicate (Fang, Guo, Huang, & Liu, 2019). The two primary activity on these forums are conducting business and harmful acts. In addition to technology-related content, the forums also contain information regarding security incidents.

Additionally, there exist communities whose primary goal is to exchange leaked material, such as databases. Thus, the disclosed data is discussed in these forums, along with the most recent data breaches. Frequently, hackers will declare that they have obtained stolen or leaked data. This results in cases when online forums may be the earliest hint of data breaches. Leaked information may originate from organizations or individuals.

If this type of surface exposure is discovered, further studies should be conducted to identify potential threats. Only then is it able to implement tailored mitigations.

6.17 Remediation to DeepPaste

There are web programs known as pastebins (Matic, Fattori, Bruschi, & Cavallaro, 2012). These pastebins allow users to share text-based information using pastes. It is known that malicious and sensitive content is posted publicly in these pastebins. Information can be shared anonymously by simply entering the desired text into the application, which then generates a URL that can be used to forward the pasted information.

DeepPaste is a dark web pastebin application. Nasdaq Helsinki had a small number of DeepPaste hits. This indicates that a domain name for an organization has been extracted from DeepPaste contents. Additional research should be conducted to identify potential threats to organizations.

6.18 Summary

In this chapter, numerous types of threats from the dark web were discussed. Some of these were mappable to MITRE ATT&CK, MITRE CAPEC, and CIS Controls, while others were not. Figure 2 illustrates surface exposures mapped to MITRE ATT&CK attack tactics and mitigations. When surface exposures are identified, the proposed immediate remediation measures are listed in Table 39. Targeted surface exposure mitigations are discussed in earlier sections of this chapter. If specific mitigations do not exist, it is advisable to examine the organization's security measures in depth. Regardless of the circumstances, it is suggested to employ extensive and systematic security measures, such as the CIS Controls mentioned in Appendix 1, and of those, at least IG1 "important cyber hygiene"-related controls and safeguards.

TABLE 39 Proposed immediate remediations

Surface exposure	Immediate remediations
Access for sale	Determine how access is organized and implement appropriate countermeasures and mitigations.

Black markets	Investigate more to identify threats.
Cleartext password	Change exposed passwords immediately.
Credit card number	Ensure that all compromised credit cards are cancelled.
Cryptocurrency addresses	Investigate more to identify threats.
DeepPaste	Investigate more to identify threats.
Discussion forums	Investigate more to identify threats.
Domain list	Examine the security of the systems linked with the mentioned domains at a minimum.
Email list	Inform personnel of potential upcoming phishing attacks.
Hacktivist campaign	Attempts should be made to placate protesters if feasible. Prepare for DDoS attacks at minimum.
IP list	Check to see if the security measures of the systems linked with the specified IP addresses are adequate.
Obtainable capabilities	Investigate more to identify threats.
Passport number	Whenever possible, inform those affected.
Password hash	Change exposed passwords.
PGP key	Expand your investigation to detect threats. If it is a private key, immediately revoke any associated keys and discontinue use of the keypair.
Phone numbers	Inform personnel of possible incoming phone-based social engineering assaults.
Source code	Investigate more to identify threats.

