jamk

Attracting the APT actors into deception system

Identifying ways to attract an APT actor

Outi Rantanen

Master's thesis
March 2024
Master's Degree Programme in Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Rantanen, Outi

Attracting the APT actors into deception system – Identifying ways to attract an APT actor

Jyväskylä: JAMK University of Applied Sciences, March 2024, 99 pages

Master's Degree Programme in Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Improving situational awareness is an emerging trend in the field of information security. The organisation's must identify the proper technical data sources and the non-technical cyber threat intelligence sources in the business environment to create and maintain situational awareness. As the cyber defence techniques develop so does the attacker's techniques. An Advanced persistent threat might prepare a cyber-attack for weeks or months ahead before the initial access by gathering information of the organisation.

A cyber deception system is a way to lure and deceive the attacker into the honeynet system, that can be monitored to set alarm of certain actions in the honeynet system. Deception systems can be used for collecting information about the attacker to create a more precise situational picture. It can also be used to collect cyber threat intelligence from the attacker.

The real-world cyber-attack cases were a way to identify and chart techniques used on a cyber-attack. These techniques were used to model lures to a honeypot system to attract an APT actor to show interest in it. The APT actor fingerprints its main targets and does not trigger the attack's next stage on main targets if the requirements of the target are not met. Therefore, an APT actor will not engage the next stages of the cyber-attack if it discovers it is inside of a deception system or a sandbox.

The deception system needs to be as real as possible and if possible integrated into a real enterprise network. The most important added value of a deception system is the ability to detect and assist on stopping a cyber-attack on its earliest stage.

The research material identifies 192 different techniques used by the APT actor Turla. The most used techniques are Discovery and Command and Control techniques. 30 % of the Turla malwares has system information capabilities and over 40 % of all the Turla software can use System Network Configuration Discovery techniques. The most sophisticated malwares that used the widest range of techniques were Empire, Kazuar, and Uroburos.

Keywords/tags (subjects)

Cyber security, deception system, deception network, honeynet, honey token, honeypot, cyber defence

Miscellaneous (Confidential information)

-

jamk

Kuvailulehti

Rantanen, Outi

Attracting the APT actors into deception system – Identifying ways to attract an APT actor

Jyväskylä: Jyväskylän ammattikorkeakoulu, Maaliskuu 2024, 99 sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma, kyberturvallisuus. Opinnäytetyö YAMK.

Julkaisulupa avoimessa verkossa: Kyllä

Julkaisun kieli: Englanti

Tiivistelmä

Kybertilannekuvan parantaminen on ollut nouseva trendi tietoturvan alalla jo pitkään. Tilannekuvan luomiseksi ja ylläpitämiseksi organisaatioiden täytyy tunnistaa tarvittavat datalähteet sekä ei-tekniset kyberuhkatiedon lähteet organisaation kybertoimintaympäristössä. Kyberturvallisuuden kehittäminen on jatkuvaa organisaatioissa, kyberpuolustus on kilpajuoksua kyberhyökkäyksien kanssa. Uusien menetelmien kehittäminen tietomurtojen toteuttamiseksi on jatkuvaa, silloin myös organisaation kyberturvallisuuden kehittämisen täytyy olla jatkuvaa. Edistyneet kyberuhkatoimijat saattavat valmistella tietomurtoa kohdeorganisaation viikkoja tai jopa kuukausia keräämällä tietoa kohdeorganisaatiosta.

Harhauttava järjestelmä on tapa houkutella ja hämätä hyökkääjää pyrkimään sisälle harhauttavaan järjestelmään, jota monitoroidaan ja joka luo hälytyksen, kun tietyt tapahtumaketjut toteutuvat. Harhauttavaa järjestelmää voidaan käyttää kyberuhkatiedon keräämiseen hyökkääjän toimista.

Reaalimaailman kyberhyökkäykset ja tietomurrot tunnistettiin ja kartoitettiin tarkastelemalla edistyneen kyberuhkatoimijan käyttämiä tekniikoita kyberhyökkäyksessä. Näiden avulla mallinnettiin houkuttimia harhauttavaan järjestelmään, jotta edistynyt kyberuhkatoimija osoittaisi kiinnostusta harhauttavaa järjestelmää kohtaan. Edistynyt kyberuhkatoimija yksilöi hyökkäyksen kohteen eikä aloita kyberhyökkäyksen seuraavaa vaihetta, jos se havaitsee olevansa harhauttavassa järjestelmässä tai hiekkalaatikossa.

Harhauttavan järjestelmän tulisi olla niin aidon oloinen kuin on järkevästi toteutettavissa sekä integroitu mahdollisuuksien mukaan oikeaan tuotantoympäristöön. Harhauttavan järjestelmän tärkein lisäarvo on sen tuoma lisähavainnointikyky tietomurron havaitsemiseksi ja kyberhyökkäyksen estämiseksi hyökkäyksen mahdollisimman varhaisessa vaiheessa.

Tutkimusmateriaalista on tunnistettavissa 192 eri hyökkäystekniikkaa, joita valtiollinen kyberuhkatoimija Turla on käyttänyt tosielämän kyberhyökkäyksissä. Käytetyimmät tekniikat olivat ‘Discovery’ sekä ‘Command and Control’ tekniikat. 30 prosentilla Turlaan yhdistetyistä haittaohjelmista on kyvykkyys hankkia järjestelmätietoja kohdeympäristöstä ja 40 prosentilla kaikista Turlan käyttämistä ohjelmistoista on kyvykkyys hankkia kohdeympäristöstä verkkokonfiguraatiotietoja. Edistyneimmät haittaohjelmat, joilla on kyvykkyys käyttää kaikista laajinta kirjoa eri hyökkäystekniikoista, olivat Empire, Kazuar, ja Uroburos.

Avainsanat (asiasanat)

Cyber security, deception system, deception network, honeynet, honey token, honeypot, cyber defence

-

Contents

Figures

Tables

Abbreviations

API	Application programming interface
APT	Advanced persistent threat
AV	AlienVault
CISA	Cybersecurity & Infrastructure Security Agency (USA)
CSOC	Cyber Security Operating Centre
DLL	Dynamic Link Libraries
EDR	Endpoint detection and response
GDPR	General Data Protection Regulation act
HA	Hybrid Analysis
IoC	Indicators of Compromise
LAN	Local Area Network
NATO	North Atlantic Treaty Organization

NIST	National Institute of Standards and Technology (USA)
OSI	Open Systems Interconnection reference model
PLC	Programmable logic controller
RDP	Remote Desktop Protocol
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information & Event Management System
SMB	Server Message Block protocol
SOAR	Security Orchestration, Automation and Response System
SSH	Secure Shell protocol
SUPO	Finnish Security and Intelligence Service
VT	Virus Total service

Definitions

API call	A call that allows an application to request data from another application
API key	A unique identifier used for API calls
AlienVault service	Threat Intelligence Community, knowledgebase
C2 communication	Command and Control server communication
Hacktivists	Groups that carry out cyber attacks in support of political causes.
Hybrid Analysis service	Malware analysis service
Injection method	Method allows an attacker to inject code into a program or query to execute remote commands that can read or modify a database, or change data on a web site (IBM, 2021).
Intranet	Internal network
Kerberos	An authentication protocol used in Windows domain environments
Local Area Network	Devices connected in one physical location
MITRE	A government-backed organisation conducting cybersecurity research
MITRE ATT&CK®	A knowledge base of adversary tactics and techniques based on real-world observations

MITRE D3FEND	A library of defensive cybersecurity countermeasures and technical components
Threat hunting	A proactive method of searching for cyber threats
User-agent	User-Agent lets servers and network peers identify the application, operating system, vendor, and/or version of the requesting user agent (MDN contributors, 2023).
Virus Total service	A multi-component web platform for analysing malware samples
Watering hole attack	Targeting users by infecting web sites
Web crawler	A bot that systematically browses the internet

1 Introduction

Events, incidents, and different types of cyber attacks are common phenomena in the cyber operational environment. There can be different level of vulnerability scans, denial of service-attacks, brute-forces attacks, identity thefts, and phishing attacks on the internet. It is unlikely that there is anybody in Finland, who has not heard about the case Vastaamo -data breach or heard about the denial-of-service attacks targeting government entities. The National Cyber Security Centre is giving warnings about not giving one's banking account information on a phone call or filling them on phishing sites stealing credentials. There are different types of cybercriminal groups carrying out cybercrimes every day, and many of those attacks are fully automated. In addition to more common and opportunistic cyber criminals, there are hacktivists, and more sophisticated adversary groups, called APT actors targeting governments and other specific institutions. The war in Ukraine has brought cyber incidents into everyday discussions. Due to the war, different types of wiper malwares have become a more common phenomenon. The war in Ukraine has increased the cyber events observed, not only in Ukraine and Russia, but many other countries also, as seen in the figure 1.

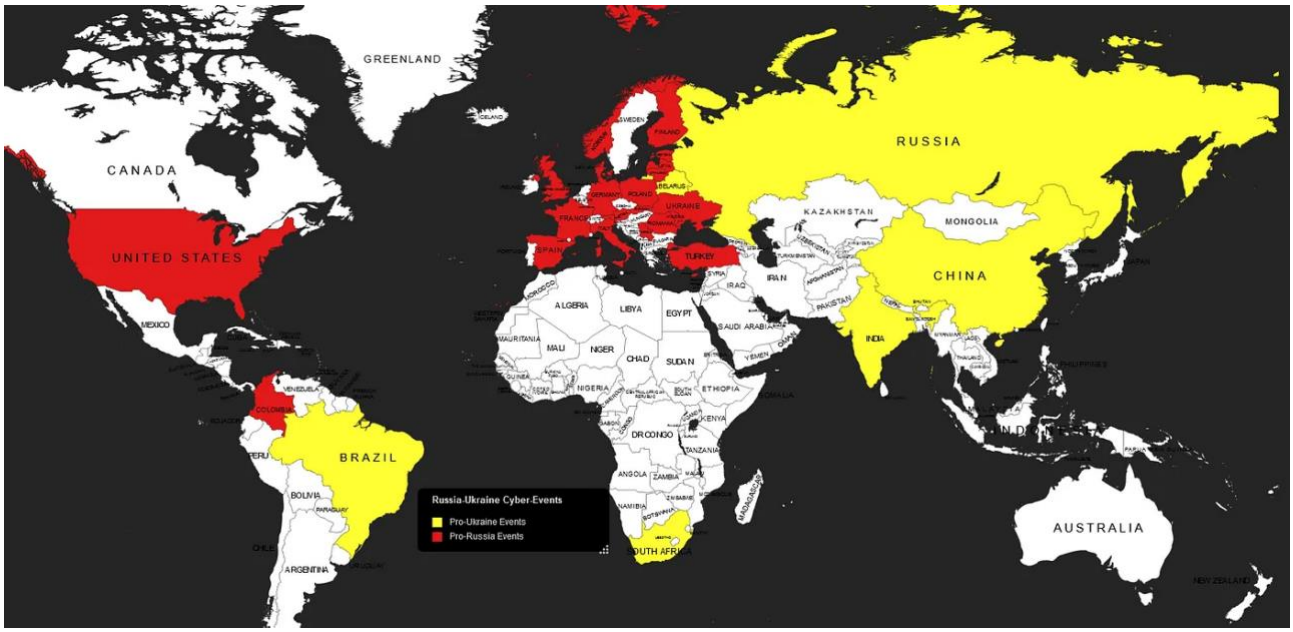


Figure 1. Cyber event-map of Russia-Ukraine war (Russia-Ukraine War Cyber-Event Map, 2022)

According to a cyber security company F-secure, it takes 220 days to identify a cyber security breach. “If you can’t see it – you can’t stop it” states the F-secure (See attacks. Stop them., 2024). The IT solution provider, Cisco, states, that it is not a matter of if an advanced threat will strike, it is a matter of when (What Is Endpoint Detection and Response (EDR)?, 2024).

The United Kingdom’s National Cyber Security Centre points out that the average cost of security breach is between £ 700 000 – 1 300 000 (NCSC Common Cyber Attacks Infographic, 2016). IBM presents that the average cost of a data breach reached an all-time high in 2023 of USD 4.45 million. The IBM report states that only 30 % of security breaches are discovered by the company’s own cyber security team. When analysing the ransomware attacks, according to the report, the attack life cycle was 33 days longer and the cost nearly 10 % more, when not including government officials. (Cost of a Data Breach Report, 2023).

In addition to money, the security breach also causes reputation damage. For example, because of the GDPR act, careless data handling or neglecting implementation of the efficient cyber security measures can cause additional sanctions that might restrict customer data handling in the EU (Regulation (EU) 2016/679). The NIS2 directive (Directive (EU) 2022/2555.) that describes the measures for a high common level of cyber security across the European Union, obliges certain industries with critical sectors to manage cyber security risks. Based on the NIS2 directive, the cyber security risk management includes, inter alia, cyber security incident handling and policies and procedures to assess the effectiveness of cybersecurity risk-management measures.

Incident handling

The incident handling covers everything from the actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident.

NIS2 directive

1.1 Situational awareness is the key to securing systems

According to the Finnish Military Intelligence Review (Sotilastiedustelu, 2023) it is critical to attain an operating environment awareness – and cyber space is no exception. Hybrid operations are problematic to identify despite a well-managed groundwork through-out the society. The variety of means in hybrid operations is already wide from political pressure and information influence on information network operations and conventional military threats. The scope includes society in terms of functionality to essential infrastructure such as

- the electricity distribution network
- network services maintained by the authorities
- influencing by causing supply interruptions
- and service production interruptions.

Improving situational awareness has been an emerging trend for some time now in the field of information security in Finland. To maintain situational awareness of the organisation's operational security environment the organisation must collect data from the technical operational environment and information from the business environment (Katakri, 2020). To do so, the organisation's must identify and collect the proper technical data sources (NCSC-FI, 2016) such as the Windows event logs, the log data from the sysmon or other agents on the intranet, firewall logs, Suricata and Zeek logs and the non-technical threat intel from the business environment (Kiraz, 2023). A common way to maintain and manage technical log data are the commercial Cyber Security Operation Centres (CSOC's). There are presently many CSOC's available in Finland to small and medium businesses and to the public sector also (List of SOC service providers, 2022). If the organisation is resourced enough, it may maintain its own CSOC and even provide it as a B2B service to other organisations.

To uphold and share situational awareness to others, these technical data sources must be collected and combined to systems such as SIEM's that will provide technical situational awareness of the organisation's technical operation environment. From these systems the information and technical IoC's can be shared to those who need the information such as

customers, partners, and government officials. To manage IoC's efficiently many organisations use commercial services such as the CrowdStrike's and the Recorded Future's IoC feeds or the publicly funded open-source platform, MISP, for sharing the technical IoC's from known and identified cyber-attacks. To identify and understand the cyber threats on the organisation's business environment the organisation's must follow the common trends in information security and cyber-attacks within the industry they are in but also for example to keep track of the more advanced and well organised supply chain attacks, where it is common that the attack is very advanced and difficult to recognise on conventional security methods, such as was the SVR's SolarWinds attack in 2020 (AA20-352A, 2020).

1.2 Background of the project

Cyber-attacks have become more common on the internet, according to specialist Mr. Tretjakov from NCSC-FI. The cyber-attacks against Finnish organisations have increased throughout the year 2022. Especially malware, phishing and denial of services attacks have increased (Kyberturvallisuuskeskuksen viikkokatsaus – 52/2022).

For situational awareness it is important to detect and observe the attacks and attack techniques used by the attacker even if the attack attempt is not successful. The defender should learn from the used attack methods and observe what it is that the attacker wants from the information system. To do this, the defender commonly uses the SIEM that the organisation has. Many of the SIEM's has also have the capability to block or use quarantines against the attacker with automation or machine learning. It is proposed that a more efficient and secure way to detect and observe cyber-attacks is a honeypot system, when configured properly.

Some of the theses (Kemppainen, 2016; Tuohimetsä, 2010; Teriö, 2011) which study the honeypots are based on a study about the arbitrary attacks against a research honeypot. Therefore, the data studied is about the number of the arbitrary attacks, the geolocation of the attacks, the method used in arbitrary attacks and even the dictionaries used in those arbitrary attacks. Which is valuable information about the trends of the cyber-attacks or the used reconnaissance techniques in cyberspace. But that kind of general information can be bought with the commercial IoC feeds and the cyber threat reports. In some cases, there is not enough

information about the attacker's motivation, because targeted APT attacks (AA20-352A, 2020; APT Case RUAG, 2016) cannot always be detected by those general honeypots or network sensors.

The published cyber-attack reports do not always include the whole analysis of the attack's cyber kill chain as it can be difficult to find out the initial attack vector hence the attack that has spread wide in the systems are usually hard or impossible to detect in the initial stages of the cyber-attack. It is difficult to detect an unknown cyber-attack because the automated detection rules might not detect the initial breach. It is hard to analyse the cyber-attacks afterwards because the system's logs might be inadequate or missing. The cyber-attack reports might also include some speculation or educated guesses of the events that happened based on the known earlier actions of the cyber threat actors. But the attack and the actors evolve in at a rapid phase, so one might come to question how reliable that is. Those cyber-attacks that exploit known vulnerabilities are usually more common to be detected at initial stages as the technical detection rules can be created to detect a certain attack technique used.

2 Research framework

The research framework section describes a problem on which the research question aims to answer. The objective of this study is to find answers to the research question. The research method is set to describe the ways this research is conducted.

The research problem:

> There are free, open-source honeypots available (Awesome honeypots, 2020), but the information collected from generic honeypots is usually common and mostly describes different cyber-attack trends on the internet. It is difficult to identify or detect targeted attacks with generic honeypots. MITRE Groups (Groups, 2024) describes 143 different APT groups and with a generic honeypot, the organisation could have all of them scanning and gathering information about it. It would be impossible to identify or separate one group from another. In addition, it would draw attention from cyber criminals and many-purpose web crawlers.

2.1 Research question

The goal of this research is to identify ways to attract an APT actor into a deception system. And the research is about finding out if there are different ways to attract an APT attacker to spend time in a deception system for study and research.

The research question:

"What type of technical considerations are there for a deception system to attract an APT actor into one?"

In this research, the techniques and methods will be charted and analysed to discover ways to lure an advanced attacker into a deception system regardless of the purpose of the deception system. For this study, it is proposed that this system could be a honeypot. The type of a honeypot was not defined for the assignment. This research will focus on charting methods used by an APT actor in a real-life cyber-attack. The research will be focusing on the technical viewpoint of the attacks, and it does not take a stand on the politics or the social considerations of the cyber-attacks nor any other than technical objects of an attacker. It does not include attacker-based threat modelling or knowledge-based threat modelling about adversary's objective, but focuses on the software used in the attacks.

This study's purpose is to find ways on how to implement credible deception system. A well-managed deception system will increase the situational awareness and cyber defence capabilities. Understanding the operating methods of the cyber threat actors is an essential part of a modern and cost-effective cyber defence. The different deceptive information systems are one way to study the activities of the cyber threat actors. The surveillance of the cyber operational environment supports the production of a situational picture, strengthens cyber countermeasures and the timeliness and effectiveness of all the defence actions.