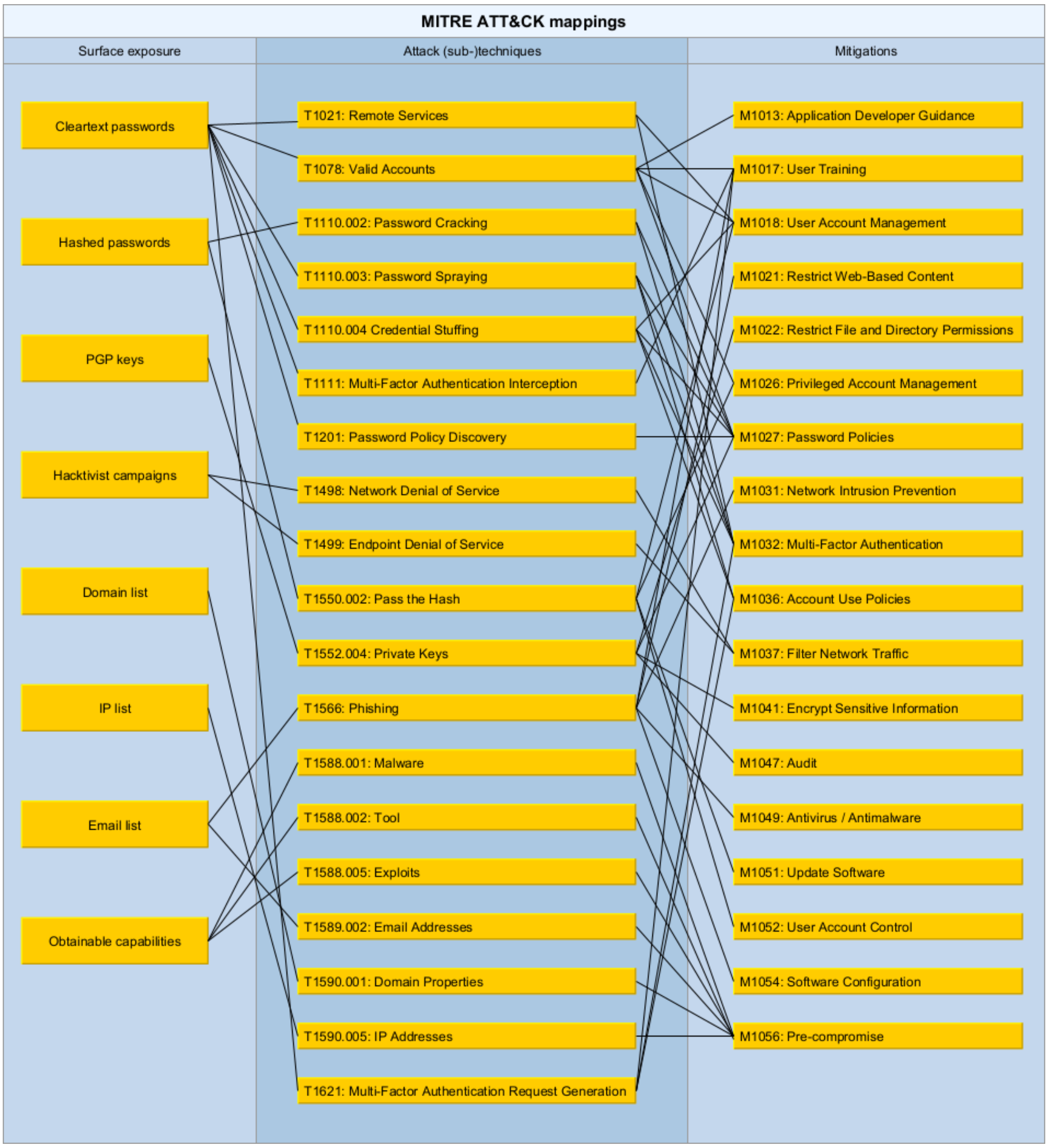
MITRE ATT&CK mappings
Surface exposure
Attack (sub-)techniques
Mitigations
Cleartext passwords
Hashed passwords
PGP keys
Hacktivist campaigns
Domain list
IP list
Email list
Obtainable capabilities
T1021: Remote Services
T1078: Valid Accounts
T1110.002: Password Cracking
T1110.003: Password Spraying
T1110.004 Credential Stuffing
T1111: Multi-Factor Authentication Interception
T1201: Password Policy Discovery
T1498: Network Denial of Service
T1499: Endpoint Denial of Service
T1550.002: Pass the Hash
T1552.004: Private Keys
T1566: Phishing
T1588.001: Malware
T1588.002: Tool
T1588.005: Exploits
T1589.002: Email Addresses
T1590.001: Domain Properties
T1590.005: IP Addresses
T1621: Multi-Factor Authentication Request Generation
M1013: Application Developer Guidance
M1017: User Training
M1018: User Account Management
M1021: Restrict Web-Based Content
M1022: Restrict File and Directory Permissions
M1026: Privileged Account Management
M1027: Password Policies
M1031: Network Intrusion Prevention
M1032: Multi-Factor Authentication
M1036: Account Use Policies
M1037: Filter Network Traffic
M1041: Encrypt Sensitive Information
M1047: Audit
M1049: Antivirus / Antimalware
M1051: Update Software
M1052: User Account Control
M1054: Software Configuration
M1056: Pre-compromise

FIGURE 2 MITRE ATT&CK mappings

7 CONCLUSION

The topic of this study was initially presented in Chapter 2 as the dark web and Tor. These were discussed in detail in the same chapter. Chapter 3 describes how this study was conducted. The following research questions were introduced in that section:

- RQ1: How can organizations prepare for emerging threats from the dark web?
    - RQ1a: How can threat actors exploit the dark web information for cyber-attacks?
    - RQ1b: How can targets mitigate threats or remediate the situation of being exposed to cyber-attacks?

The research strategy was a case study, and the case concerned the surface exposure of Nasdaq Helsinki-listed companies. Each company was associated with a single domain name. These domain names served as search terms for Cyber Intelligence House's dark web data. That methodology chapter also provided a quick introduction to the frameworks used for mapping attack techniques and patterns as well as potential mitigations against findings.

In Chapter 4, results were presented. Bitcoin address, cleartext password, credentials for sale, credit card number, DeepPaste, discussion, domain list, email list, hacking for sale, hack-tivist campaign, hashed password, Litecoin address, malware for sale, marketplace, Monero address, Neo address, Nmap, passport number, PGP key, phone numbers, source code, SQL, and username were discovered. Except for results linked to email lists and cleartext passwords, the median number of findings across businesses was zero. This was a situation, for instance, including discussions and hashed passwords, despite the fact that there were a substantial number of discoveries involving those topics. This raises the issue, should businesses be concerned if they have findings? It appears that approximately 70% of Nasdaq Helsinki-listed companies have exposures, which suggests that private companies who operate in a similar manner or are substantially comparable to these companies should examine their exposures.

In Chapter 5, the phrase surface exposure was introduced, which refers to factors that raise possible cyber compromise vectors. All findings presented in Chapter 4 can be categorized as surface exposures. These have been classified under the proper headings, which provide concise summaries of their contents. In addition, the entire number of findings from the study is shown, along with some suggestions about how these may be utilized in cyberattacks.

In Chapter 6, surface exposures were mapped to MITRE ATT&CK attack methodologies, MITRE CAPEC attack patterns, and, when relevant, mitigations for both. In addition, relevant CIS Controls were mapped to the attack tactics and patterns that were mapped. In the summary part, there is also a table that proposes quick measures that can be taken upon finding a dark web threat targeted at the organization. When organizations confront these results, they can use the preceding findings and remedies as assistance. Accordingly, Chapter 6 provides answers to all of the study's research questions. The answer to RQ1a is that threat actors can exploit all of these surface exposures for malicious reasons, as detailed in Chapter 6. Answers to RQ1 and RQ1b suggest that organizations can prepare for emerging threats from the dark web by adopting a dark web monitoring or cyber threat intelligence service to determine their cyber exposure and by implementing the appropriate mitigations, controls, or safeguards.

This study's contribution was to map dark web surface exposures to known cyber-attack techniques and patterns, as well as mitigating or corrective measures. As demonstrated by this case study, the dark web contains a plethora of surface exposures to organizations. Some of these can be utilized by threat actors in cyber-attacks, while others may suggest ongoing events or potential cyber-attacks. The first two CIS Controls are concerned with inventorying and controlling various types of assets, including hardware and software assets. When the existence of assets is known, inventorying helps to safeguard them. Similarly, if organizations are unaware of their cyber exposure on the dark web, they may not secure themselves adequately. Based on this, it can be concluded that monitoring the dark web and extracting information from it is profitable and recommended for preserving the information systems, assets, and business continuity of enterprises. In other words, enterprises can receive early warnings of cyber threats based on dark web cyber threat intelligence. Compared to other reactive methods, such as analyzing security event logs after a successful cyberattack on an organization, this might be referred to as proactive cyber threat intelligence. In addition, every company should adopt at least the IG1 group safeguards from the CIS Controls, also known as "essential cyber hygiene," in order to prepare for known and possibly unforeseen threats.

8 LIMITATIONS AND FUTURE WORK

It would be interesting to know what percentage of hashes can be cracked in a reasonable amount of time, as some hashed passwords are easier to decipher than others. Additionally, some businesses received greater visibility than others. This raises the question of what features make businesses more vulnerable.