According to the Government's Defence report (2021) the cyber defensive ability is demonstrated through active actions. Based on the Katakri (2020), the Finnish national audit criteria, and Government's Defence report (2021) officials must be able to monitor all operating environments and, if necessary, to be able to initiate defensive measures. The identification of a cyber threat or an impending cyber threat is an essential element of cyber deterrence.

2.2 Research strategy

The qualitative research method is flexible, and the researcher does not set out to test a pre-set hypothesis. With qualitative research the researcher can acquire latest information, describe a phenomenon, deepen an understanding, interpret a phenomenon, or challenge a theory or construction. In qualitative research, the hypotheses are derived from the analysis of individual cases. The hypotheses are generated during the data collection and analysis phase throughout the research and not from preceding literature or separate theory. The qualitative research aims to produce holistic understanding about the research subject. (Juuti; Puusa 2020.).

Theoretical research enables researching a subject without directly observing the research subject. A Theoretical research ambitions is to define and outline conceptual models, explanations, and structures. Theoretical research is based on the research literature such as white papers. A case study focuses on a particular case aiming to produce detailed information of the chosen case. A case study has a narrow focus with the objective of understanding the phenomenon. A case study enables specific interpretations of a phenomenon in a particular context. A case study can include generalisations relating to the phenomenon (Case study, 2010).

Case study can be exploratory, descriptive, interpretive, and explanatory, according to the research paper by Zucker, 2009. Therefore, it was selected for this thesis research method. The goal is to interpret and explain the research subject APT TURLA and the software used on different stages of the cyber attacks. Case study is a way to study an event, seek patterns and causes of behaviour.

Case study is a way to outline the research and limit the used material for specific target or function. The case study must be a reasoned choice or approach for the research. In assessing the generalisability of the case study, the premise is defined on how successfully the area to be studied is represented in the research material. Therefore, case study must be research which is generalisable in their presentable context. This thesis is a case study implementing as applicable a combination of event analysis and a case study to find the ways to identify, chart and analyse ways to use a honeypot to make an APT actor interested in it. In qualitative research, the aim is to understand the phenomenon examined in the research from the perspective of the persons who are the subject of the research (Juuti; Puusa 2020).

It is typical for qualitative research that the research problem is specified throughout the research because the instrument collecting the research data is human. The interpretations and perspectives related to the research material develop as the research process progresses. The research activity should be understood as a kind of learning event (Kiviniemi 2018).

2.3 Research methods

Classification analysis will benefit categorising the results. Classification divides the information into categories, groups, and classes. The typification analysis method will assist on defining what is characteristic for the research subject by generalisations that will help on identifying the methods which attract the APT actors. Classification and typification deepen the understanding of the phenomenon (Categories, Classes and Types, 2010). Typification is a way to simplify and generalise data into illustrative types (Data analysis, 2016).

Data collection strategy is to use existing materials: reports and publicly available cyber threat databases. The research material is delimited to a specific APT actor and the software documented from its cyber attacks. The research material will be scored, charted, colour coded and labelled by numbers to ease the conclusive analysis.

The research data is collected from the MITRE ATT&CK database. The different data sets from the MITRE ATT&CK are combined using the MITRE ATT&CK Navigator -tool. The used techniques are colour coded and scored as separate datasets and finally the different datasets are combined into a one table that characterise the APT actor’s techniques used in a real-life attack.

The colour-coding and number-coding separates the unique attack tools in a way, that reveals the most used attack technique used by the research subject. The dataset-analysis also reveals the most used software in different attack phases. The MITRE ATT&CK Navigator -tool enables the analyse of the datasets and the used attack techniques, attack phases, and used tools. The white papers and publications describe the motivation and abilities of an APT actor and increase understanding of the threat actor's cyber attacks.

3 Theoretical framework

In this section the cyber attacks and deception systems are introduced.

According to European Union agency for Cybersecurity ENISA the cyber security threat actors are categorised to:

- State-Sponsored threat actors
- Cybercrime actors
- Hacker-for-hire actors
- Hacktivists.

The ENISA's Threat Landscape Report (2022) states that the most used attack vector of state-sponsored threat actors was an exploitation of a vulnerability. In the year 2021 the number of disclosed 0-day vulnerabilities reached an all-time high of 66. Also, the use of destructive attacks has risen because of the conflict in Ukraine. The report notes that state-sponsored cyber actors conducted operations in co-operation with kinetic military action by using wiper attacks to destroy networks of governmental agencies and critical infrastructure entities. The use of fear, uncertainty and doubt is a way to create confusion and undermine public trust. (ENISA Threat Landscape 2022, 2022).

Commonly, in information systems, several types of malicious scanning, phishing, intrusions, and denial of services are considered as "cyber-attacks". Those attacks are meant to be malicious and cripple or halt businesses or actions in a factory or power plant - for example. According to F-secures article *Mikä on kyberhyökkäys*? (2023), the cyber-attacks aim to paralyse systems, steal data, or otherwise just cause harm. Microsoft defines a cyber-attack as a way to damage or access

important files and systems in a company's or a person's computer network (What is a cyber attack, n.d.).

3.1 Cyber attack trends

It is seen in the graph (Figure 2) by ENISA that the public administration is the most common target of cyber-attacks per number of reported incidents. The energy sector is 3,8 % and the military 3,4 %. This could mean that many of the power plants are well protected or there is now visibility to attacks. Because there are information technology networks and operational technology networks in power plants it could be that there just is not that many attacks detected. But according to ENISA's threat report the attacks against OT networks could be an increasing trend.

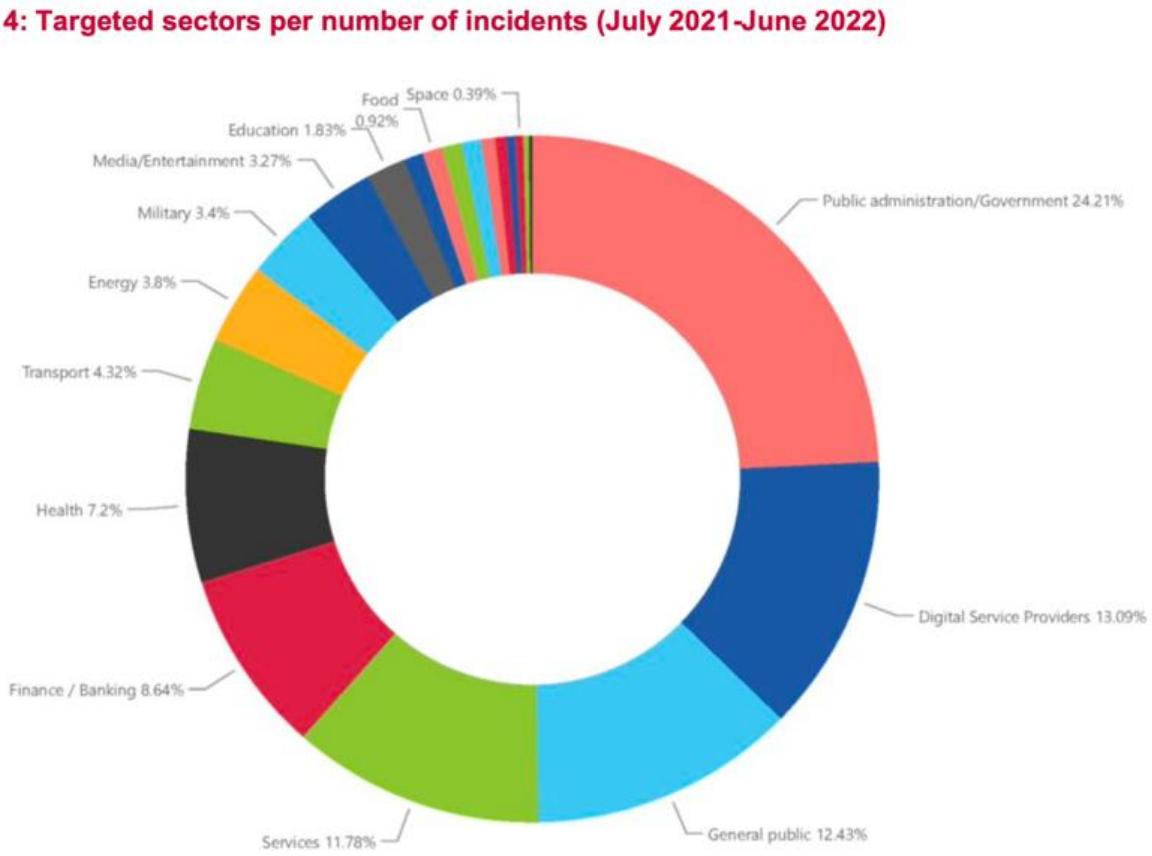


Figure 2. Targeted sectors per number of reported incidents (ENISA Threatlandscape 2022, 2022)

Based on the IBM's Data Breach report (2022) it takes approximately 323 days to identify and contain a data breach – and AI cuts 74 days out of the 323 days. According to the report it takes 249 days to identify and contain attacks with security systems which use AI. Nearly 20 % of all attacks are done with stolen or compromised credentials. These attacks are also the most difficult to identify and therefore those have the longest life cycle of approximately 327 days, 243 days to identify the breach, and additional 84 days to contain the breach. Stolen or compromised credentials are the most used attack vector and phishing attacks the second most common cause of the breach. (Cost of a Data Breach, 2022).

According to IBM's report a hybrid cloud model had shorter breach lifecycles than organisations that merely adopted a public or private cloud model and the cost difference between those solutions was nearly 30 %. There has not been much of a difference between earlier years on detecting and containing a data breach (Figure 3). There could be public holidays or other human reasons for those differences, or it could describe the continuous race between the cyber attacker and the defender. As the defender improves methods to defend and monitor information systems the attacker advances on developing new methods to attack and to automatise attacks.

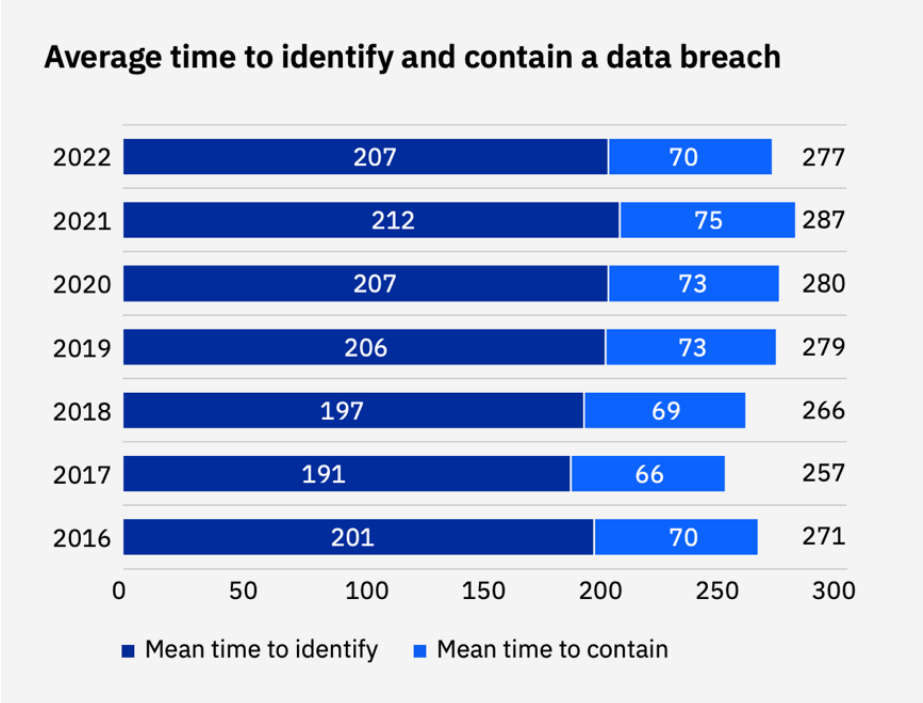


Figure 3. Average time to identify and contain a data breach (Cost of a Data Breach, 2022)

According to Microsoft's Digital Defence report the nation state actors are using obfuscation in their operations by using open-source and legitim software (Cost of a Data Breach, 2022). The cyber security company CrowdStrike's Global threat report (2023) presents that over 70 % of all the detected cyber attacks on 2022 were malware-free. According to the report, the attack takes approximately 84 minutes from the initial access to move laterally from one compromised host to another; in 2018 the corresponding value was under 40 %.

Based on the research by Biggio et al (2023) the artificial Intelligence (AI) can sift the attack rhythm to fasten the initial access. With the help of AI, the adversaries may shift from having a few slow veiled campaigns to having numerous fast-paced campaigns to increase their chances of success in cyber attacks. The offensive AI impacts to the beginning of the cyber attack the most since the attacker has more information on the reconnaissance phase from the initial access to the malware delivery. The attacker can use reconnaissance information to refine and evaluate the attacks offsite before proceeding to initial access.

3.2 Detecting cyber attacks

Information security is based on confidentiality, integrity, and availability. And those are the basics also in cyber security, but it also includes a wider point of view to the information security. It includes threat-based thinking, threat modelling, security controls, such as the anti-virus solutions, firewalls, VPNs, and other technical security controls. The cyber security also includes risk-based approach, meeting the compliance requirements, continuous evaluations, reputation damage and so on. Cyber security is more than just technical cyber security controls. To gain security, the organisation must defend against cyber threats, attacks, and exploits. Cybersecurity engages a combination of people, technology, and methodology. (Cuofano, 2023)

Some of the cyber-attacks are easy to detect because of the diverse kinds of monitoring systems in CSOC's, such systems are called EDR, SOAR and SIEM. SIEM systems alert security analysts of a potential event, SOAR platforms use automation, artificial intelligence, and machine learning to provide greater context and automated responses to these threats (Niemi, J. 2022). The EDR solution focuses on detecting advanced treats, with the capability to evade the perimeter security controls of the system and enter the environment. The EDR solution helps to detect, contain, and remove the treats. These security solutions are only as good as the cyber threat intelligence

behind them (What Is Endpoint Detection and Response (EDR)?, 2024). That is because the rule based cyber security monitoring systems can only detect the known cyber threats. If there is no monitoring rule to raise the alert the monitoring system will not detect the cyber attack. They are similar rule based cyber security control system such as an anti-virus system is. Thus, it will not raise an incident or alert about something it sees as normal internet traffic or user-based action.

It is suggested, by the that the defender should meet the 1-10-60 rule (Letema&Trevino, 2020):

- detecting threats within the first minute,
- understanding the threats within 10 minutes,
- and responding within 60 minutes.

Endpoints are usually the most vulnerable parts of an organisation, which makes them probable targets for threat actors aiming to install malware, gain unauthorised access and exfiltrate data. The attack surfaces are more commonly wide in the organisations and therefor there are diverse ways for the adversary to get inside a network (Zpedia, 2024).

3.3 Analysis of the cyber attacks – Cyber kill chains

> *If defenders implement countermeasures faster than their known adversaries evolve, they maintain a tactical advantage. Amin et al, 2011.*

The cyber kill chain is commonly acknowledged model to describe the different phases of the cyber attack. The first cyber kill chain presented was introduced by Lockheed Martin. At each step of the cyber attack the defender can implement a set of defensive measures to stop or restrict the attack or the attacker (Cen et al, 2023). A kill chain is systematic, integrated end-to-end process to target and engage an adversary to create desired effect. The cyber kill chain is a Lockheed Martin's implementation of the U.S. military doctrines kill chain F2T2EA. The model is designed to aid the defender to learn and react to cyber attacks and to identify ways to protect the defender's system from the similar attack techniques in the future (Amin et al, 2011).

The efficient defensive measures force the attacker to modify its technical attack methods. The more time and effort the attacker must use to gain access to the system, the more expensive the attack is going to be for the attacker. The attackers re-use infrastructure, tool, and techniques to save money and other resources. Depending on the attack phase on which the defender detects the attack, the defender must complete the attack analysis on all the prior attack phases to be able to mitigate the future intrusion attempt using the same attack methods from the same adversary. (Amin et al, 2011).

The evolution of the cyber kill chains is presented at the table 1.

F2T2EA (Amin et al, 2011).	**Cyber Kill Chain** (Amin et al, 2011).	**MITRE** (Enterprise tactics, 2023)	**Unified Kill Chain** (Pols, 2023)
Find	Reconnaissance	Reconnaissance	Reconnaissance
Fix	Weaponization	Resource Development	Resource Development
Track	Delivery	Initial Access	Delivery
Target	Exploitation	Execution	Social Engineering
Engage	Installation	Persistence	Exploitation
Assess	Command and Control	Privilege Escalation	Persistence
	Actions on Objectives	Defense Evasion	Defense Evasion
		Credential Access	Command and Control
		Discovery	Pivoting
		Lateral Movement	Discovery
		Collection	Privilege Escalation
		Command and Control	Execution
		Exfiltration	Credential Access
		Impact	Lateral Movement
			Collection
			Exfiltration
			Impact
			Objectives

Table 1. Evolution of the cyber kill chains

The same elements are present regardless of the cyber kill chain model (Table 1). The Lockheed Martin's cyber kill chain has seven phases focusing on the certain stages of an attack, while the MITRE ATT&CK framework with 14 attack phases focuses more on the tactics and techniques used by attackers (Cyber kill chain, 2024). Whereas the Lockheed Martin's cyber kill chain approaches

the cyber attack from the attacker's perspective, the MITRE ATT&CK focuses on the techniques used by the attacker and when combined, they are providing a comprehensive understanding of the cyber threats. The two frameworks' synergies each other (Exabeam, 2024). The unified cyber kill chain describes modern cyber attacks through 18 attack tactics. The kill chains have similar tactics, but with different names. For example, the Lockheed Martin's Weaponization is called Resource Development in both MITRE's and Unified kill chain. Target Manipulation on Unified kill chain was renamed as Impact to unify the models and enhance the usability of different models. The Unified kill chain offers understanding on the attack specific kill chains and the actor specific kill chains depending on the point of view of which the attack is being analysed on. (Pols, 2023)

The cyber kill chains produce understanding and knowledge for building the cyber defensive measures to protect the organisation's critical assets instead of trying to defend all organisation's internet connected systems with the same level of effort and resources (Pols, 2023).

3.4 The MITRE adversarial tactics, techniques, and common knowledge

The MITRE ATT&CK framework (2023) tracks cyber adversary tactics and techniques across the entire attack lifecycle of the cyber attack. The ATT&CK is an acronym for Adversarial Tactics, Techniques, and Common Knowledge and was released to public in 2015. It is a tool intended to be used to strengthen an organisation's security stance. The knowledge base is populated primarily by publicly available threat intelligence and incident reporting. As stated by MITRE (n.d.), a not-for-profit corporation operating federally funded R&D centres on behalf of U.S. government sponsors, there is a lot we can learn from cyber adversaries. The cyber adversaries are intelligent shapeshifters that learn from every attack whether it is successful or not. The MITRE ATT&CK is a knowledge base that helps model cyber adversaries' tactics and techniques, and how to detect or stop them. The MITRE ATT&CK enables threat-informed cyber defence.

The MITRE ATT&CK framework (2023) includes datasets of matrices, tactics, and techniques for Enterprise, Mobile, and Industrial Control Systems (ICS). Defences from data sources, mitigations, and assets and Cyber Threat Intelligence (CTI) about groups, software, and Campaigns. It also has a dataset for campaign relationships.

The MITRE ATT&CK framework has 14 tactics in the enterprise matrix (Figure 4). The tactics describes adversary's tactical coal; what the adversary is trying to achieve. The framework includes 201 adversary techniques and 424 sub-techniques. The techniques describe a way an adversary tries to achieve its coal (Figure 5). The enterprise matrix includes a description about the method and information of which systems it was used. The matrix unites the techniques used to an adversary group, ways to mitigate the activity, the references to the reports to its use in the real-world attacks. (Enterprise tactics, 2023). The MITRE ATT&CK can be used to produces heat maps of the attacks, tactics, techniques, threat actors, software and mitigation or detection techniques.

The ATT&CK Navigator -tool is a web-based tool for annotating and exploring ATT&CK matrices. It can be used for example to visualise defensive coverage, red and blue team planning, and the frequency of detected techniques (MITRE ATT&CK framework, 2023).

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Figure 4. The MITRE ATT&CK framework tactics (Enterprise tactics, 2023)

Figure 5. MITRE ATT&CK Enterprise matrix (Enterprise matrix, 2023). The Attack phase advances from left to right.

The MITRE ATT&CK database of data sources (Figure 6) that characterise the various subjects of information that can be collected from data sources. Data sources helps to identify specific properties of a data source relevant to detecting a given ATT&CK technique or sub-technique. The MITRE ATT&CK data sources include 41 data sources of which 38 are applicable to enterprise (Data sources, 2024).

ID	Name	Domain	Description
DS0001	Firmware	Enterprise	Computer software that provides low-level control for the hardware and device(s) of a host, such as BIOS or UEFI/EFI
DS0002	User Account	Enterprise	A profile representing a user, device, service, or application used to authenticate and access resources
DS0003	Scheduled Job	Enterprise	Automated tasks that can be executed at a specific time or on a recurring schedule running in the background (ex: Cron daemon, task scheduler, BITS)
DS0004	Malware Repository	Enterprise	Information obtained (via shared or submitted samples) regarding malicious software (droppers, backdoors, etc.) used by adversaries
DS0005	WMI	Enterprise	The infrastructure for management data and operations that enables local and remote management of Windows personal computers and servers
DS0006	Web Credential	Enterprise	Credential material, such as session cookies or tokens, used to authenticate to web applications and services
DS0007	Image	Enterprise	A single file used to deploy a virtual machine/bootable disk into an on-premise or third-party cloud environment
DS0008	Kernel	Enterprise	A computer program, at the core of a computer OS, that resides in memory and facilitates interactions between hardware and software components
DS0009	Process	Enterprise Mobile	Instances of computer programs that are being executed by at least one thread. Processes have memory space for process executables, loaded modules (DLLs or shared libraries), and allocated memory regions containing everything from user input to application-specific data structures
DS0010	Cloud Storage	Enterprise	Data object storage infrastructure hosted on-premise or by third-party providers, made available to users through network connections and/or APIs
DS0011	Module	Enterprise	Executable files consisting of one or more shared classes and interfaces, such as portable executable (PE) format binaries/dynamic link libraries (DLL), executable and linkable format (ELF) binaries/shared libraries, and Mach-O format binaries/shared libraries
DS0012	Script	Enterprise	A file or stream containing a list of commands, allowing them to be launched in sequence
DS0013	Sensor Health	Enterprise Mobile	Information from host telemetry providing insights about system status, errors, or other notable functional activity
DS0014	Pod	Enterprise	A single unit of shared resources within a cluster, comprised of one or more containers
DS0015	Application Log	Enterprise ICS	Events collected by third-party services such as mail servers, web applications, or other appliances (not by the native OS or platform)
DS0016	Drive	Enterprise	A non-volatile data storage device (hard drive, floppy disk, USB flash drive) with at least one formatted partition, typically mounted to the file system and/or assigned a drive letter
DS0017	Command	Enterprise Mobile	A directive given to a computer program, acting as an interpreter of some kind, in order to perform a specific task
DS0018	Firewall	Enterprise	A network security system, running locally on an endpoint or remotely as a service (ex: cloud environment), that monitors and controls incoming/outgoing network traffic based on predefined rules
DS0019	Service	Enterprise	A computer process that is configured to execute continuously in the background and perform system tasks, in some cases before any user has logged in
DS0020	Snapshot	Enterprise	A point-in-time copy of cloud volumes (files, settings, etc.) that can be created and/or deployed in cloud environments
DS0021	Persona	Enterprise	A malicious online profile representing a user commonly used by adversaries to social engineer or otherwise target victims
DS0022	File	Enterprise	A computer resource object, managed by the I/O system, for storing data (such as images, text, videos, computer programs, or any wide variety of other media).
DS0023	Named Pipe	Enterprise	Mechanisms that allow inter-process communication locally or over the network. A named pipe is usually found as a file and processes attach to it
DS0024	Windows Registry	Enterprise ICS	A Windows OS hierarchical database that stores much of the information and settings for software programs, hardware devices, user preferences, and operating-system configurations
DS0025	Cloud Service	Enterprise	Infrastructure, platforms, or software that are hosted on-premise or by third-party providers, made available to users through network connections and/or APIs
DS0026	Active Directory	Enterprise	A database and set of services that allows administrators to manage permissions, access to network resources, and stored data objects (user, group, application, or device)
DS0027	Driver	Enterprise	A computer program that operates or controls a particular type of device that is attached to a computer. Provides a software interface to hardware devices, enabling operating systems and other computer programs to access hardware functions without needing to know precise details about the hardware being used
DS0028	Logon Session	Enterprise	Logon occurring on a system or resource (local, domain, or cloud) to which a user/device is gaining access after successful authentication and authorization
DS0029	Network Traffic	Enterprise Mobile	Data transmitted across a network (ex: Web, DNS, Mail, File, etc.), that is either summarized (ex: Netflow) and/or captured as raw data in an analyzable format (ex: PCAP)
DS0030	Instance	Enterprise	A virtual server environment which runs workloads, hosted on-premise or by third-party cloud providers
DS0032	Container	Enterprise	A standard unit of virtualized software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another
DS0033	Network Share	Enterprise	A storage resource (typically a folder or drive) made available from one host to others using network protocols, such as Server Message Block (SMB) or Network File System (NFS)
DS0034	Volume	Enterprise	Block object storage hosted on-premise or by third-party providers, typically made available to resources as virtualized hard drives
DS0035	Internet Scan	Enterprise	Information obtained (commonly via active network traffic probes or web crawling) regarding various types of resources and servers connected to the public Internet
DS0036	Group	Enterprise	A collection of multiple user accounts that share the same access rights to the computer and/or network resources and have common security rights
DS0037	Certificate	Enterprise	A digital document, which highlights information such as the owner's identity, used to instill trust in public keys used while encrypting network communications
DS0038	Domain Name	Enterprise	Information obtained (commonly through registration or activity logs) regarding one or more IP addresses registered with human readable names (ex: mitre.org)
DS0039	Asset	ICS	Data sources with information about the set of devices found within the network, along with their current software and configurations
DS0040	Operational Databases	ICS	Operational databases contain information about the status of the operational process and associated devices, including any measurements, events, history, or alarms that have occurred
DS0041	Application Vetting	Mobile	Application vetting report generated by an external cloud service.
DS0042	User Interface	Mobile	Visual activity on the device that could alert the user to potentially malicious behavior.

Figure 6. MITRE ATT&CK data sources for logging and monitoring

3.5 Advanced persistent threats

The Finnish Security and Intelligence Service (SUPO) defines the advanced persistent threats, APT's, as an abbreviation that is used to describe cyber espionage operations and the set of technical traces. The technical way to identify interconnected cyber operations is through the methods, tools, and the network infrastructure used in the attack. The APT identifiers give strong indications that there is a state behind the cyberespionage operation (SUPO, n.d.).

3.5.1 The ”target-oriented” cyber threats

According to the SUPO, when the notion “APT” was adopted, the state-run cyber espionage operations objective was at gaining access to the target and staying there as long as possible without being noticed. It was common to exploit targeted systems through software vulnerabilities and the software code used in the operations was very advanced. But today, the APT actors are known to have used also simple methods with persistent efforts, and therefore a ”target-oriented” would be a more descriptive term than “advanced”. The aim of the APT actors is to acquire access into a specific target information system, and the attacker is prepared to try various methods in a persistent manner until a well-functioning one is found (SUPO, n.d.).

3.5.2 Nation-state actors or state-sponsored groups

According to the United States of America's CISA (Cybersecurity & Infrastructure Security Agency) the APT actors are often nation-state actors or state-sponsored groups (CISA, n.d.). The NIST, National Institute of Standards and Technology defines Advanced Persistent threat in a NIST Special Publication 800-39 (2011) as

> *An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future.*

The advanced persistent threat:

(i) pursues its objectives repeatedly over an extended period of time;

(ii) adapts to defenders' efforts to resist it;

(iii) and is determined to maintain the level of interaction needed to execute its objectives. NIST 800-39, 2011.

The MITRE ATT&CK recognises 143 different APT groups (Groups, 2024). The cyber security company Mandiant lists 37 different APT groups. The cyber security company CrowdStrike acknowledges 232 threat actor groups, of which some are e-crime groups (Global Threat Report, 2024). According to Malwarebytes (Figure 7) almost 80% of distinct groups are associated with Peoples Republic of China.

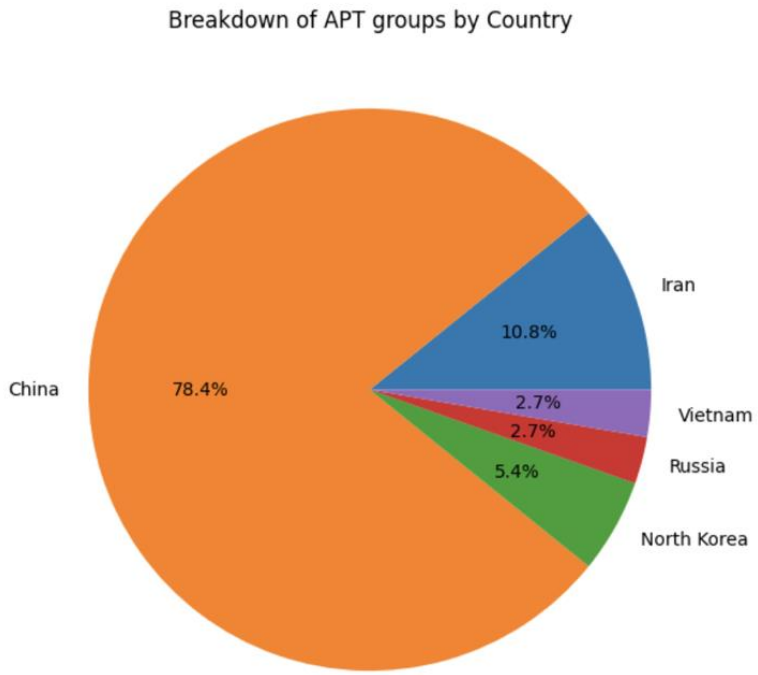


Figure 7. APT groups classified by the country associated (Cozens, 2023)

3.5.3 The breakout times of the APT actors

According to the cyber security company CrowdStrike, a breakout time, a time it takes for the attacker from the initial access to lateral movement, is at average of 118 minutes (Busselen, 2018). In 2022 the breakout time was 84 minutes, and in 2023 62 minutes (Global Threat Report, 2024). The CrowdStrike (Figure 8) calls the Russian-based threat actors as ”bears” and the average breakout time of the Russian-based threat actor is 18 minutes and 49 second. The “Chollima” is the Democratic People's Republic of Korea-based threat actor and its breakout time, 2 hours 20 minutes, which is over 2 hours longer than the breakout time of the “bears”. The “Panda” is People’s Republic of China-based threat actor with the breakout time of 4 hours. The “Kitten” is Iran -based treat actor with breakout time of over 5 hours. The ”Spiders” are e-crime groups with breakout time of nearly 10 hours. (Ali-Ahmed&Sullivan, 2019).

Figure 8. The Breakout times of the diffrent APT actors (Ali-Ahmed&Sullivan, 2019)

3.6 The deception systems

According to Dickinson (2020) the deception systems can help organisations to decrease the time of detection of the attacker on system, to collect attack attribution information and threat intelligence about the attacker. Dickinson (2020) states that threat detection is the main purpose and highest mature advantage of cyber deception. The different deception systems work best as a part of the comprehensive security program. Deception systems can be small and low-cost files or appliances such as token-based deceptions and appliance-based deception such as emulated decoy systems or more expensive and more maintenance demanding enterprise-level deception such as full OS virtual machine decoys. Simplest way to deploy a deception system is to place these deception assets on the locations where the organisation does not normally have internet traffic, or which does not need to be accessed by users or admins. If there are attempts to interact with those deception assets that is anomalous and suspicious. (Dickinson, 2020).

Dickinson (2020) describes the honeypot technology as the foundation of deception. When measured in the amount of interaction the attacker has with a honeypot, it correlates with how realistic and detailed the honeypot seems to the attacker. The more interaction with honeypot, the more time the attacker will use with it. The higher volume of interaction with deception systems will increase the amount and quality of gathered threat intelligence. Making the deception systems more attractive to the attacker with false or deceptive information on responses, breadcrumbs leading to deceptions systems and making deception systems seem like easier targets. To gain reconnaissance, initial foothold, persistence and enable later movement on deception systems will increase the time the attack will take to attack against the real assets. The deception systems might delay the attack to the production environment enough to implement effective response and increase the likelihood of the attack being detected. (Dickinson, 2020).

3.6.1 The decoy environment

Based on the MITRE Defend chart, a decoy environment includes (Figure 9) specific hosts and networks for the purposes of deceiving an attacker. A decoy environment, also referred as honeypot, is used for managing the decoy artefacts. The decoy environment spoofs local area networks and intranet networks of the organisation. A decoy environment can include connected honeynets, integrated honeynets and standalone honeynets. A standalone honeynet is entirely

isolated from the enterprise network and it will not interact directly with the enterprise resources. A standalone honeynet has fewer risks compared to connected or integrated honeynets on the grounds of its isolation from the enterprise network. A standalone system's disadvantages are its un-authenticity and unrealism. A lot of effort needs to be placed on the development and implementation of a standalone system to make it seem like a real production or enterprise system. A connected honeynet is connected to the enterprise environment network and it simulates different functionalities to the network, without exposing full access to a production system. The integrated honeynets use production environments connected to the enterprise network and operate computing resources or software that attract attackers. It grants full interaction and access that provides a wide-ranging understanding of an attack chain. (Decoy Environment, n.d.)

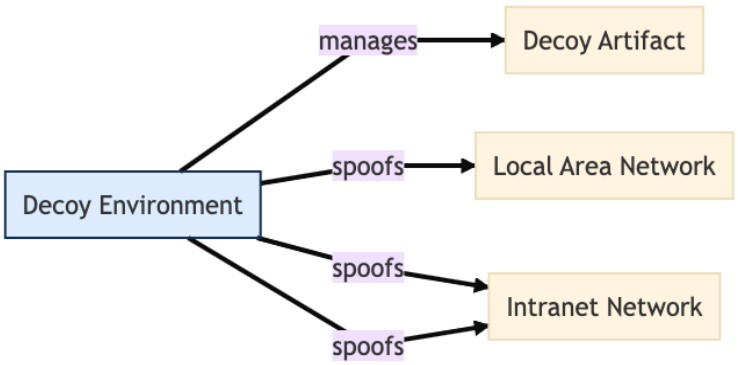


Figure 9. A Decoy environment (Decoy Environment, n.d.)

3.6.2 The Honeypot systems

The RFC 4949 states:

> *honey pot*
>
> *(N) A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears. (See: entrapment.) Usage: It is likely that other cultures use different metaphors for this concept. Therefore, to avoid international misunderstanding, an IDOC SHOULD NOT use this term without providing a definition for it.(See: Deprecated Usage under "Green Book".) RFC 4949*

And entrapment:

> *entrapment*
>
> *(I) "The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit." [FP039] (See: honey pot.) RFC 4949*

The definition of honeypot from the publication of the Finnish Defence University #Kyberpuolustus

> *Honeypot*
>
> *In cyberspace, a honeypot refers to a trap into which an opponent is lured and at the same time gathering information about the opponent's abilities and interests (Laari et al. 2019).*

According to the cyber security company Imperva, a honeypot is a virtual trap to lure attackers into vulnerable systems. The honeypots are vulnerable systems on purpose intended to look like a legitimate system to lure cyber criminals. When the attacker exploits the vulnerabilities, it is possible to study the attackers' actions by monitoring the honeypot. The organisation can apply a honeypot into any information system. Honeypots can be used for collecting intel on attackers' behaviour patterns. (What is a honeypot, n.d.)

The Imperva classifies the honeypots into two types of honeypots. Production honeypots are often part of an intrusion detection system. Production honeypots are part of the operating information systems used to side-track the attacker. Research honeypots are used for educational purposes and to improve security systems. Those honeypots contain trackable data that can be traced. (What is a honeypot, n.d.)

Imperva categorises honeypot deployment into three distinct types. Pure honeypots are complete production systems, low-interaction honeypots mimic services and systems which often attract attackers, and high-interaction honeypots look and behave like a real production infrastructure. Imperva sees that honeypots cannot detect security breaches in legitimate systems and do not identify the attacker. A network that contains one or more honeypots is called a honeynet. (What is a honeypot, n.d.)

According to the cyber security company CrowdStrike a honeypot is a cyber security mechanism manufactured to lure cybercriminals from legitimate targets and gather intelligence about adversaries. Honeypots are designed to impersonate legitimate targets but are intentionally vulnerable. With the help of the honeypot the organisation can determine the origin of the cyber-attack, the sophistication level of the attack, techniques used by the adversary, the most attractive targets in the organisation and evaluate the effectiveness of the existing security measures. The honeypots help the organisation to enhance their security policies against known threats and identified techniques used by the adversary. (Honeypots in cybersecurity explained, 2021).

CrowdStrike describes a Honeynet as a network of honeypots, which looks like an organisational network with multiple components. With honeynets it is possible to manipulate the honeynet environment to lure adversaries deeper into the honeynet system to gain knowledge about their

capabilities or identities. According to CrowdStrike the production honeypot is the most common type of honeypot. The production honeypot decoy is used to collect information about the adversary's actions within the production network. Production honeypots are mostly used by corporations, private companies, and high-profile individuals. Those are simple to design and deploy, but the intelligence production honeypots produce is not as sophisticated as from research honeypots. Most production honeypots are considered low-interaction honeypots. Many adversaries are highly advanced and capable of detecting these low-level decoys and avoiding them. It is also possible to exploit these honeypots by feeding the misinformation. Low-level honeypots are unlikely to gain attackers attention for long and the offered intelligence about the adversary will be limited. (Honeypots in cybersecurity explained, 2021).

CrowdStrike defines a research honeypot as a system which collects information with specific methods and techniques used by the adversaries. Research honeypots are commonly used by governments, intelligence organisations and research organisations to identify different security risks. Usually research honeypots are considered high-interaction honeypots which consist of exploratory targets to engage cybercriminals for extended periods of time. These honeypots give a deeper understanding about threat actors methods; therefore, it is vital to use proper isolation and monitoring. (Honeypots in cybersecurity explained, 2021).