Remediations are merely a proposal, which has not been evaluated or ranked based on their feasibility or speed. That is a topic worthy of deeper examination. Overall, the sample reflects a small number of companies, hence the findings cannot be extrapolated beyond public companies in Finland. Additionally, only one domain name per organization was utilized as a keyword in the case study. In reality, companies may own numerous domain names, and these should all be included. The MITRE corporation also has the DEFEND framework, which can be mapped, and the CIS Controls' safeguards could be mapped completely.

It is also important to understand that the data used cannot cover all locations on the dark web, but they do cover a substantial number of significant locations. There may be additional data sources for cyber threat information in addition to the dark web. The deep web, the surface web, and data already compromised could be added to data sources. Additionally, several darknets could be included as sources.

REFERENCES

Akhgar, B., Gercke, M., Vrochidis, S., & Gibson, H. (2021). *Dark Web Investigation.* Springer.

Aldridge, J., & Decary-Hetu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy, 35*, 7-15.

Basheer, R., & Alkhatib, B. (2021). Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. *Journal of Computer Networks and Communications, 2021*, 1-21.

Benjamin, V., Valacich, J., & Chen, H. (2019). DICE-E: A Framework for Conducting Darknet Identification, Collection, Evaluation, with Ethics. *MIS Quarterly, 43*(1), 1-22.

Ebrahimi, M., Nunamaker Jr, J., & Chen, H. (2020). Semi-Supervised Cyber Threat Identification in Dark Net Markets: A Transductive and Deep Learning Approach. *Journal of Management Information Systems, 37*(3), 694-722.

Fang, Y., Guo, Y., Huang, C., & Liu, L. (2019). Analyzing and Identifying Data Breaches in Underground Forums. *IEEE Access, 7*, 48770-48777.

Finklea, K. (2017). *Dark Web.* U.S. Congressional Research Service.

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically Understanding the Cyber Attack Business: A Survey. *ACM Computing Surveys, 51*(4), 1-36.

Jardine, E. (2019). The trouble with (supply-side) counts: the potential and limitations of counting sites, vendors or products as a metric for threat trends on the Dark Web. *INTELLIGENCE AND NATIONAL SECURITY, 34*(1), 95-111.

Liu, Y., Lin, F. Y., Ahmad-Post, Z., Ebrahimi, M., Zhang, N., Hu, J. L., . . . Chen, H. (2020). Identifying, Collecting, and Monitoring Personally Identifiable Information: From the Dark Web to the Surface Web. *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 1-6). IEEE.

Matic, S., Fattori, A., Bruschi, D., & Cavallaro, L. (2012). Peering into the Muddy Waters of Pastebin. *ERCIM NEWS 90*(90), 16-17.

Mazurczyk, W., & Caviglione, L. (2021, March). Cyber Reconnaissance Techniques. *Communications of the ACM, 64*(3), 86-95.

Nasdaq, Inc. (n.d.). *Companies listed on Nasdaq Helsinki*. Retrieved March 19, 2022, from Nasdaq Nordic: http://www.nasdaqomxnordic.com/shares/listed-companies/helsinki

Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. *IEEE Access, 8*, 171796-171819.

Nurmi, J., & Niemelä, M. S. (2018). PESTEL Analysis of Hacktivism Campaign Motivations. *Nordic Conference on Secure IT Systems* (pp. 323-335). Springer.

OpenPGP. (2020, November 25). *About*. Retrieved April 30, 2022, from OpenPGP: https://www.openpgp.org/about/

Positive Technologies. (2020, May 20). *Access for sale*. Retrieved April 18, 2022, from Positive Technologies: https://www.ptsecurity.com/ww-en/analytics/access-for-sale-2020/

Samtani, S., Chinn, R., Chen, H., & Nunamaker Jr, J. (2017). Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. *Journal of Management Information Systems, 34*(4), 1023-1053.

Samtani, S., Li, W., Benjamin, V., & Chen, H. (2021). Informing Cyber Threat Intelligence through DarkWeb Situational Awareness: The AZSecure Hacker Assets Portal. *Digital Threats: Research and Practice, 2*(4).

Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., . . . Wolf, R. D. (2017). *Finding Cyber Threats with ATT&CK™-Based Analytics.* The MITRE Corporation.

The Center for Internet Security, Inc. (2021). *CIS Critical Security Controls Version 8*. The Center for Internet Security, Inc. (CIS).

The MITRE Corporation. (2019a, April 4). *About CAPEC*. Retrieved May 1, 2022, from Common Attack Pattern Enumeration and Classification (CAPEC): https://capec.mitre.org/about/index.html

The MITRE Corporation. (2019b, October 16). *ATT&CK Comparison*. Retrieved May 1, 2022, from Common Attack Pattern Enumeration and Classification (CAPEC): https://capec.mitre.org/about/attack_comparison.html

The MITRE Corporation. (2020, March 29). *Unsecured Credentials: Private Keys*. Retrieved April 29, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1552/004/

The MITRE Corporation. (2021a, April 6). *Brute Force: Credential Stuffing*. Retrieved April 29, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1110/004/

The MITRE Corporation. (2021b, April 6). *Brute Force: Password Spraying*. Retrieved April 29, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1110/003/

The MITRE Corporation. (2021c, October 21). *CAPEC-415: Pretexting via Phone*. Retrieved April 30, 2022, from Common Attack Pattern Enumeration and

Classification (CAPEC): https://capec.mitre.org/data/definitions/415.html

The MITRE Corporation. (2021d, October 21). *CAPEC-474: Signature Spoofing by Key Theft*. Retrieved April 30, 2022, from Common Attack Pattern Enumeration and Classification (CAPEC): https://capec.mitre.org/data/definitions/474.html

The MITRE Corporation. (2021e, October 21). *CAPEC-49: Password Brute Forcing*. Retrieved April 29, 2022, from Common Attack Pattern Enumeration and Classification (CAPEC): https://capec.mitre.org/data/definitions/49.html

The MITRE Corporation. (2021f, October 21). *CAPEC-55: Rainbow Table Password Cracking*. Retrieved April 29, 2022, from Common Attack Pattern Enumeration and Classification (CAPEC): https://capec.mitre.org/data/definitions/55.html

The MITRE Corporation. (2021g, October 21). *CAPEC-560: Use of Known Domain Credentials*. Retrieved April 18, 2022, from Common Attack Pattern Enumeration and Classification (CAPEC): https://capec.mitre.org/data/definitions/560.html

The MITRE Corporation. (2021h, December 9). *Gather Victim Identity Information: Email Addresses*. Retrieved April 30, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1589/002/

The MITRE Corporation. (2021i, April 15). *Gather Victim Network Information: Domain Properties*. Retrieved April 30, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1590/001/

The MITRE Corporation. (2021j, April 15). *Gather Victim Network Information: IP Addresses*. Retrieved April 30, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1590/005/

The MITRE Corporation. (2021k, April 15). *Obtain Capabilities: Exploits*. Retrieved May 5, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1588/005/

The MITRE Corporation. (2021l, October 17). *Obtain Capabilities: Malware*. Retrieved May 5, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1588/001/

The MITRE Corporation. (2021m, October 17). *Obtain Capabilities: Tool*. Retrieved May 5, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1588/002/

The MITRE Corporation. (2021n, August 31). *Use Alternate Authentication Material: Pass the Hash*. Retrieved April 29, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1550/002/

The MITRE Corporation. (2022a, April 19). *Brute Force: Password Cracking*. Retrieved April 29, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1110/002/

The MITRE Corporation. (2022b, April 12). *Endpoint Denial of Service*. Retrieved April 30, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1499/

The MITRE Corporation. (2022c, April 1). *Multi-Factor Authentication Interception*. Retrieved April 29, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1111/

The MITRE Corporation. (2022d, April 20). *Multi-Factor Authentication Request Generation*. Retrieved April 29, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1621/

The MITRE Corporation. (2022e, March 25). *Network Denial of Service*. Retrieved April 30, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1498/

The MITRE Corporation. (2022f, April 20). *Password Policy Discovery*. Retrieved April 29, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1201/

The MITRE Corporation. (2022g, January 4). *Phishing*. Retrieved April 30, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1566/

The MITRE Corporation. (2022h, March 28). *Remote Services*. Retrieved April 29, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1021/

The MITRE Corporation. (2022i, April 1). *Valid Accounts*. Retrieved April 29, 2022, from MITRE ATT&CK: https://attack.mitre.org/techniques/T1078/

The Tor Project, I. (n.d.). *How can we help?* Retrieved April 26, 2022, from Tor Project: https://support.torproject.org/

UNODC. (2020). *Darknet Cybercrime Threats to Southest Asia.* United Nations Office on Drugs and Crime (UNODC).