Ian Carnaghan is a software developer, solutions architect, and interaction designer for government, education, and private sector industries. Carnaghan states that organisations deploying honeypots should invest and have enough resources to maintain a secure implementation of the honeypot system. According to Carnaghan, the honeypots can be used as an active defence mechanism. A standard honeypot traps attacks and monitors intrusion information about activities of the hacking process. Honeypots are suitable for organisations which are capable of correctly implementing and maintaining the honeypot. Unmaintained or poorly configured honeypot can lead to an unintended vulnerability and even security breaches. If an organisation deploys a honeypot or a honeypot network as a part of the organisation's security plan, they should make sure they understand the risks related to them and proceed accordingly. (Carnaghan, 2014).

Honeypots are information systems, which are used for monitoring and identifying the techniques, tactics and procedures used by a threat actor who has managed to compromise the system, or systems monitored. Honeypots are used for letting attackers intentionally compromise information systems by letting them exploit different vulnerabilities to get access to intentionally vulnerable systems or systems pretending to be vulnerable. Honeypots can also be used for collecting cyber threat intelligence about cyber criminals and cyber threat actors. There are several types of honeypots available but what those have in common is that they pretend to be legitimate systems. These decoys help to gain understanding about the attacker's behaviour patterns. There are two types of honeypots: production honeypots and research honeypots. But if classified by the technology, there are numerous types of honeypots, for example database, web, service, anti-honeypots, SCADA, data collection, VM monitoring, SSH, and honeytokens (Awesome Honeypots, 2022). Eissa (2021) presents a pure honeypot. A pure honeypot is a real production system’s twin, a replica, that has wide-ranging monitoring and fake confidential data.

CrowdStrike lines up that honeypots can be used to detect both internal and external threats (Honeypots in cybersecurity explained, 2021). Honeypots work in a vary of systems that exists or do not exists meaning that one may create a honeypot of a lure system that does not really exist in the enterprise network. A honeypot can be a legacy system, that has been removed from the real production work to operate as a lure system. The advantage of a honeypot system is that they do not require known attack signatures to work correctly (Peter, E; Schiller, T., 2008).

T-pot is a honeypot platform supporting over 20 different honeypot systems. It is using Kibana for visualization. It is a way for the organisation to test out the capabilities of a honeypot in an easy manner. The figure 10 shows data from installed honeypots. There are 36 152 alerts in 60 seconds period, 1 359 233 alerts in an hour, and 31 514 620 alerts in a day. The attack map shows visualisation of the attacks with green lines. The graph shows how alerts are distributed to distinct types of honeypots, from which country the attack is launched, and which is the target country. It also shows the location of the honeypots and the ports the attacker is targeting. By building the custom honeypots, the organisation can visualise and analyse the data that is important to protecting their business. And use that data to improve the situation picture.

Figure 10. Visualisation of a T-Pot from a sicherheitstacho.io (sicherheitstacho, 2024)

3.6.3 The Honeypot systems in the governments use

NATO's cyber exercise Cyber Coalition 2020 used a deceptive cybersecurity practice in a cyber exercise. The idea on these honeypots was to get the attacker to attack against these easy targets on a honeynet environment to get information about the attacker's methods, techniques and interact with the attacker. According to Defence One the use of honeypots by governments is a recent phenomenon. Also, the NSA has said that they have begun to utilise honeypots as a means of gathering intelligence. According to NSA's director of research Deborah Frincke they are looking for new ways to understand defences and we should think about defensive deception. A honeypot can give you a peek into an adversary's mindset. The honeypots can also provide insight on how to determine if the attacker is a human or automated system. (Tucker, 2020).

The chief of NATO's Cyber Security Centre will not say whether NATO currently has honeypots in real-world settings, because they will not reveal their active tactics but states that they use every defensive means that is available to defend networks (Tucker, 2020).

According to Breaking Defence's Defense Innovation Unit DIU has prototyped CounterCraft's platform which will help to detect and provide intelligence on cyber threats. In the year 2020 the platform was experimented by NATO to lure and identify hackers. This modern technology will assist the military to catch and stop insider threats and compromised networks. The Cyber Deception Platform is a honeypot for trapping a hostile actor to reveal their techniques, tools, and command structure (Atherton, 2021).

The United Kingdom's National Grid is planning to implement honeypots to improve security resilience. The plans include false resources and lure documents (Corfield; Leake, 2023). The United Kingdom has a National Cyber Deception Laboratory (NCDL), that was established in 2019 by Cranfield University in partnership with the UK MOD's Defence Cyber School. The NCDL offers guidance on using the cyber deception as part of a cyber defence strategy (NCDL, n.d.).

3.6.4 The honey tokens

> *"Imagine being able to bait cyber attackers into revealing their presence before they compromise your systems." Levy, 2023*

Honey tokens are digital entities for detecting an on-going cyber-attack at its initial stages. The honey tokens can dispatch an alarm when accessed allowing the security team to mitigate the impact of a cyber-attack, monitor the attacker and deceive the attacker. Honey tokens are a simple and cost-effective way to add an additional non-intrusive layer of security to the production systems. There are several types of honey tokens for different purposes. A data-based honey token can be fake user credentials or fake access keys. When the fake credentials are used an alarm is triggered. A database honey token is triggered when queries are made to these fake data tables or records. When file-based honey tokens, such as confidential documents or sensitive documents are accessed, an incident emerges. A token-based honey tokens operate as digital breadcrumbs, those are unique tracking tokens for web applications, links, or API keys. In addition to implementing the honey tokens to the production environment, it is important to test the tokens periodically to make sure tokens work as intended. (Levy, 2023).

3.6.5 Detecting honeypots

As it is important to build deception systems that looks like a real environment, there are ways to validate deception systems. The organisation can use general open-source reconnaissance tools to check what information they are able to collect from the deception systems. There are numerous tools of where to pick the ones that fits. One can use general tools like Nmap network mapper, or framework such as OpenVAS – a vulnerability assessment scanner (OpenVAS, 2023), and PenBox – a penetration testing framework (PenBox, 2014) to collect information about the honeypots to find obvious mistakes. If the deception system is connected to the internet, there are also some service providers, such as Shodan (Honeyscore, 2024) and Checkpot scanner, that helps to improve deception systems. These tools can help to detect mistakes in the configuration of honeypots (Checkpot, 2018), but these same tools can also help the adversary to identify the deception environment.

4 Introducing the research case: Turla

Turla (also known as: Snake, UNC4210, Group 88, Venomous Bear, Waterbug, and Uroburos) is a sophisticated APT group with espionage and intelligence-gathering motivations primarily focusing on government entities, militaries, and embassies. It is widely believed that the group has been active since the late 1990s and it is believed to be one of the earliest examples of cyber espionage. Turla is sophisticated group famous for the ability to hijack satellite communications to control their malware and exfiltrate data (APT Profile: Turla, 2023). It is widely acknowledged that Turla is a Russian-based cyber threat group. It has victims in over 45 countries. Turla is known for spear phishing attacks, leveraging inhouse tools and malwares (Turla, 2023).

Turla campaigns from 1996 to 2023 presented in table 2.

Year	Campaign
1996	Moonlight Maze, widely known cyberespionage campaign
2008	Breach of the US Department of Defense
2013	Epic Turla, Turla infected several hundred computers in more than 45 countries
2014	Breach of the Swiss military firm RUAG
2014	Penguin Turla, built to infect servers running Linux
2015	Satellite Turla, build to hijack satellite-based internet traffic
2015	WITCHCOVEN, uses profiling techniques to collect technical information on the victim's computer
2015	Dubbed Crutch, backdoor & document stealer, used from 2015 to early 2020
2016	Skipper Turla, JavaScript payload and specific macro variant
2017	Turla Mosquito
2017	Carbon, sophisticated backdoor
2017	Kazuar, backdoor
2017	Gazer, backdoor
2018	Neuron & Nautilus
2018	KopiLuwak, javascript backdoor
2019	Topinambou, .NET malware
2019	PowerShell
2019	Poison Frog, C2
2020	COMrat, a second stage implant. The first version was identified in 2007.
2020	NewPass, C2
2020	HyperStack, backdoor. Kazuar, Carbon
2021	IronNetInjector, a loader
2021	TinyTurla, backdoor
2022	Phishing-based reconnaissance campaign in Eastern Europe
2023	Microsoft: Hackers turn Exchange servers into malware control centres

Table 2. Turla campaigns 1996-2023 (ETDA, 2023)

4.1 Summary of the events: APT case RUAG

The initial attack vector remains undetermined and the earliest logs containing technical traces from the attack are from September 2014; there were no proxy logs available beyond September 2014. The attack was discovered in January 2016 – nearly 1,5 years posterior of the moment where they could observe the attack from logs. The first C2 traffic is traced back to September 2014. According to the report they managed to monitor the attacker from February 2016 to early May 2016, before the discovery of the cyber-attack was breached (Figure 11) (GovCERT, 2016). Did the attacker discover before the attack that there was a deficient monitoring and logging system? Or was it a factor at all?

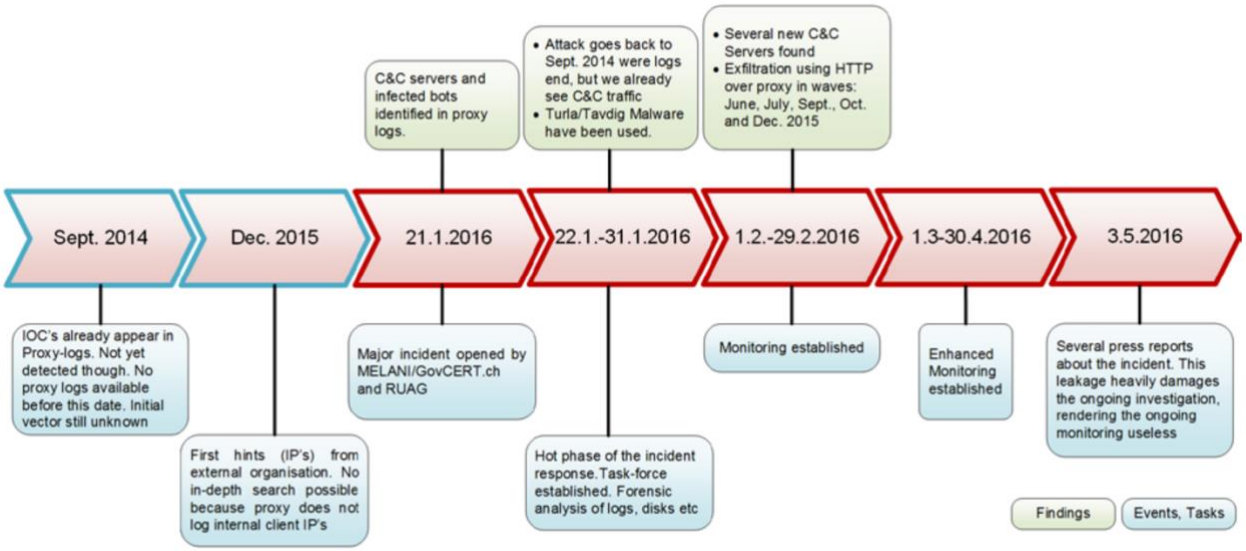


Figure 11. Case RUAG timeline (GovCERT 2016)

The chain of infection is undetermined, but the GovCERT-CH has based its analysis on the initial attack on the modus operandi of the attack group. The infection phase has three stages. The first one is a typical link to a watering hole -site that redirects to another site which has the actual harmful. The redirection can vary (GovCERT, 2016). It is common that these first reconnaissance steps are simple, such as user-agent information etc. According to the report, at the next step the attacker will test if the user's computer or other device meets the set requirements including manual confirmation by the attacker before the fingerprinting script is returned to the user. If the

requirements are met, the attacker will send a payload containing an exploit code to the user or use social engineering techniques to exploit the user's computer (GovCERT, 2016).

The attacker used Tavdig (also called as Epic and Wipbot) and Carbon DLL as most likely self-written malwares for reconnaissance of the user's computer, infecting the computer to gain initial foothold and persistence in the system, and for the C2 communication. The Tavdig malware used an injection method to compromise the user's computer. And after which, the attacker used publicly available tools for lateral movement and fingerprinting the system and environment. According to the report the attacker used mimikatz, pipelist, psexec, wmi, dsquery, dsget, ShareEnum as an addition to self-written patch scripts used in the attack. The attacker had two working C2 connections from the infected computers all the time, and if the user's computer were no longer employable the attacker would strive to delete its malicious files and stop the malicious services. The lateral movement can take a long time, when trying to hide your actions. To achieve control over the AD, the attacker used keyloggers, sniffing tools and relied on the Mimikatz tool. The attacker used some of the RUAG network's computers for executing tasks and collecting data and some for the communications; the report refers to them as worker drones and communications drones. Based on the report, the attacker did not steal all the information, but validated the targets of which it extracted the information from (GovCERT, 2016). This has some similarities to the SolarWinds Orion supply-chain attack, where the attacker had access into 18 000 compromised systems word widely but did not steal data from all the compromised systems (CFCS-DK, 2021) whereas the cyber-criminal would try to steal and encrypt all the information to gain most profit. Techniques used for the attack was Windows named pipes, hacked websites as C2 servers, and exfiltrating typically encrypted data.

The carbon malware is a sophisticated backdoor which can be used to steal sensitive information. It is described as a "second stage" malware in the RUAG report (GovCERT, 2016), but that only describes how the security researchers comprehend a cyber-attack, it does not mean it was the attacker's second stage of the cyber-attack.

Referring to the RUAG report, only a small amount of data had been transferred outside of the infected system during the eight months of the data breach. Total amount of (mostly) compressed data exfiltrated out of the system was 23Gb. Also, the volume of exfiltrated data varies strongly

during the period observed in their investigation. The most active periods took place from September to December (GovCERT, 2016).

Identified techniques used by the attacker are encryption, hacked websites and exfiltration. The attacker used hacked websites to initial attack, and exfiltrated target system's information encrypted to C2 server.

4.2 Summary of the events: Peering into Turla's second stage backdoor

According to the ESET's blog post a typical Carbon attack includes a reconnaissance stage on which the attacker uses spear phishing emails or compromised web pages to watering hole attacks to compromise the target system with a first stage malware, such as Tavdig. If the target is measured noteworthy enough, it will later receive a more sophisticated malware. After a successful first stage attacks the attacker uses the Carbon malware (ESET research, 2017).

According to ESET's malware analysis, the Carbon malware framework consists of several files. The Carbon also creates several files to keep logs and execute tasks. These filenames are hardcoded in the orchestrator file. The files sent to the C2 server are not compressed or encrypted. The Carbon malware uses mutexes to have exclusive access to its files in the working directory and to confirm that the orchestrator has been executed. The Carbon configuration file can be modified during the attack. The Carbon configuration file includes for example the unique UUID of the user's computer, list of processes a code is injected with, and the configuration for the C2 traffic. The Carbon logs carry actions performed by the malware and information on the system and are stored to the log file for further actions. The dropper file (SERVICE.EXE) is the only Carbon malware file that is not a DLL file. The loader (SERVICE.DLL) is a service that ensures Carbon's persistence is created. The orchestrator (MSIMGHELP.DLL) is used to inject code into a process that communicates legitimately over the internet and to dispatch the tasks received from the injected library to other computers on the same network. The malware has seven threads with roles:

- Monitor C2 addresses
- Monitor Carbon working directory, create log if not enough space
- Task execution, with different user modes

- dispatch tasks to computers from the same network
- communication channels
- Check internet connection
- Check packet capture software, if they are running, no communication is done

4.3 Summary of the events: Hunting Russian intelligence “Snake” malware

Snake, also called as Uroburos, is built to avoid large-scale cyber security monitoring detection. The malware is hard to detect because the attacker can change the modular malwares network-based signatures as they are discovered. The artefacts on the hosts (main targets or implants) can be moved into a different location or renamed. The files used are fully encrypted and accurately identifying them is difficult. The memory analysis provides the best visibility into attacker’s behaviour and artefacts left behind, but the scaling of memory analysis into a business network wide is difficult. Updated systems and meeting the password requirements protects the environment (AA23-129A, 2023).

According to the security advisory, the Snake malware is a sophisticated tool for cyber espionage and for long-term intelligence collection on sensitive targets. The malware has been evolving over 20 years and it has several variants. This malware has an ability to create peer-to-peer network of the snake-infected systems worldwide. These systems are ‘slaves’ that works as relay nodes between the infected systems and Turla’s main targets. The Snake infrastructure has been detected in over 50 countries worldwide. The malware has infected government networks, research facilities, and journalists. The Snake malware can be cross compiled to infect Windows, Linux, and MacOS systems. It has high level of stealth with its host components and network communication with means to employ modularity to merge new or replacement components. The Snake has capability to avoid detection from both host- and network-based defensive tools. AA23-129A (2023).

The Snake malware is used with combination of other tools, including native operating system tools to enumerate the network to obtain administrator credentials and to finally access the domain controllers. The Turla does not typically implement other heavyweight implants on

infected system but rely on credentials and lightweight remote-access tools within a victim network. Turla uses a reverse shell as a backup access vector to preserve a minimal presence in a network and avoid detection while moving laterally. The Snake malware uses legitimate servers as infrastructure. With Snakes stealthy network communication, the implanted systems which are not the command's main target will act as servers for other Snake nodes. The custom network communication protocols blend in with traffic that the compromised server normally would receive. This enables malware's C2 communication without opening any new ports and to avoid detection. (AA23-129A, 2023).

The malware has a custom communication protocol over common network protocols such as HTTP, SMTP, DNS, TCP, UDP, and ICPM with encryption and fragmentation capabilities. Snake malware has two custom transport encryption layers. Both layers have different encryption mechanisms. The transport encryption layer, enc, operates on peer-to-peer session and the application layer provides end-to-end encryption between the controller and the command's main target (victim). (AA23-129A, 2023).

The Snake installer is packed using a customized obfuscation methodology. The installer drops the kernel driver and a custom DLL which is used to load the driver into a single AES encrypted file on the disk (AA23-129A, 2023).

All the identified attack techniques as described in the advisory are presented in the appendix 3 and the attack techniques inserted to MITRE ATT&CK Navigator -tool are presented in the appendix 4.

4.4 The Turla malwares

The MITRE ATT&CK database comprises information from 27 software used by Turla (Table 3).

Software	Description
Arp	Address Resolution Protocol
Carbon	Also known as Cobra. A second-stage backdoor and framework (MITRE, 2021)
Certutil	Certutil.exe is a command-line program that is installed as part of Certificate Services (Certutil, 2016).
ComRAT	Also known as Chinch. A Remote Access Trojan (Faou, 2020)
Crutch	A backdoor. (Tavares, 2021)
Empire	A post-exploitation tool used to establish C2 (Microsoft Security Intelligence, 2023)
Epic	Also known as Tavdig, Wipbot. A backdoor (MITRE, 2020)
Gazer	A backdoor (Mohit, 2017)
HyperStack	An RPC backdoor (Schneier, 2021)
IronNetInjector	A malware downloading tool (Reichel, 2021)
Kazuar	A backdoor trojan (Falcone et al., 2017)
KOPILUWAK	A JavaScript backdoor (Huss, 2017)
LightNeuron	A backdoor specifically designed to target Microsoft's Exchange mail servers (Faou, 2019)
Mimikatz	A tool for extracting sensitive information from a system's memory (Mulder, 2016)
Mosquito	A backdoor (Diplomats in Eastern Europe bitten by a Turla mosquito, 2018)
NBTscan	NBTscan is a program for scanning IP networks for NetBIOS name information (nbtscan, 2022)
Nbstat	Displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache (nbstat, 2023)
Net	Net Commands can be used to perform operations for example on groups, users, account policies, and shares (Net Commands on Operating Systems, 2023)

Netstat	Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 & IPv6 statistics (netstat, 2023)
Penguin	A remote access trojan targeting Linux operating systems (MITRE, 2022)
PowerStallion	A lightweight PowerShell backdoor using Microsoft OneDrive as C2 server (Dumont, 2019)
PsExec	A sysinternals tool
Reg	Performs operations on registry subkey information and values in registry entries (reg commands, 2023)
Systeminfo	Displays configuration information about a computer and its operating system (systeminfo, 2023)
Tasklist	A list of currently running processes
TinyTurla	A backdoor and a second-stage dropper (Unterbrink, 2021)
Uroburos	Also known as Snake. A sophisticated cyber espionage tool written in C (MITRE, 2023)

Table 3. Turla software from the MITRE ATT&CK database

4.5 Identifying and charting the Turla techniques with MITRE ATT&CK Navigator -tool

In the MITRE ATT&CK Navigator -tool the different software techniques are separated with colours and then given a unique score to simplify the assortment (Figure 12). Comparing the collected data to the data chart from MITRE ATT&CK “Turla techniques” on Figure 13, it is notable that there is much more information that could be harvested from the software chart (Figure 12) than in “Turla techniques” chart (Figure 13).

There are some difficulties with the Navigator -tools suitability for the research because it does not allow to analyse the data with enough precision, therefor it is replaced with the Excel -tool instead. The data is collected manually from the MITRE ATT&CK Enterprise database to an Excel. The techniques and sub-techniques are scored with 1 or 0:

- 1 if the tool used the technique and
- 0 if the technique was not used.

After the scoring phase, the unused cells are removed to chart out what are the techniques used, which is used most, and which less. All the data that was collected and charted is presented in the Appendix 1.

Excel sheets are used for the more precise assortment of the data; the Navigator -tool gives a good overall understanding of the wide broad of techniques the Turla uses.

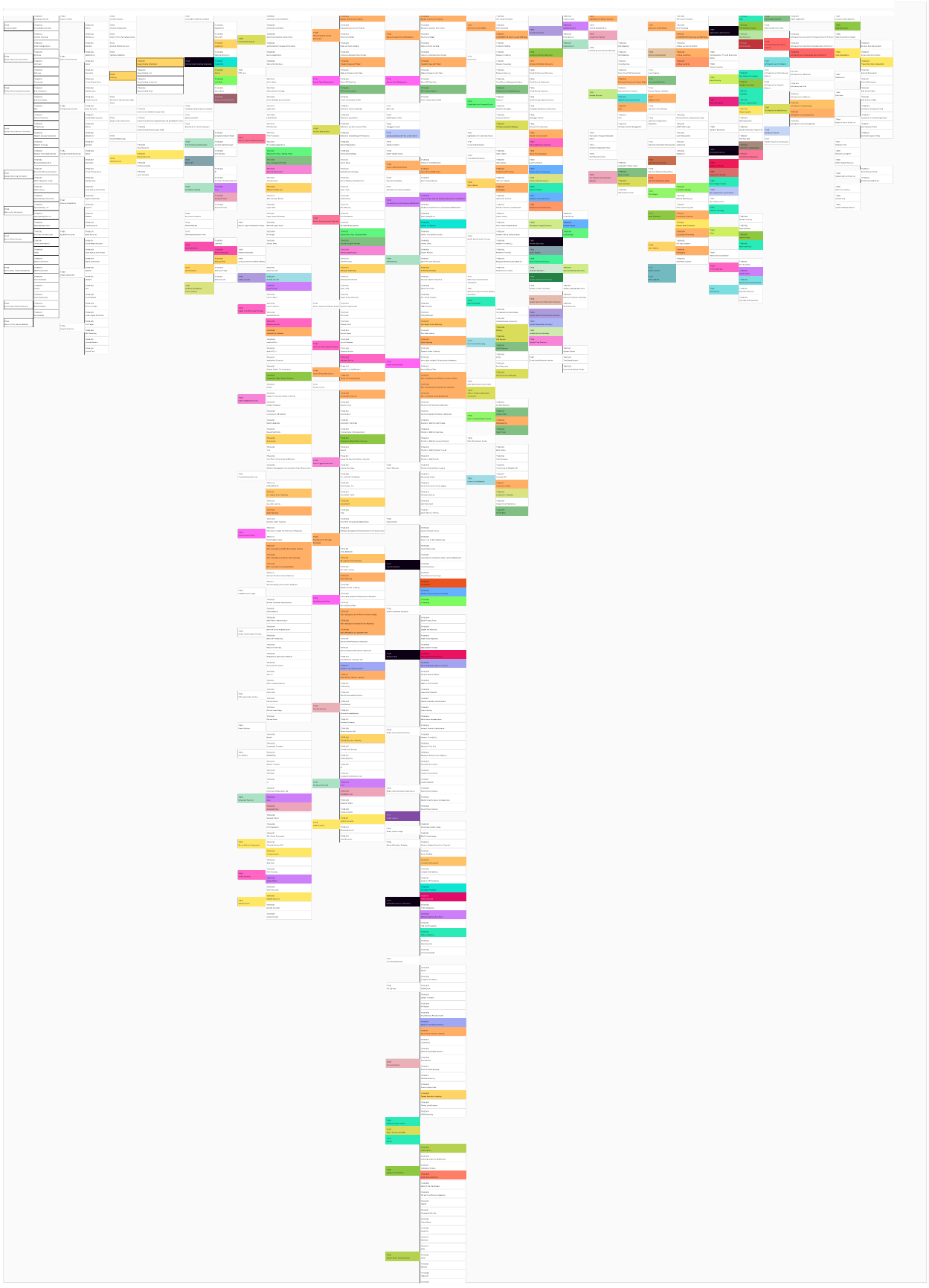


Figure 12. The MITRE ATT&CK Navigator -view from collected data with color-coding and scores

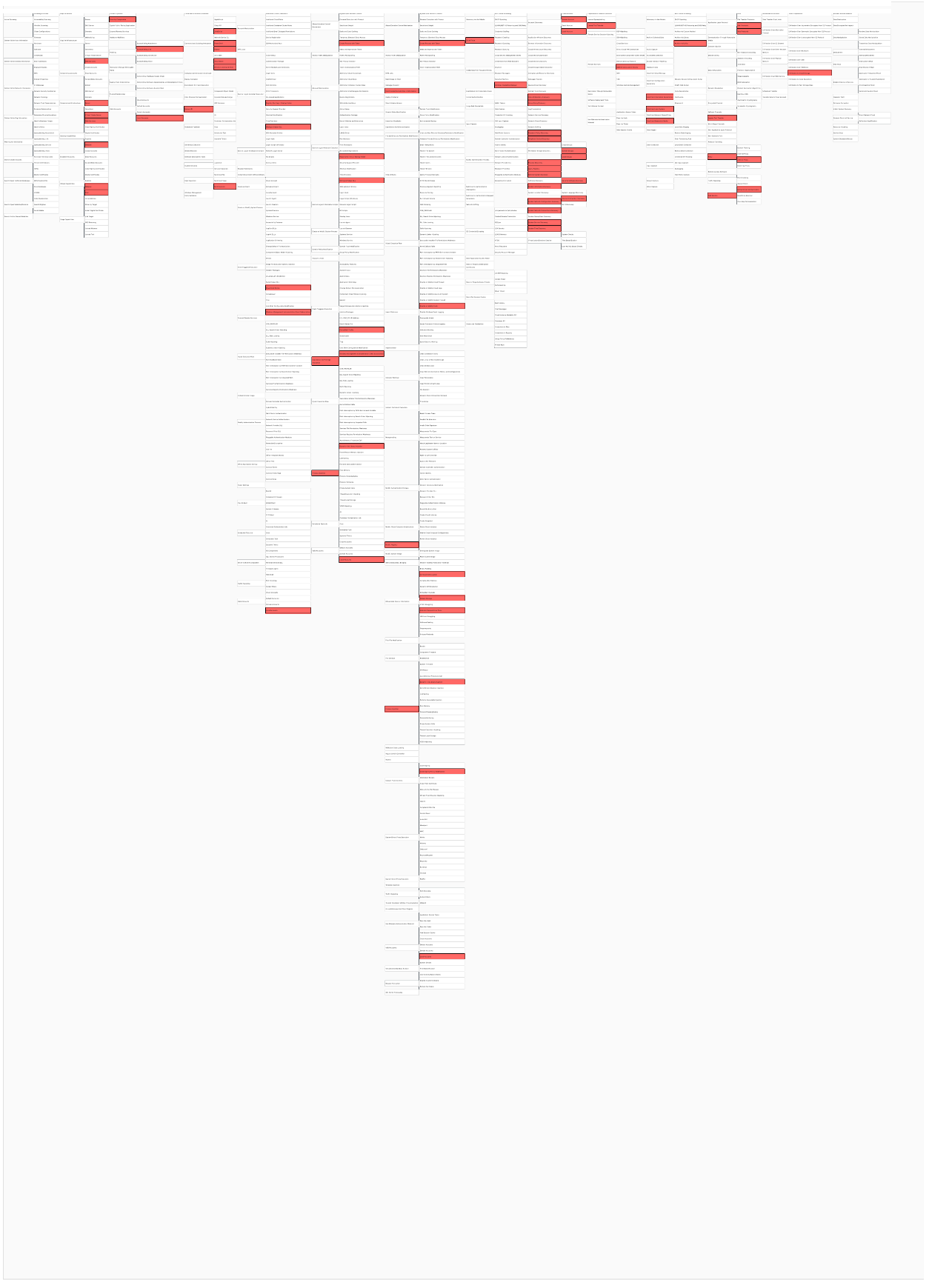


Figure 13. The APT actor Turla's TTP's as presented in MITRE ATT&CK Navigator

5 The results

Some of the used software are common tools on operating systems, such as Sysinternals (advanced system utilities) in Windows or Cron at Linux. The MITRE ATT&CK Enterprise matrix includes 201 techniques and 424 sub-techniques. After charting and scoring all the Turla software techniques with the Excel, the sheet has 192 rows: 192 techniques or sub-techniques all presented in the appendix 1. The Turla's most used attack techniques are presented on the appendix 2. The attack techniques with Snake malware are inserted to MITRE ATT&CK Navigator -tool and presented in the appendix 4. One example of a heatmap of Turla's techniques with MITRE ATT&CK Navigator -tool is presented in the appendix 5.

5.1 The discovered cyber kill chain of the Turla

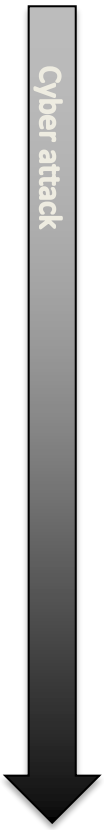
Based on the attack phases, the Turla's most used techniques are presented on the Figure 14. Based on the MITRE ATT&CK enterprise database, for the initial access Turla have used only two malwares, Kopiluvak and HyperStack -backdoors. (Figure 12;Figure 14). For the Execution phase Turla have used the command and scripting technique with nine different malwares, most operating systems offer a build-in command line interface and scripting capability. The attacker can use these tools for executing arbitrary commands. To gain persistence and privilege escalation Turla used boot or logon autostart execution -technique. Some of the autostart programs run with higher privileges, therefor the attacker can use those programs for leverage to elevate privileges. The attacker can modify the system configurations, such as Windows registry, to automate a program to start at system boot or logon to gain persistence and elevate privileges. (MITRE ATT&CK, 2024)

For the defence evasion the Turla used obfuscated files or information technique. The malicious file, payload or script can be encrypted, encoded, archived or other way obfuscated to avoid automated or signature-based detection and other security control mechanisms. To gain credential access, Turla used operating system credential jumping and stealing or forging Kerberos ticket -techniques. The Turla malwares include a keylogging abilities and credential dumping for gaining access to legitimate credentials for more difficult detection and adding more users. For the system discovery Turla used system network configuration discovery and process discovery – techniques with native operating system tools and malwares to access information about the

network configuration and settings. In Windows environment the Turla gathered information about the processes with native api calls and using tasklist -command. (MITRE ATT&CK, 2024)

For the lateral movement, Turla used the Empire malware and native operating system tools with use alternate authentication material -technique. To perform a successful use of the alternate authentication material -technique attack, the Turla had to have a successful credential access -attack phase to be able to bypass system access controls and authenticate to systems. For the remote services -technique Turla used the Mimikaz software. Before the lateral movement, the Turla has carried out different system and network discovery techniques, and privilege escalation operation to enable the pivoting through systems. To use remote services -technique the Turla used valid accounts -technique for persistence, privilege escalation, and defence evasion (Appendix 1). The valid account technique enables attacker to log in to remote services and perform actions as a logged-on user. (MITRE ATT&CK, 2024)

Data from local system – and data staged – techniques were used for the collection phase. According to the MITRE ATT&CK database, Turla collected information successfully from the local system. To command and control, Turla used OSI application layer protocol - and encrypted channel -technique. The application layer protocols are used to hide the C2 traffic from detection, and therefor commonly used DNS, file transfer protocols (SMB), mail protocols, and web protocols. Turla also used an encryption algorithm to conceal C2 traffic from detection. For the exfiltration, Turla used C2 channels and scheduled transfer -techniques. The stolen information was transferred by encoding it to the C2 traffic and exfiltrating it onward on certain time. The malwares, such as the Empire (Appendix 1), has a capability to automate exfiltration and exfiltrate information through cloud storage. (MITRE ATT&CK, 2024)



Tactics	ID	Technique
TA0001: Initial Access	T1566	Phishing
	T1078	Valid Accounts
TA0002: Execution	T1059	Command and Scripting Interpreter
TA0003: Persistence	T1547	Boot or Logon Autostart Execution
TA0004: Privilege Escalation	T1547	Boot or Logon Autostart Execution
TA0005: Defense Evasion	T1027	Obfuscated Files or Information
TA0006: Credential Access	T1003	OS Credential Dumping
	T1558	Steal or Forge Kerberos Tickets
TA0007: Discovery	T1016	System Network Configuration Discovery
	T1057	Process Discovery
TA0008: Lateral Movement	T1021	Remote Services
	T1550	Use Alternate Authentication Material
TA0009: Collection	T1005	Data from Local System
	T1074	Data Staged
TA0011: Command and Contro	T1071	Application Layer Protocol
	T1573	Encrypted Channel
TA0010: Exfiltration	T1041	Exfiltration Over C2 Channel
	T1029	Scheduled Transfer

Figure 14. Turla's cyber kill chain

5.2 Identified attack techniques based on the most used malwares

Of the 192 techniques through different attack phases charted from MITRE ATT&CK database (Figure 12), the Empire malware have used almost 50 % of all the identified techniques, the Uroburos have used 20 % of the identified techniques, and the Kazuar have used 17 % of all the identified techniques. It is noticeable that the Turla software (Table 3) did not use that many correlating techniques; over 40 % of all the Turla software used under ten different techniques of the full 192 identified Turla techniques. The Empire, Kazuar and Uroburos have six common techniques that all the three malwares have used (Figure 15). The Empire is a post-exploitation tool, with the C2 capability, the Kazuar is a backdoor trojan and the Uroburos is a cyber espionage tool. When comparing to the other used malwares by Turla, these are the malwares with the widest range of capabilities.

Based on the techniques identified (Figure 15;Figure 15) in addition to already identified techniques, Turla used system information technique for the discovery tactic. With system information discovery the Turla is accessing information about the victim operating system and hardware. This can be implemented with malwares or native operating system tools; Turla used both native tools and malwares. 30 % of the Turla malwares has system information capabilities. For the C2, Turla also used ingress tool transfer -technique to transfer tool from external system to the victim system. Turla used both malwares and certutil -native operating system tool. Carbon, Empire, Kazuar, and Uroburos can use create and modify system process -techniques for privilege escalation. This technique is commonly used with combination of masquerading techniques, for example TinyTurla and Uroburos have masquerading capabilities.

ID	Technique	ID	Sub-technique
T1057	Process Discovery		
T1059	Command and Scripting Interpeter	T1059.003	Windows Command Shell
T1071	Application Layer Protocol	T1071.001	Web Protocols
T1082	System Information Discovery		
T1105	Ingress Tool Transfer		
T1543	Create or Modify System Process	T1543.003	Windows Service

Figure 15. The most used techniques of the malwares with the most wide range of techniques

5.3 Identified Turla techniques based on the most used techniques in the attacks

According to the dataset collected from MITRE ATT&CK database, the most used techniques presented in the figure 16 are:

1. Discovery: System Network Configuration Discovery (41 %)
2. Discovery: Process Discovery (37 %)
3. Command and Control: Application Layer Protocols: Web Protocols (37 %) and
4. Discovery: System Information Discovery (30%).

Tactics	ID	Techniques	Sub-Technique ID	Sub-Technique	%
TA0007: Discovery	T1057	Process Discovery	Process Discovery		37 %
	T1082	System Information Discovery	System Information Discovery		30 %
	T1016	System Network Configuration Discovery	System Network Configuration Discovery		41 %
TA0011: Command and Control	T1071	Application Layer Protocol	T1071.001	Web Protocols	37 %

Figure 16. Most used tactics and techniques

Over 40 % of all the Turla software used System Network Configuration Discovery technique for the discovery -tactic. Almost 40 % of the software also used Process Discovery for the Discovery tactic. For the Command & Control, the most used technique was Application Layer Protocols with Web Protocols. 30 % of the software used System Information Discovery for the Discovery tactic.

This data shows the importance of the Discovery-phase of the attack for the adversary, and many of the software are capable for collecting system discovery information of the victim system.

5.4 Detecting Turla attacks with MITRE ATT&CK Data Sources

The detection method data is collected manually from the MITRE ATT&CK Data Sources (Data sources, 2024) and then joined with the most used attack techniques presented on the Appendix 2. When cross referencing the attack technique used by the ATP actor to the detection technique, it helps to identify ways to build credible honeypot which has two purposes: to deceit and to detect. According to the data collected the most efficient way to detect Turla attacks is Command execution, DS0017, that can detect 15 different attack techniques used by Turla (Figure 17). Based on the information collected, it can detect the Turla attack on all attack phases, except the initial access. DS0009, Process creation and, OS API execution can also create the capability to detect an Turla attacks' on almost every attack phase except the initial access, exfiltration, and C2. Monitoring the DS0022, File access and File creation, provide an opportunity to detect Turla attack on many of the attack phases (Table 4).