Woods, D. W., & Böhme, R. (2021). Systematization of Knowledge: Quantifying Cyber Risk. *42nd IEEE Symposium on Security and Privacy.*

Yin, R. K. (2003). *Case Study Research: Design and Methods (Third Edition).* SAGE Publications.

APPENDIX 1 CIS CONTROLS AND SAFEGUARDS

The CIS Controls (v8) are listed in the table below (The Center for Internet Security, Inc., 2021).

ID	Name
1	Inventory and Control of Enterprise Assets
2	Inventory and Control of Software Assets
3	Data Protection
4	Secure Configuration of Enterprise Assets and Software
5	Account Management
6	Access Control Management
7	Continuous Vulnerability Management
8	Audit Log Management
9	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

The safeguards of the CIS Controls (v8) are listed in the table below (The Center for Internet Security, Inc., 2021). The main number of the identifiers (IDs) indicates the relevant CIS Control from the preceding list.

ID	Asset Type	Title	IG1	IG2	IG3
1.1	Devices	Establish and Maintain Detailed Enterprise Asset Inventory	x	x	x
1.2	Devices	Address Unauthorized Assets	x	x	x
1.3	Devices	Utilize an Active Discovery Tool		x	x
1.4	Devices	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		x	x
1.5	Devices	Use a Passive Asset Discovery Tool			x

2.1	Applications	Establish and Maintain a Software Inventory	x	x	x
2.2	Applications	Ensure Authorized Software is Currently Supported	x	x	x
2.3	Applications	Address Unauthorized Software	x	x	x
2.4	Applications	Utilize Automated Software Inventory Tools		x	x
2.5	Applications	Allowlist Authorized Software		x	x
2.6	Applications	Allowlist Authorized Libraries		x	x
2.7	Applications	Allowlist Authorized Scripts			x
3.1	Data	Establish and Maintain a Data Management Process	x	x	x
3.2	Data	Establish and Maintain a Data Inventory	x	x	x
3.3	Data	Configure Data Access Control Lists	x	x	x
3.4	Data	Enforce Data Retention	x	x	x
3.5	Data	Securely Dispose of Data	x	x	x
3.6	Devices	Encrypt Data on End-User Devices	x	x	x
3.7	Data	Establish and Maintain a Data Classification Scheme		x	x
3.8	Data	Document Data Flows		x	x
3.9	Data	Encrypt Data on Removable Media		x	x
3.1	Data	Encrypt Sensitive Data in Transit		x	x
3.11	Data	Encrypt Sensitive Data at Rest		x	x
3.12	Network	Segment Data Processing and Storage Based on Sensitivity		x	x
3.13	Data	Deploy a Data Loss Prevention Solution			x
3.14	Data	Log Sensitive Data Access			x
4.1	Applications	Establish and Maintain a Secure Configuration Process	x	x	x
4.2	Network	Establish and Maintain a Secure Configuration Process for Network Infrastructure	x	x	x
4.3	Users	Configure Automatic Session Locking on Enterprise Assets	x	x	x
4.4	Devices	Implement and Manage a Firewall on Servers	x	x	x
4.5	Devices	Implement and Manage a Firewall on End-User Devices	x	x	x
4.6	Network	Securely Manage Enterprise Assets and Software	x	x	x
4.7	Users	Manage Default Accounts on Enterprise Assets and Software	x	x	x