Attack tactics / attack phase	Command DS0017	Process DS0009	File DS0022
TA0001: Initial Access	✗	✗	✗
TA0002: Execution	✓	✓	✗
TA0003: Persistence	✓	✓	✓
TA0004: Privilege Escalation	✓	✓	✓
TA0005: Defense Evasion	✓	✓	✓
TA0006: Credential Access	✓	✓	✓
TA0007: Discovery	✓	✓	✗
TA0008: Lateral Movement	✓	✓	✗
TA0009: Collection	✓	✓	✓
TA0010: Exfiltration	✓	✗	✓
TA0011: Command and Control	✓	✗	✓

Table 4. Detecting Turla attacks

To detect the initial access by monitoring valid account -techniques, phishing attacks -techniques, and remote access -techniques could lead to detecting the Turla actor, because the data shows that Turla has used remote services -technique for lateral movement and valid accounts for credential access with stealing Kerberos tickets and credential dumping (Figure 17). It is quite typical for threat actor to use techniques that have worked before. Only after the technique has been discovered and blocked; new ways need to be discovered and implemented. The Turla has used data staging technique that might help to identify what data have been exfiltrated and for how long.

Tactics	ID	Attack technique	Detection ID	Detection data source	Detection data component
TA0002: Execution	T1059	Command and Scripting Interpreter	DS0017	Command	Command Execution
			DS0009	Process	Process Creation
TA0003: Persistence	T1547	Boot or Logon Autostart Execution	DS0017	Command	Command Execution
			DS0022	File	File Creation
			DS0009	Process	OS API Execution
TA0004: Privilege Escalation	T1543	Create or Modify System Process	DS0017	Command	Command Execution
			DS0022	File	File Creation
			DS0009	Process	OS API Execution
	T1547	Boot or Logon Autostart Execution	DS0017	Command	Command Execution
			DS0022	File	File Creation
			DS0009	Process	OS API Execution
			DS0009	Process	OS API Execution
			DS0017	Command	Command Execution
			DS0022	File	File Creation
			DS0017	Command	Command Execution
			DS0022	File	File Access
			DS0009	Process	OS API Execution
			DS0017	Command	Command Execution
			DS0022	File	File Access
TA0007: Discovery	T1016	System Network Configuration Discovery	DS0017	Command	Command Execution
			DS0009	Process	OS API Execution
	T1057	Process Discovery	DS0017	Command	Command Execution
			DS0009	Process	OS API Execution
	T1082	System Information Discovery	DS0017	Command	Command Execution
			DS0009	Process	OS API Execution
TA0008: Lateral Movement	T1021	Remote Services	DS0017	Command	Command Execution
			DS0009	Process	Process Creation
TA0009: Collection	T1005	Data from Local System	DS0017	Command	Command Execution
			DS0022	File	File Access
			DS0009	Process	OS API Execution
	T1074	Data Staged	DS0017	Command	Command Execution
			DS0022	File	File Access
	T1105	Ingress Tool Transfer	DS0017	Command	Command Execution
			DS0022	File	File Creation
TA0010: Exfiltration	T1041	Exfiltration Over C2 Channel	DS0017	Command	Command Execution
			DS0022	File	File Access

Figure 17. Detecting Turla attacks on almost every attack phases

5.5 A connected, integrated or a standalone honeypot?

A connected honeynet can spoof local area networks as a decoy for the different system discovery requests. The connected honeynet would not deliver all the functionalities to detect new attack patterns or zero-day exploits but could provide enough functionality for specific known vulnerabilities (A knowledge graph of cybersecurity countermeasures, n.d.). Where an integrated honeynet could provide more information about the attack but the risks for the attacker to reach the production environment are greater. The attacker might be able to hide its actions and stop security controls in the system.

As it was seen in the cyber-attacks before (GovCERT, 2016), the attacker who already has access to the environment is also able to stop security processes monitoring the environment. When knowing the fact that the APT actors are doing thorough work to fingerprint and identify systems and users before proceeding the attacks; the integrated honeynet seems to be the only valid option for luring APT actors to attack deeper than just the initial access. A standalone honeynet is fully isolated from the production environment and it would be an option for simple monitoring purposes. The standalone honeynet would be easier to run down in a case, where the attacker would have full access to the system or when it would be encrypted. It would be easier to automate the rebuilding of a standalone system, but it would not be cost-effective to build a fully isolated honeynet for simple monitoring purposes, only. The probability of a generic cyber attack and ransomware attack would be high on a fully isolated generic honeypot. Therefor the fully isolated honeypot would not meet the set requirements.

According to MITRE D3fend, a decoy file could be a way to detect and deceive an attacker in the system if the attacker is using System owner/user discovery -technique. In addition to that, the deception system should include many available decoy objects for monitoring purposes and those objects should not be used or accessed for any real-life business purposes. When inserting these objects to the production environment, logging and monitoring for these assets needs to be configured to detect indicators of compromise. It is vital to modify and obfuscate the decoy objects to look as real as possible. One might also use a threat modelling method to model the APT actors targeting the production environment to make those decoy objects more inviting to the attacker. This method might also be a way to distract an on-going cyber-attack and redirect the attacker to a certain direction in the production environment. And to get the attacker to spent

time with the deception systems to implement and execute defensive methods during an on-going cyber-attack. For example, a ransomware or a wiper attack can be a time sensitive cyber attack when trying to isolate a cyber attack.

6 Conclusions

The assignment was to identify different types of technical considerations for a deception system to attract an APT actor into one, and based on the research material these aspects can be identified.

Based on the research material, a deception system needs to look and function as a real-life information system. First, the organisation needs to chart the systems it already has. For example, if there are no Linux servers, it does not matter – a honeypot can be a Linux system or SCADA- or PLC-system can be honeypot even though the organisation does not have any SCADA- or PLC-systems in the enterprise network. The attacker will not know it beforehand, what belongs there and what is not. The is a GitHub repository (Nazario, 2024) listing several types of deception systems. Some of them can redirect attackers on the honeypots, based on the IP address they use. One of the honeypots lets the attacker use stolen credentials and it logs distinct types of logins attempts and credentials used. These can all trigger an alarm to the SIEM system. Several of those honeypots include known vulnerabilities, such as LOG4J, that help to monitor distinct types of attack attempts and attack techniques. One of the listed honeypots is a masscanned, that offers information if the organisation is being scanned. It supports both network layer protocols and application layer protocols. For example, masscanned answers to arp, which was one of the software Turla is reported to have used.

Turla used NBTscan, that can list active users, scan IP networks, list NetBIOS computer names and collect MAC addresses. This indicates that the honeypots need to have users and internet traffic. Based on the research data the Turla uses several types of discovery techniques widely. Therefor the honeypot needs to be developed with the same frame as all the other systems in the network – to look real. But it should have some vulnerabilities, configuration errors, and some older version software to enable lateral movement and defence evasion. The Turla used defence evasion techniques to avoid detection. These techniques include obfuscation and uninstalling or disabling security software. An older version of the antivirus product could give the attacker a free pass to

use simpler but malicious software. If not an older version, leave the antivirus product out from the centralised maintenance, that it would have outdated fingerprints.

The material shows that there should be ways to exfiltrate data or enable C2 traffic. This must be done in such a way that the organisation is still able to monitor the data traffic. To get the attacker interested in the honeypot, there should be interesting material on it – or at least material that seems to be interesting. If the organisation is volunteering and willing to let the attacker steal the information from some network share or etcetera, it must be kept in mind that there might be great reputational damage to the organisation even then, when the material is fake. A canary token would be a correct choice to employ a deception tool to the folder including seemly interesting documents. This can also help to identify an insider threat or even a mole.

10 % of the software used persistence techniques, there are some risks included when allowing willingly the attacker to get that comprehensive access to the system. But if the system is not integrated honeypot, that can be a one way to implement a honeypot. It would be difficult to recommend that for integrated honeypot.

To build a honeypot from the techniques used in the RUAG attack, the environment should look real enough with real tools, users, and protection. The environment should be on regular maintenance and security patches should be installed – but not all and not in every system. It should seem a legit system. Therefore, not to update systems with specific versions with certain vulnerabilities. The attack should be difficult but not hard, even easy on some targets. The deception system should have entry points to honeynet and honeypots, some can be easy, but it should be kept in mind that the purpose is to attract APT actors and not the automated attacks or cyber criminals. To observe these attacks on a honeypot, all the opportunistic attacks should be monitored and identified to distinguish them from a targeted cyber-attack. A network proxy should be implemented, but not an efficient one, but to have calculated mistakes on the configurations. A management workstation in the production environment is an efficient lure. On a honeypot workstation the applications and client to client communication should be allowed.

Based on the case RUAG, there is no need to give internet access to the management workstations, because of the peer-to-peer traffic allowed. Insert management tools and folders in the management honeypot system to make it a more appealing and interesting target for the attacker. To lure an attacker to the system, use a decoy person to open and click phishing emails, to be active on social media and to draw attention. Use decoy files in the system. The decoy files could be configuration files, documents, images, inventory list, personnel lists, and contract drafts. Those files should seem real, credible, and interesting. A honey token would seem like a valid option to fill these technical requirements for a decoy object.

A deception system can be used for different purposes, but mainly to collect information and to protect the production environment. When using it for collecting information of the cyber-attack, it might be enough to use a connected deception system to gather the cyber threat intelligence information or different trends of the cyber-attacks targeting the organisation. If using deception systems for cyber threat hunting, to find an on-going cyber attack, the honey tokens might be a proficient way. Furthermore, the honey tokens could be a way to detect an insider threat. To protect the production environment, an implementation of the integrated honeynet system would be the most effective way – when tested regularly that it works correctly. The integrated honeynet comes with the biggest cyber threats, because the attacker can find a way to utilise or exploit them against the organisation itself. The deception system would be a way to detect a cyber-attack at its earliest stage as possible.

The most efficient and cost-effective way to implement a deception system seems to be implementing an integrated deception system inside the enterprise network and into production networks. Implementing needs to be based on the assessment of the protected environment. The best results come, when combining larger integrated honeynet with the simpler honey tokens. The honey tokens are an easy and effective way to get started when willing to increase security layers of the production networks. The honeypot with the capabilities to redirect the attacker to a certain network sector is also an effective defensive mechanism.

7 Discussions

The research was successful, but there were some struggles with the original intended research method used, in which the data was scored and classified with the MITRE ATT&CK Navigator-tool. The original method did not give answers with sufficient precision. In addition, there were some limitations with the MITRE ATT&CK Navigator, bacause it had a capability for charting only ten software at the time, and therefore the collection needed to be done in series of ten software and united to one chart. Eventually, the data was collected manually and there might be some human errors with the collection process. The Excel charting worked with adequate precision for the data analysis of this amount of data and information.

7.1 The reliability of the research

There are few aspects to consider when evaluating the reliability of the research. The research material in the MITRE ATT&CK knowledge base does not include all the advanced persistent threat groups, for example, the MITRE knowledge base does not chart out cyber actor groups from the United States of America. The MITRE material can include biases of the cyber threat reports from which the material is gathered. There can also be inaccuracies with the attributions made, both with the malwares and techniques used. Regarding the research material used in this study, many of the common software are used by many cyber threat actors. The cyber threat actors are also known to recycle or borrow techniques or malwares from other cyber threat actor groups. It would also be useful to analyse, what is not being detected in the MITRE ATT&CK Enterprise Matrix and why.

The MITRE ATT&CK (Table 3) does not include all the identified Turla malwares, for example, such as Andromeda and QuietCanary that are reported by Mandiant (Hawley et al, 2023) are missing. The ETDA (Table 2) does not include all the Turla campaign attacks, for example, such as reported by ESET: the Finnish Foreign Ministry in 2013, and the German government at the end of 2017 to beginning of 2018 (Diplomats in Eastern Europe bitten by a Turla mosquito, 2018). These are merely examples, that the databases and the reports are not all-comprehensive power tools, and there is still some work and information gathering that needs to be done manually to get a complete sampling of a threat actor. And it also needs upkeeping and alterations.

The research material needed to be chart and scored manually, because the original data collection methods produced information that could not be analysed with the precision needed. To data collection manually was slow and challenging task, if there were more data and information to be collected, this would not be an efficient way to do it. The processing of the information and data would be unrewarding. The changes in the original data would be difficult to follow up and maintain in the Excel chart. The scoring could be more complex than 1 or 0, because some techniques were used by the operating system native tools, example, and other are custom malwares.

A sufficient heat map could be a better way to evaluate the actions of the threat actor. Also, the different attack techniques and attack phases could get a scoring, that would support ways to identify more important attack phases or techniques compared to the research now, where all techniques and phases had same value and therefor the same importance. When identifying the assets of the organisation, the scoring could also come from the organisational need to protect targets that are more important to the business.

7.2 The original scoring method and MITRE ATT&CK Navigator -tool

As can be seen from figure 12, the number coding -method with the original research method with ATT&CK Navigator was a somewhat failure and the colour coding is unreliable, the black cells should be the techniques used most, as presented in the figure 18. But it did not work as planned. The number coding had to be done again with different scoring methods. The unique score differs the malwares in the Navigator, but it does not allow the reversing from the final score to factor the malwares in a method, that would separate the times malware was used for specific technique, because the techniques can occur in multiple tactics.

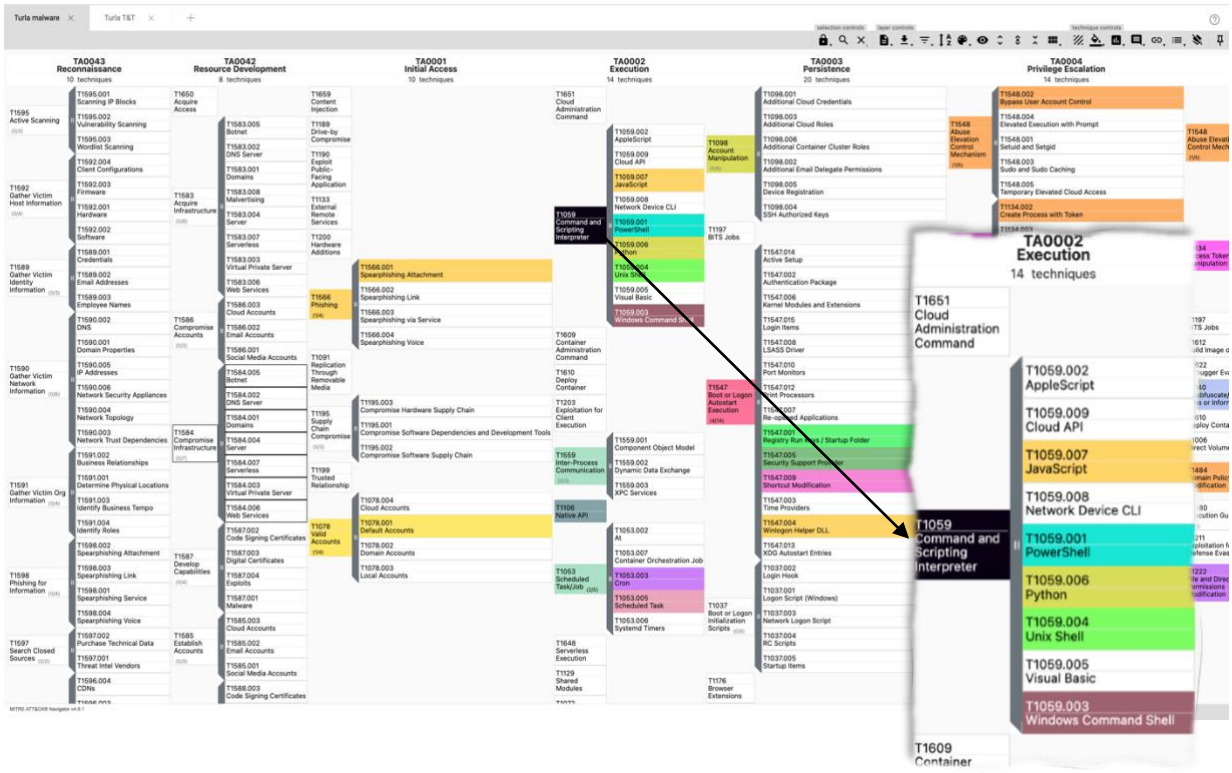


Figure 18. MITRE ATT&CK Navigator -tool with the color coding error

As demonstrated on figure 19, the JavaScript (score 144), PowerShell (score 770), Python (200), Unix Shell (score 642), and Windows Command Shell (score 2145) and total score 3973. It would be impossible to count backwards to the original factors behind the score as presented in the Excel sheet (Figure 20).

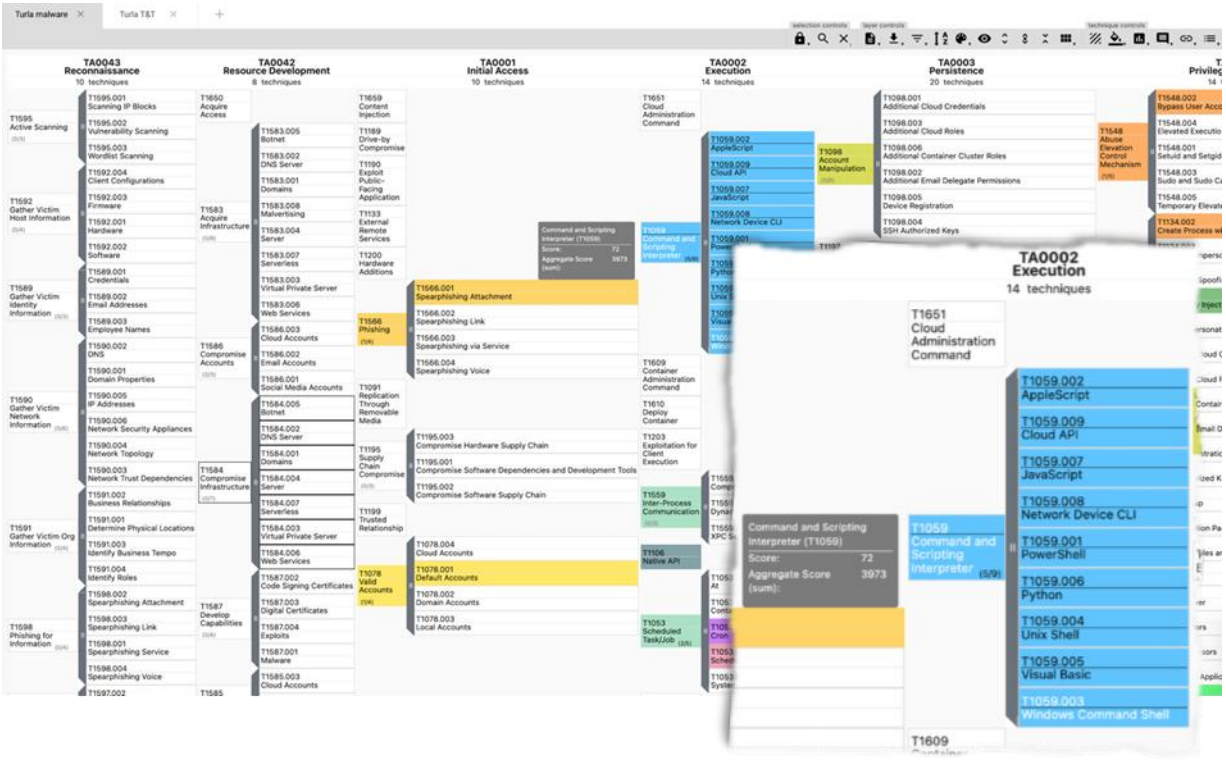


Figure 19. The scoring scenery in MITRE ATT&CK Navigator -tool

ution	T1059	Command and Scripting Interpreter	T1059.007	JavaScript	4 %
			T1059.001	PowerShell	15 %
			T1059.006	Python	4 %
			T1059.004	Unix Shell	7 %
			T1059.003	Windows Command Shell	26 %

Figure 20. Example of the properly functioning scoring system

The MITRE ATT&CK Navigator -tool allows to export data tables as csv, JSON, and svg, but imports must be in JSON format. There could be more suitable tools for analysing the data than Excel. But for this research, when the data amount was small, including only one threat actor and its 27 software, it was enough. But for future applications, more flexible tool could be better for this kind of data analyses and visualisation. There are also commercial products available with threat actor data included, that could be suitable for this kind of data handling and threat actor modelling.

7.3 The deception systems and further studies

The next step should be a proof of concept -honeypot to collect real-life indicators of the cyber attacks from the honeypots to verify the findings. The simplest way to further study the research results could be to implement the honey tokens in a single simple standalone deception network and see the results. And from there and from those results, to develop honey tokens for the enterprise environment. Monitoring the (vulnerability) scanning targeted to the organisation, there could be a way to identify more specific ways to improve the deception systems and the detection methods used.

To get more comprehensive coverage about the study, it would be useful to choose a few APT actors whose objects and interests would be the defender's organisation or business and learn from the tactics and techniques they used in the recent cyber attacks. And to threat model those cyber threat actors based on the assets and information the organisation aims to protect. It is difficult to find technical APT reports that include the whole cyber attack chain (cyber kill chain), because the initial access cannot always be confirmed by the cyber security team. It could be that the initial attack has been too long ago from the moment the attack is discovered, consequently there are not any logs left to observe. There might be inefficient overall logging in the breached system, or the attacker might have had a chance to delete security logs to cover its traces. In some of the APT cases, the attacker has had the initial access to the system, for example in the well-known supply chain attack case SolarWinds Orion, but the next stages of the attack never occurred for all the victims. Maybe it was because the targeted systems did not meet the requirements of the attacker, hence not the original target or the target was not interesting enough.

References

AA20-352A. (2020, April 15). Advanced Persistent Threat Compromise of Government Agencies. Critical Infrastructure, and Private Sector Organizations. CISA. Accessed 3 January 2024. Retrieved from https://www.cisa.gov/uscert/ncas/alerts/aa20-352a

AA23-129A. (2023, May 9): Joint Cybersecurity Advisory. Hunting Russian Intelligence “Snake” Malware. CISA. Accessed 3 January 2024. Retrieved from https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_2.pdf

A knowledge graph of cybersecurity countermeasures. (n.d.). Mitre. Accessed 3 December 2023. Retrieved from https://d3fend.mitre.org/

Ali-Ahmed, W., Sullivan, T. (2019). Survival of the Fastest: The 1-10-60 Rule. Splunk & CrowdStrike. Accessed 3 December 2023. Retrieved from https://conf.splunk.com/files/2019/slides/SEC1573.pdf

Amin, R., Cloppert, M., Hutchins, E. (2011). White paper. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Research Gate. Accessed 16 March 2024. Retrieved from https://www.researchgate.net/publication/266038451_Intelligence-Driven_Computer_Network_Defense_Informed_by_Analysis_of_Adversary_Campaigns_and_Intrusion_Kill_Chains

APT Case RUAG. (2016). Technical report. GOVCERT-CH. Accessed 15 June 2023. Retrieved from https://www.govcert.ch/downloads/whitepapers/Report_Ruag-Espionage-Case.pdf

APT profile: Turla. (2023, June 29). Accessed 2 January 2024. Retrieved from https://socradar.io/apt-profile-turla/

Atherton, K. (2021). DIU Turns to Honeypots for Advanced Cyber Defense. Breaking Defense. Accessed 15 June 2023. Retrieved from https://breakingdefense.com/2021/01/diu-turns-to-honeypots-for- advanced-cyber-defense/

Awesome Honeypots. (2022). Accessed 15 June 2023. Retrieved from https://github.com/paralax/awesome-honeypots

Biggio, B., Demontis, A., Elovici, Y., Gelei, D., Kotak, J., Lee, W., Mirsky, Y., Pintor, M., Shankar, R., Yang, L., Zhang, X. (2023). The Threat of Offensive AI to Organizations. Computers & Security. Volume 124. ISSN 0167-4048. https://doi.org/10.1016/j.cose.2022.103006. Accessed 16 March 2024. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404822003984

Boutin, J., Faou, M. (2018, March 8). Visiting the Snake Nest. Recon Brussels 2018. Accessed 3 December 2023. Retrieved from https://www.youtube.com/watch?v=7-H4KurTCUQ

Busselen, M. (2018, May 9). CrowdStrike on Dark Reading: Why “Breakout Time” Is Critical to Your Security Strategy. Blog. Endpoint security and EDR. Accessed 3 December 2023. Retrieved from https://www.crowdstrike.com/blog/crowdstrike-discusses-breakout-time-in-an-article-on-dark-reading/

Carnaghan, I. (2014, September 11). Honeypots: To lure or not to lure. Accessed 3 December 2023. Retrieved from https://www.carnaghan.com/honeypots-to-lure-or-not-to-lure/

Case study. (2010, March 9). Accessed 15 June 2023. Retrieved from https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/strategies/case-study

Categories, Classes and Types. (2010, March 9). Accessed 15 June 2023. Retrieved from https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/strategies/case-study

Cen, M., Doss, R., Jiang, F., Qin, X. (2023). Hybrid cyber defense strategies using Honey-X: A survey, Computer Networks. Volume 230. ISSN 1389-1286. https://doi.org/10.1016/j.comnet.2023.109776. Accessed 16 March 2024. Retrieved from https://www.sciencedirect.com/science/article/pii/S1389128623002219

Certutil. (2016, August 31). Microsoft Windows documentation. Accessed 15 January 2024. Retrieved from https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc732443(v=ws.11)

CFCS-DK. (2021). Investigation report: SolarWinds: State-sponsored global software supply chain attack The story behind one of the largest supply chain attacks in history. Accessed 3 December 2023. Retrieved from https://www.cfcs.dk/globalassets/cfcs/dokumenter/rapporter/en/CFCS-solarwinds-report-EN.pdf

Checkpot. (2018). GitHub-repository. Accessed 3 December 2023. Checkpot scanner. Retrieved from https://github.com/honeynet/checkpot

CISA. (n.d.) Advanced Persistent Threats and Nation-State Actors. Cybersecurity & Infrastructure Security Agency. Accessed 15 January 2024. Retrieved from https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors

Cozens, B. (2023, May 18). A business blogs. APT attacks: Exploring Advanced Persistent Threats and their evasive techniques. Accessed 15 January 2024. Retrieved from https://www.malwarebytes.com/blog/business/2023/05/apt-attacks-exploring-advanced-persistent-threats-and-their-evasive-techniques

Cost of a Data Breach. (2022). Report. IBM Security. Accessed 3 December 2023. Retrieved from https://www.ibm.com/downloads/cas/3R8N1DZJ

Cuofano, G. (2023, October 31). Cybersecurity in A nutshell and why it matters in business. A blog. Accessed 10 January 2024. Retrieved from https://fourweekmba.com/cybersecurity/

Cyber kill chain. (2024). Accessed 16 March 2024. Retrieved from https://cloudprotection.withsecure.com/en/resources/articles/cyber-kill-chain

Data analysis. (2016, September 2). Accessed 13 June 2023. Retrieved from https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/data-analysis

Data sources. (2024). MITRE ATT&CK. Accessed 5 February 2024. Retrieved from https://attack.mitre.org/datasources/

Decoy Environment. (n.d.). Accessed 22 December 2023. Retrieved from https://d3fend.mitre.org/technique/d3f:DecoyEnvironment/

Dickinson, K. (2020). Implementer's Guide to Deception Technologies. White paper. Accessed 22 December 2023. Retrieved from https://sansorg.egnyte.com/dl/TaCELsutca

Diplomats in Eastern Europe bitten by a Turla mosquito. (2018). White paper. ESET. Accessed 22 December 2023. Retrieved from https://web-assets.esetstatic.com/wls/2018/01/ESET_Turla_Mosquito.pdf

Directive (EU) 2022/2555. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Accessed 16 March 2024. Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555

Dumont, R., Faou, M. (2019, May 29). Article. A dive into Turla PowerShell usage. ESET RESEARCH. Accessed 5 December 2023. Retrieved from https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/

Eissa, A. (2021, August 11). A Blog. Honeypot Types, Technologies, Detection Techniques, and Tools. Accessed 6 December 2023. Retrieved from https://www.linkedin.com/pulse/honeypots-types-technologies-detection-techniques-tools-ahmed-eissa

ENISA Threat Landscape. (2022, October 19). Accessed 6 December 2023. Retrieved from https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

Enterprise matrix. (2023). Accessed 8 December 2023. Retrieved from https://attack.mitre.org/matrices/enterprise/

Enterprise tactics. (2023). Accessed 8 December 2023. Retrieved from https://attack.mitre.org/tactics/enterprise/

Eskola, J., Saarela, M., Vilka, H. (2018). Ikkunoita tutkimusmetodeihin 1: Riittääkö yksi? Tapaustutkimus kuvaajana ja selittäjänä. PS-Kustannus. Jyväskylä.

ESET Research. (2017, March 30). A blog. Carbon Paper: Peering into Turla's second stage backdoor. Accessed 10 December 2023. Retrieved from https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/

ETDA. (2023). Threat Group Cards: A Threat Actor Encyclopaedia. Accessed 27 December 2023. Retrieved from https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Turla%2C%20Waterbug%2C%20Venomous%20Bear

Exabeam. (2024). Cyber Kill Chain vs. Mitre ATT&CK®: 4 Key Differences and Synergies. Accessed 16 March 2024. Retrieved from https://www.exabeam.com/explainers/mitre-attck/cyber-kill-chain-vs-mitre-attck-4-key-differences-and-synergies/

Faou, M. (2019, May). White paper. TURLA LIGHTNEURON - One email away from remote code execution. Accessed 10 December 2023. Retrieved from https://web-assets.esetstatic.com/wls/2019/05/ESET-LightNeuron.pdf

Faou, M. (2020, May 26). Article. Accessed 10 December 2023. Retrieved from https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/

General Data Protection Regulation (EU) 2016/679. (2016, May 5). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Global Threat Report. (2024). CrowdStrike. Accessed 25 February 2024. Retrieved from https://www.crowdstrike.com/global-threat-report/

Global threat report. (2023). CrowdStrike. Accessed 3 January 2024. Retrieved from https://www.crowdstrike.com/global-threat-report/

GovCERT. (2016). Summary: Technical Report about the Espionage Case at RUAG. Swiss Government Computer Emergency Response Team. Accessed 15 June 2023. Retrieved from https://www.govcert.ch/downloads/whitepapers/Summary_Report_Ruag-Espionage-Case.pdf

Government's Defence report. (2021, September 9). Publications of the Finnish Government 2021:80. Accessed 15 June 2023. Retrieved from https://julkaisut.valtioneuvosto.fi/handle/10024/163407

Groups. (2024). Accessed 10 February 2024. Retrieved from https://attack.mitre.org/groups/

Hawley, S., Mattos, E., McLellan, T., Roncone, G., Wolfram, J. (2023, January 5). Turla: A Galaxy of Opportunity. A blog. Accessed 28 December 2023. Retrieved from https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

Honeypots in cybersecurity explained. (2021, March 9). Accessed 10 December 2023. Retrieved from https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/

Honeyscore. (2024). Honeypot or not? Accessed 10 February 2024. Retrieved from https://honeyscore.shodan.io/

Huss, D. (2017, August 17). A blog. Turla APT actor refreshes KopiLuwak JavaScript backdoor for use in G20-themed attack. Accessed 10 February 2024. Retrieved from https://www.proofpoint.com/us/threat-insight/post/turla-apt-actor-refreshes-kopiluwak-javascript-backdoor-use-g20-themed-attack

IMB. (2021, March 8). Injection attacks. Accessed 3 February 2024. Retrieved from https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-injection-attacks

Juuti, P., Puusa, A. (2020). Laadullisen tutkimuksen näkökulmat ja menetelmät. E-book. Gaudeamus.

Katakri. (2020). Information Security Audit Tool for Authorities. Subdivision I: Information Assurance: I-10. NSA. Accessed 15 June 2023. Traficom publication series. ISBN 978-952-311-767-9. 29/2021. ISSN 2669-8757. Retrieved from https://um.fi/documents/35732/0/FINAL+-+Katakri-2020_201218_en.pdf/705d2bc6-6f1b-90dd-52e1-1ef97dae0623?t=1625140100978

Kemppainen, Simo. (2016). Tietoturvaloukkausten analysointi hunajapurkkijärjestelmän avulla. Accessed 15 June 2023. Retrieved from https://jyx.jyu.fi/bitstream/handle/123456789/50040/URN%3aNBN%3afi%3ajyu-201606022818.pdf?sequence=1&isAllowed=y

Kiraz, A. (2023, April 11). Threat Hunting for Windows Event Logs. Accessed 27 December 2023. Retrieved from https://alican-kiraz1.medium.com/threat-hunting-with-windows-event-logs-338255a0da4a

Kiviniemi, K. (2018). Ikkunoita tutkimusmetodeihin 2: Laadullinen tutkimus prosesseina. E-kirja. Gaudeamus.

Kyberturvallisuuskeskuksen viikkokatsaus – 52/2022. (2022, December 30). Accessed 15 June 2023. Retrieved from https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-522022

Falcone, R., Halfpop, T., Levene, B. (2017, May 3). Unit42. A Blog. Kazuar: Multiplatform Espionage Backdoor with API Access. Accessed 27 December 2024. Retrieved from https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Laari et al. (2019). #Kyberpuolustus. National defence university. Department of warfare. Series 3: working papers NO. 12. Accessed 16 June 2023. Retrieved from https://www.doria.fi/bitstream/handle/10024/173254/%23kyberpuolustus%20verkko%20%28interaktiivinen%20pdf%29%20%28002%29.pdf?sequence=1&isAllowed=y

Letema, C., Trevino, M. (2020, April 22). The 1/10/60 Minute Challenge, A Framework for Stopping Breaches Faster with WTG and CrowdStrike. Winslow Technology Group & CrowdStrike. Accessed 3 December 2023. Retrieved from https://www.youtube.com/watch?v=eUvvhTHvK2E&ab_channel=WinslowTechnologyGroup

Levy, E. (2023, April 24). The Beginner's Guide to Honeytokens (AKA Canary Tokens). Accessed 2 January 2024. Retrieved from https://www.securityengineering.dev/the-beginners-guide-to-honeytokens-aka-canary-tokens/

List of SOC service providers. (2022, September 24). Accessed 15 June 2023. Retrieved from https://csoc.fi/

Microsoft Security Intelligence. (2023, April 12). A summary. Accessed 10 February 2024. Retrieved from https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=VirTool:PowerShell/Empire.A&threatId=-2147188011

Mikä on kyberhyökkäys. (2023). Article. F-secure. Accessed 7 September 2023. Retrieved from https://www.f-secure.com/fi/articles/what-is-a-cyber-attack

Mitre. (n.d.). Accessed 10 December 2023. Retrieved from https://www.mitre.org/focus-areas/cybersecurity/mitre-attack

MITRE. (2020). MITRE ATT&CK matrix: Epic malware. Accessed 10 December 2023. Retrieved from https://attack.mitre.org/software/S0091/

MITRE. (2021). MITRE ATT&CK matrix: Carbon malware. Accessed 10 December 2023. Retrieved from https://attack.mitre.org/software/S0335/

MITRE. (2022). MITRE ATT&CK matrix. Accessed 10 December 2023. Retrieved from https://attack.mitre.org/software/S0587/

MITRE. (2023). MITRE ATT&CK matrix. Accessed 10 December 2023. Retrieved from https://attack.mitre.org/software/S0022/

MITRE ATT&CK. (2024). Enterprise techniques. Accessed 10 December 2023. Retrieved from https://attack.mitre.org/techniques/enterprise/

Mitre ATT&CK framework. (2023, September 20). Accessed 10 December 2023. Retrieved from https://www.crowdstrike.com/cybersecurity-101/mitre-attack-framework/

Mohit, K. (2017, August 30). An article. Accessed 5 January 2024. Retrieved from https://thehackernews.com/2017/08/gazer-backdoor-malware.html

Mulder, J. (2016, February 18). White paper. Mimikatz Overview, Defenses and Detection. Accessed 5 January 2024. Retrieved from https://sansorg.egnyte.com/dl/XMHRwR5lRO

Mutex objects. (2021, January 7). Documentation. Accessed 22 December 2023. Retrieved from https://learn.microsoft.com/en-us/windows/win32/sync/mutex-objects

Nazario, J. (2024). GitHub-repository. Awesome honeypots. Accessed 5 January 2024. Retrieved from https://github.com/paralax/awesome-honeypots

nbtscan. (2022, November 16). Kali-Linux tools. Accessed 5 January 2024. Retrieved from https://www.kali.org/tools/nbtscan/

nbstat. (2023, March 2). Article. Windows server. Accessed 5 January 2024. Retrieved from https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/nbtstat

NCDL. (n.d.). Cyber deception. National Cyber Deception Laboratory. Accessed 5 January 2024. Retrieved from https://www.cyberdeception.org.uk/cyber-deception/deceptive-thinking/

NCSC-FI. (2016). Lokien keräys ja käyttö – Ohje lokitietojen tallentamiseen ja hyödyntämiseen. Ohje 04-2026. Accessed 3 September 2023. Retrieved from https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitusohje.pdf

NCSC Common Cyber Attacks Infographic. (2016, January). White paper. Accessed 5 January 2024. Retrieved from https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact

Net Commands on Operating Systems. (2023, December 26). Article. Accessed 28 December 2023. Retrieved from https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/net-commands-on-operating-systems

Netstat. (2023, February 3). Article. Windows server. Accessed 28 December 2023. Retrieved from https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat

Niemi. J. (2022, May 4). Blogi. SIEM vs. SOAR, mitä eroa näillä on? Accessed 2 December 2023. Retrieved from https://sulava.com/tietoturva/siem-vs-soar-mita-eroa-nailla-on/

NIST 800-39. (2011, March). Managing Information Security Risk: Organization, Mission, and Information System View. Accessed 3 September 2023. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

OpenVAS. (2023). Bundesamt für Sicherheit in der Informationstechnik. Accessed 22 December 2023. Retrieved from https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Freie-Software/Tools/OpenVAS/OpenVAS.html

Parliament’s Defence Policy Guidelines. (2021). Valtioneuvostonjulkaisuja 2021:78. Retrieved from https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163405/VN_2021_78.pdf

Penbox. (2014). GitHub-repository. Accessed 28 December 2023. Retrieved from https://github.com/x3omdax/PenBox

Peter, E., Schiler, T. (2008, April 15). A project reports. A Practical Guide to Honeypots. Accessed 7 December 2023. Retrieved from https://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/index.html

Pols, P. (2023, February). The Unified Kill Chain. Raising resilience against advanced cyber attacks. Accessed 17 March 2024. Retrieved from https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