4.8	Devices	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		x	x
4.9	Devices	Configure Trusted DNS Servers on Enterprise Assets		x	x
4.1	Devices	Enforce Automatic Device Lockout on Portable End-User Devices		x	x
4.11	Devices	Enforce Remote Wipe Capability on Portable End-User Devices		x	x
4.12	Devices	Separate Enterprise Workspaces on Mobile End-User Devices			x
5.1	Users	Establish and Maintain an Inventory of Accounts	x	x	x
5.2	Users	Use Unique Passwords	x	x	x
5.3	Users	Disable Dormant Accounts	x	x	x
5.4	Users	Restrict Administrator Privileges to Dedicated Administrator Accounts	x	x	x
5.5	Users	Establish and Maintain an Inventory of Service Accounts		x	x
5.6	Users	Centralize Account Management		x	x
6.1	Users	Establish an Access Granting Process	x	x	x
6.2	Users	Establish an Access Revoking Process	x	x	x
6.3	Users	Require MFA for Externally-Exposed Applications	x	x	x
6.4	Users	Require MFA for Remote Network Access	x	x	x
6.5	Users	Require MFA for Administrative Access	x	x	x
6.6	Users	Establish and Maintain an Inventory of Authentication and Authorization Systems		x	x
6.7	Users	Centralize Access Control		x	x
6.8	Data	Define and Maintain Role-Based Access Control			x
7.1	Applications	Establish and Maintain a Vulnerability Management Process	x	x	x
7.2	Applications	Establish and Maintain a Remediation Process	x	x	x
7.3	Applications	Perform Automated Operating System Patch Management	x	x	x
7.4	Applications	Perform Automated Application Patch Management	x	x	x
7.5	Applications	Perform Automated Vulnerability Scans of Internal Enterprise Assets		x	x

7.6	Applications	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		x	x
7.7	Applications	Remediate Detected Vulnerabilities		x	x
8.1	Network	Establish and Maintain an Audit Log Management Process	x	x	x
8.2	Network	Collect Audit Logs	x	x	x
8.3	Network	Ensure Adequate Audit Log Storage	x	x	x
8.4	Network	Standardize Time Synchronization		x	x
8.5	Network	Collect Detailed Audit Logs		x	x
8.6	Network	Collect DNS Query Audit Logs		x	x
8.7	Network	Collect URL Request Audit Logs		x	x
8.8	Devices	Collect Command-Line Audit Logs		x	x
8.9	Network	Centralize Audit Logs		x	x
8.1	Network	Retain Audit Logs		x	x
8.11	Network	Conduct Audit Log Reviews		x	x
8.12	Data	Collect Service Provider Logs			x
9.1	Applications	Ensure Use of Only Fully Supported Browsers and Email Clients	x	x	x
9.2	Network	Use DNS Filtering Services	x	x	x
9.3	Network	Maintain and Enforce Network-Based URL Filters		x	x
9.4	Applications	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		x	x
9.5	Network	Implement DMARC		x	x
9.6	Network	Block Unnecessary File Types		x	x
9.7	Network	Deploy and Maintain Email Server Anti-Malware Protections			x
10.1	Devices	Deploy and Maintain Anti-Malware Software	x	x	x
10.2	Devices	Configure Automatic Anti-Malware Signature Updates	x	x	x
10.3	Devices	Disable Autorun and Autoplay for Removable Media	x	x	x
10.4	Devices	Configure Automatic Anti-Malware Scanning of Removable Media		x	x
10.5	Devices	Enable Anti-Exploitation Features		x	x
10.6	Devices	Centrally Manage Anti-Malware Software		x	x
10.7	Devices	Use Behavior-Based Anti-Malware Software		x	x
11.1	Data	Establish and Maintain a Data Recovery Process	x	x	x

11.2	Data	Perform Automated Backups	x	x	x
11.3	Data	Protect Recovery Data	x	x	x
11.4	Data	Establish and Maintain an Isolated Instance of Recovery Data	x	x	x
11.5	Data	Test Data Recovery		x	x
12.1	Network	Ensure Network Infrastructure is Up-to-Date	x	x	x
12.2	Network	Establish and Maintain a Secure Network Architecture		x	x
12.3	Network	Securely Manage Network Infrastructure		x	x
12.4	Network	Establish and Maintain Architecture Diagram(s)		x	x
12.5	Network	Centralize Network Authentication, Authorization, and Auditing (AAA)		x	x
12.6	Network	Use of Secure Network Management and Communication Protocols		x	x
12.7	Devices	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		x	x
12.8	Devices	Establish and Maintain Dedicated Computing Resources For all Administrative Work			x
13.1	Network	Centralize Security Event Alerting		x	x
13.2	Devices	Deploy a Host-Based Intrusion Detection Solution		x	x
13.3	Network	Deploy a Network Intrusion Detection Solution		x	x
13.4	Network	Perform Traffic Filtering Between Network Segments		x	x
13.5	Devices	Manage Access Control for Remote Assets		x	x
13.6	Network	Collect Network Traffic Flow Logs		x	x
13.7	Devices	Deploy a Host-Based Intrusion Prevention Solution			x
13.8	Network	Deploy a Network Intrusion Prevention Solution			x
13.9	Devices	Deploy Port-Level Access Control			x
13.1	Network	Perform Application Layer Filtering			x
13.11	Network	Tune Security Event Alerting Thresholds			x
14.1	N/A	Establish and Maintain a Security Awareness Program	x	x	x

14.2	N/A	Train Workforce Members to Recognize Social Engineering Attacks	x	x	x
14.3	N/A	Train Workforce Members on Authentication Best Practices	x	x	x
14.4	N/A	Train Workforce on Data Handling Best Practices	x	x	x
14.5	N/A	Train Workforce Members on Causes of Unintentional Data Exposure	x	x	x
14.6	N/A	Train Workforce Members on Recognizing and Reporting Security Incidents	x	x	x
14.7	N/A	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	x	x	x
14.8	N/A	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	x	x	x
14.9	N/A	Conduct Role-Specific Security Awareness and Skills Training		x	x
15.1	N/A	Establish and Maintain an Inventory of Service Providers	x	x	x
15.2	N/A	Establish and Maintain a Service Provider Management Policy		x	x
15.3	N/A	Classify Service Providers		x	x
15.4	N/A	Ensure Service Provider Contracts Include Security Requirements		x	x
15.5	N/A	Assess Service Providers			x
15.6	Data	Monitor Service Providers			x
15.7	Data	Securely Decommission Service Providers			x
16.1	Applications	Establish and Maintain a Secure Application Development Process		x	x
16.2	Applications	Establish and Maintain a Process to Accept and Address Software Vulnerabilities		x	x
16.3	Applications	Perform Root Cause Analysis on Security Vulnerabilities		x	x
16.4	Applications	Establish and Manage an Inventory of Third-Party Software Components		x	x
16.5	Applications	Use Up-to-Date and Trusted Third-Party Software Components		x	x
16.6	Applications	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		x	x

16.7	Applications	Use Standard Hardening Configuration Templates for Application Infrastructure		x	x
16.8	Applications	Separate Production and Non-Production Systems		x	x
16.9	Applications	Train Developers in Application Security Concepts and Secure Coding		x	x
16.1	Applications	Apply Secure Design Principles in Application Architectures		x	x
16.11	Applications	Leverage Vetted Modules or Services for Application Security Components		x	x
16.12	Applications	Implement Code-Level Security Checks			x
16.13	Applications	Conduct Application Penetration Testing			x
16.14	Applications	Conduct Threat Modeling			x
17.1	N/A	Designate Personnel to Manage Incident Handling	x	x	x
17.2	N/A	Establish and Maintain Contact Information for Reporting Security Incidents	x	x	x
17.3	N/A	Establish and Maintain an Enterprise Process for Reporting Incidents	x	x	x
17.4	N/A	Establish and Maintain an Incident Response Process		x	x
17.5	N/A	Assign Key Roles and Responsibilities		x	x
17.6	N/A	Define Mechanisms for Communicating During Incident Response		x	x
17.7	N/A	Conduct Routine Incident Response Exercises		x	x
17.8	N/A	Conduct Post-Incident Reviews		x	x
17.9	N/A	Establish and Maintain Security Incident Thresholds			x
18.1	N/A	Establish and Maintain a Penetration Testing Program		x	x
18.2	Network	Perform Periodic External Penetration Tests		x	x
18.3	Network	Remediate Penetration Test Findings		x	x
18.4	Network	Validate Security Measures			x
18.5	N/A	Perform Periodic Internal Penetration Tests			x