RFC 4949. (2007, August). Accessed 16 June 2023. Retrieved from https://www.ietf.org/rfc/rfc4949.txt

Reg commands. (2023, February 3). Article. Windows server. Accessed 28 December 2023. Retrieved from https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/reg

Reichel, D. (2021, February 19). A Blog. IronNetInjector: Turla's New Malware Loading Tool. Accessed 25 December 2023. Retrieved from https://unit42.paloaltonetworks.com/ironnetinjector/

Russia-Ukraine War Cyber-Event Map. (2022, July 8). Medium. Accessed 26 December 2023. Retrieved from https://cyberknow.medium.com/russia-ukraine-war-cyber-event-map-f538d23c9ce4

See attacks. Stop them. (2024). Accessed 10 February 2024. Retrieved from https://www.withsecure.com/gb-en/solutions/software-and-services/elements-endpoint-detection-and-response

Schneier, B. (2021, February 3). A blog. More SolarWinds News. Accessed 3 September 2023. Retrieved from https://www.schneier.com/blog/archives/2021/02/more-solarwinds-news.html

SolarWinds Orion Platformin takaovi mahdollisti vakoilun ja tietomurtoja. (2020, December 18). Accessed 3 September 2023. Retrieved from https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/solarwinds-orion-platformin-takaovi-mahdollisti-vakoilun-ja-tietomurtoja

Sotilastiedustelu. (2023). Julkinen katsaus. Accessed 23 December 2023. Retrieved from https://puolustusvoimat.fi/documents/1948673/73396483/Sotilastiedustelun+julkinen+katsaus+2023.pdf/

SUPO. (n.d.) APT is a toolbox for cyber spies. Accessed 10 December 2023. Retrieved from https://supo.fi/en/apt-operations

systeminfo. (2023, February 3). Article. Windows server. Accessed 3 January 2024. Retrieved from https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/systeminfo

Tavares, P. (2021, April 15). A Blog. Turla Crutch backdoor: analysis and recommendations. Accessed 7 January 2024. Retrieved from https://resources.infosecinstitute.com/topics/vulnerabilities/turla-crutch-backdoor-analysis-and-recommendations/

Teriö, Jarkko. (2011). Honeypot Systems: Advantages and Disadvantages. Accessed 15 June 2023. Retrieved from http://urn.fi/URN:NBN:fi:jyu-2011082211264

Tucker, P. (2020, November 20). Defence One. NATO Experiments with Deceptive Tactics to Lure Russian Hackers. Accessed 3 September 2023. Retrieved from https://www.defenseone.com/technology/2020/11/nato-experiments-deceptive-tactics-lure-russian-hackers/170248/

Tuohimetsä, J. (2010). Applying honeypots against bot networks and self-propagating malware in the Internet. Accessed 3 September 2023. Retrieved from http://urn.fi/URN:NBN:fi:aalto-2020122357856

Turla. (2023). Enterprise Evaluation 2023. Accessed 26 December 2023. Retrieved from https://attackevals.mitre-engenuity.org/enterprise/turla/

Unterbrink,H. (2021, September 21). A news. TinyTurla - Turla deploys new malware to keep a secret backdoor on victim machines. Accessed 26 December 2023. Retrieved from https://blog.talosintelligence.com/tinyturla/

What is a cyber attack. (n.d.) Security 101. Microsoft. Accessed 3 September 2023. Retrieved from https://www.microsoft.com/fi-fi/security/business/security-101/what-is-a-cyberattack

What Is Endpoint Detection and Response (EDR)? (2024). Accessed 10 February 2024. Retrieved from https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html#~edr-capabilities

What is a honeypot. (n.d.). Accessed 4 September 2023. Retrieved from imperva.com/learn/application-security/honeypot- heynet/

Zeltser, L. (2012, July 24). A blog. SANS. Looking at Mutex Objects for Malware Discovery & Indicators of Compromise. Accessed 26 December 2023. Retrieved from https://www.sans.org/blog/looking-at-mutex-objects-for-malware-discovery-indicators-of-compromise/

Zpedia. (2024). Accessed 5 January 2024. Retrieved from https://www.zscaler.com/zpedia/what-is-endpoint-detection-response-edr

Zucker, D. (2009, January). How to Do Case Study Research. Article. ResearchGate. Accessed 15 June 2023. Retrieved from https://www.researchgate.net/publication/39729804_How_to_Do_Case_Study_Research

Appendices

Appendix 1. The original dataset from the MITRE ATT&CK

Tactics	ID	Attack technique	ID	Sub-technique	SUM
TA0001: Initial Access	T1566	Phishing	T1566.001	Spearphishing Attachment	4 %
	T1078	Valid Accounts	T1078.001	Default Accounts	4 %
TA0002: Execution	T1059	Command and Scripting Interpreter	T1059.007	JavaScript	4 %
			T1059.001	PowerShell	15 %
			T1059.006	Python	4 %
			T1059.004	Unix Shell	7 %
			T1059.003	Windows Command Shell	26 %
	T1559	Inter-Process Communication			7 %
	T1106	Native API			26 %
	T1053	Scheduled Task/Job	T1053.003	Cron	4 %
			T1053.005	Scheduled Task	19 %
	T1569	System Services	T1569.002	Service Execution	15 %
	T1204	User Execution	T1204.002	Malicious File	4 %
	T1047	Windows Management Instrumentation			11 %
TA0003: Persistence	T1505	Server Software Component	T1505.002	Transport Agent	4 %
	T1205	Traffic Signaling	T1205.002	Socket Filters	7 %
	T1098	Account Manipulation			4 %
	T1547	Boot or Logon AutoStart Execution	T1547.001	Registry Run Keys / Startup Folder	15 %
			T1547.005	Security Support Provider	7 %
			T1547.009	Shortcut Modification	11 %

			T1547.004	Winlogon Helper DLL	4 %
	T1136	Create Account	T1136.002	Domain Account	11 %
			T1136.001	Local Account	7 %
	T1078	Valid account	T1078.001	Default Accounts	4 %
	T1543	Create or Modify System Process	T1543.003	Windows Service	19 %
				Accessibility Features	4 %
	T1546	Event Triggered Execution	T1546.015	Component Object Model Hijacking	7 %
			T1546.002	Screensaver	4 %
	T1053	Scheduled Task/Job	T1053.003	Cron	4 %
			T1053.005	Scheduled Task	19 %
	T1574	Hijack Execution Flow	T1574.001	DLL Search Order Hijacking	7 %
			T1574.004	Dylib Hijacking	4 %
			T1574.007	Path Interception by PATH Environment Variable	4 %
			T1574.008	Path Interception by Search Order Hijacking	4 %
			T1574.009	Path Interception by Unquoted Path	4 %
TA0004: Privilege Escalation	T1548	Abuse Elevation Control Mechanism	T1548.002	Bypass User Account Control	4 %
	T1134	Access Token Manipulation	T1134.002	Create Process with Token	4 %
			T1134.005	SID-History Injection	7 %
	T1098	Account Manipulation			4 %
	T1547	Boot or Logon AutoStart Execution	T1547.001	Registry Run Keys / Startup Folder	15 %
			T1547.004	Winlogon Helper DLL	4 %
			T1547.005	Security Support Provider	7 %
			T1547.009	Shortcut Modification	11 %

	T1543	Create or Modify System Process	T1543.003	Windows Service	19 %
	T1484	Domain Policy Modification	T1484.001	Group Policy Modification	4 %
	T1546	Event Triggered Execution	T1546.008	Accessibility Features	4 %
			T1546.015	Component Object Model Hijacking	7 %
			T1546.002	Screensaver	4 %
	T1574	Hijack Execution Flow	T1574.012	COR_PROFILER	
			T1574.001	DLL Search Order Hijacking	7 %
			T1574.004	Dylib Hijacking	4 %
			T1574.007	Path Interception by PATH Environment Variable	4 %
			T1574.008	Path Interception by Search Order Hijacking	4 %
			T1574.009	Path Interception by Unquoted Path	4 %
	T1055	Process Injection	T1055.001	Dynamic-link Library Injection	19 %
			T1055.011	Extra Window Memory Injection	4 %
			T1055.003	Thread Execution Hijacking	4 %
	T1053	Scheduled Task/Job	T1053.003	Cron	4 %
			T1053.005	Scheduled Task	22 %
	T1078	Valid Accounts	T1078.001	Default Accounts	4 %
TA0005: Defense Evasion	T1548	Abuse Elevation Control Mechanism	T1548.002	Bypass User Account Control	4 %
	T1134	Access Token Manipulation	T1134.002	Create Process with Token	4 %
			T1134.005	SID-History Injection	7 %

	T1140	Deobfuscate/Decode Files or Information			15 %
	T1484	Domain Policy Modification	T1484.001	Group Policy Modification	4 %
	T1222	File and Directory Permissions Modification	T1222.002	Linux and Mac File and Directory Permissions Modification	4 %
	T1564	Hide Artifacts	T1564.005	Hidden File System	7 %
			T1564.004	NTFS File Attributes	4 %
	T1574	Hijack Execution Flow	T1574.001	DLL Search Order Hijacking	7 %
			T1574.004	Dylib Hijacking	4 %
			T1574.007	Path Interception by PATH Environment Variable	4 %
			T1574.008	Path Interception by Search Order Hijacking	4 %
			T1574.009	Path Interception by Unquoted Path	4 %
	T1070	Indicator Removal	T1070.004	File Deletion	26 %
			T1070.005	Network Share Connection Removal	4 %
			T1070.006	Timestomp	11 %
	T1036	Masquerading	T1036.004	Masquerade Task or Service	19 %
			T1036.005	Match Legitimate Name or Location	11 %
	T1112	Modify Registry			22 %
	T1027	Obfuscated Files or Information			26 %
			T1027.002	Software Packing	4 %
			T1027.005	Indicator Removal from Tools	4 %
			T1027.009	Embedded Payloads	7 %
			T1027.010	Command Obfuscation	7 %

			T1027.011	Fileless Storage	15 %
	T1055	Process Injection			11 %
			T1055.001	Dynamic-link Library Injection	11 %
			T1055.011	Extra Window Memory Injection	4 %
			T1055.003	Thread Execution Hijacking	4 %
	T1620	Reflective Code Loading			4 %
	T1207	Rogue Domain Controller			4 %
	T1014	Rootkit			4 %
	T1553	Subvert Trust Controls			
			T1553.002	Code Signing	7 %
			T1553.004	Install Root Certificate	4 %
	T1218	System Binary Proxy Execution	T1218.011	Rundll32	4 %
	T1205	Traffic Signaling	T1205.002	Socket Filters	7 %
	T1127	Trusted Developer Utilities Proxy Execution	T1127.001	MSBuild	4 %
	T1550	Use Alternate Authentication Material	T1550.002	Pass the Hash	7 %
			T1550.003	Pass the Ticket	4 %
	T1078	Valid Accounts	T1078.001	Default Accounts	4 %
TA0006: Credential Access	T1557	Adversary-in-the-Middle	T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay	4 %
	T1555	Credentials from Password Stores	T1555.003	Credentials from Web Browsers	7 %
			T1555.004	Windows Credential Manager	4 %
	T1056	Input Capture	T1056.004	Credential API Hooking	4 %
			T1056.001	Keylogging	4 %
	T1040	Network Sniffing			11 %
	T1003	OS Credential Dumping	T1003.006	DCSync	4 %

			T1003.004	LSA Secrets	4 %
			T1003.001	LSASS Memory	7 %
			T1003.002	Security Account Manager	4 %
	T1649	Steal or Forge Authentication Certificates			4 %
	T1558	Steal or Forge Kerberos Tickets	T1558.001	Golden Ticket	7 %
			T1558.003	Kerberoasting	4 %
			T1558.002	Silver Ticket	7 %
	T1552	Unsecured Credentials	T1552.001	Credentials In Files	4 %
			T1552.002	Credentials in Registry	4 %
			T1552.004	Private Keys	7 %
TA0007: Discovery	T1087	Account Discovery	T1087.002	Domain Account	7 %
			T1087.001	Local Account	15 %
	T1010	Application Window Discovery			4 %
	T1083	File and Directory Discovery			15 %
	T1046	Network Service Discovery			4 %
	T1135	Network Share Discovery			11 %
	T1040	Network Sniffing			11 %
	T1201	Password Policy Discovery			4 %
	T1120	Peripheral Device Discovery			4 %
	T1069	Permission Groups Discovery			4 %
			T1069.002	Domain Groups	4 %
			T1069.001	Local Groups	11 %
	T1057	Process Discovery			37 %
	T1012	Query Registry			22 %
	T1018	Remote System Discovery			19 %

	T1518	Software Discovery			4 %
			T1518.001	Security Software Discovery	15 %
	T1082	System Information Discovery			30 %
	T1016	System Network Configuration Discovery			41 %
	T1049	System Network Connections Discovery			26 %
	T1033	System Owner/User Discovery			26 %
	T1007	System Service Discovery			11 %
	T1124	System Time Discovery			15 %
TA0008: Lateral Movement	T1210	Exploitation of Remote Services			4 %
	T1570	Lateral Tool Transfer			4 %
	T1021	Remote Services	T1021.003	Distributed Component Object Model	4 %
			T1021.002	SMB/Windows Admin Shares	7 %
			T1021.004	SSH	4 %
	T1550	Use Alternate Authentication Material	T1550.002	Pass the Hash	7 %
			T1550.003	Pass the Ticket	4 %
TA0009: Collection	T1557	Adversary-in-the-Middle	T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay	4 %
	T1560	Archive Collected Data			4 %
			T1560.002	Archive via Library	4 %
			T1560.001	Archive via Utility	7 %
	T1119	Automated Collection			11 %
	T1115	Clipboard Data			4 %
	T1005	Data from Local System			22 %
	T1025	Data from Removable Media			4 %

	T1074	Data Staged	T1074.001	Local Data Staging	19 %
			T1114.001	Local Email Collection	4 %
			T1114.002	Remote Email Collection	4 %
	T1056	Input Capture	T1056.004	Credential API Hooking	4 %
			T1056.001	Keylogging	4 %
	T1113	Screen Capture			7 %
	T1125	Video Capture			11 %
TA0011: Command and Control	T1071	Application Layer Protocol	T1071.004	DNS	4 %
			T1071.002	File Transfer Protocols	4 %
			T1071.003	Mail Protocols	11 %
			T1071.001	Web Protocols	37 %
	T1132	Data Encoding	T1132.002	Non-Standard Encoding	4 %
			T1132.001	Standard Encoding	4 %
	T1001	Data Obfuscation	T1001.001	Junk Data	4 %
			T1001.003	Protocol Impersonation	4 %
			T1001.002	Steganography	4 %
	T1573	Encrypted Channel	T1573.002	Asymmetric Cryptography	26 %
			T1573.001	Symmetric Cryptography	19 %
	T1008	Fallback Channels			15 %
	T1105	Ingress Tool Transfer			26 %
	T1104	Multi-Stage Channels			4 %
	T1095	Non-Application Layer Protocol			11 %
	T1572	Protocol Tunneling			4 %
	T1090	Proxy	T1090.001	Internal Proxy	4 %
			T1090.003	Multi-hop Proxy	4 %
	T1205	Traffic Signaling	T1205.002	Socket Filters	7 %
	T1102	Web Service			4 %
			T1102.002	Bidirectional Communication	15 %

TA0010: Exfiltration	T1020	Automated Exfiltration			11 %
	T1048	Exfiltration Over Alternative Protocol	T1048.003	Exfiltration Over Unencrypted Non-C2 Protocol	4 %
	T1041	Exfiltration Over C2 Channel			19 %
	T1567	Exfiltration Over Web Service	T1567.002	Exfiltration to Cloud Storage	7 %
			T1567.001	Exfiltration to Code Repository	4 %
	T1029	Scheduled Transfer			15 %
	T1565	Data Manipulation	T1565.002	Transmitted Data Manipulation	4 %

Appendix 2. The most used Turla techniques and detection method

Tactics	ID	Attack technique	Detection ID	Detection data source	Detection data component
TA0001: Initial Access	T1566	Phishing	DS0028	Logon Session	Logon Session Creation
	T1078	Valid Accounts	DS0002	User Account	User Account Authentication
TA0002: Execution	T1059	Command and Scripting Interpreter	DS0017	Command	Command Execution
			DS0011	Module	Module Load
			DS0009	Process	Process Creation
			DS0012	Script	Process Metadata
					Script Execution
TA0003: Persistence	T1547	Boot or Logon AutoStart Execution	DS0017	Command	Command Execution
			DS0027	Driver	Driver Load
			DS0022	File	File Creation
					File Modification
			DS0008	Kernel	Kernel Module Load
			DS0011	Module	Module Load
			DS0009	Process	OS API Execution
					Process Creation
			DS0024	Windows Registry	Windows Registry Key Creation
					Windows Registry Key Modification
TA0004: Privilege Escalation	T1543	Create or Modify System Process	DS0017	Command	Command Execution
			DS0027	Driver	Driver Load

			DS0022	File	File Creation
					File Modification
			DS0009	Process	OS API Execution
					Process Creation
			DS0019	Service	Service Creation
					Service Modification
			DS0024	Windows Registry	Windows Registry Key Creation
					Windows Registry Key Modification
	T1547	Boot or Logon AutoStart Execution	DS0017	Command	Command Execution
			DS0027	Driver	Driver Load
			DS0022	File	File Creation
					File Modification
			DS0008	Kernel	Kernel Module Load
			DS0011	Module	Module Load
			DS0009	Process	OS API Execution
					Process Creation
			DS0024	Windows Registry	Windows Registry Key Creation
					Windows Registry Key Modification
TA0005: Defense Evasion	T1027	Obfuscated Files or Information	DS0005	WMI	WMI Creation
			DS0009	Process	OS API Execution
					Process Creation
			DS0011	Module	Module Load
			DS0012	Script	Script Execution
			DS0017	Command	Command Execution
			DS0022	File	File Creation
					File Metadata

			DS0024	Windows Registry	Windows Registry Key Creation
TA0006: Credential Access	T1003	OS Credential Dumping	DS0026	Active Directory	Active Directory Object Access
			DS0017	Command	Command Execution
			DS0022	File	File Access
			DS0029	Network Traffic	Network Traffic Content
					Network Traffic Flow
			DS0009	Process	OS API Execution
					Process Access
					Process Creation
			DS0024	Windows Registry	Windows Registry Key Access
	T1558	Steal or Forge Kerberos Tickets	DS0026	Active Directory	Active Directory Credential Request
			DS0017	Command	Command Execution
			DS0022	File	File Access
			DS0028	Logon Session	Logon Session Metadata
TA0007: Discovery	T1016	System Network Configuration Discovery	DS0017	Command	Command Execution
			DS0009	Process	OS API Execution
	T1057	Process Discovery	DS0017	Command	Command Execution
			DS0009	Process	OS API Execution
	T1082	System Information Discovery	DS0017	Command	Command Execution
			DS0009	Process	OS API Execution
					Process Creation

TA0008: Lateral Movement	T1021	Remote Services	DS0017	Command	Command Execution
			DS0028	Logon Session	Logon Session Creation
			DS0011	Module	Module Load
			DS0033	Network Share	Network Share Access
			DS0029	Network Traffic	Network Connection Creation
					Network Traffic Flow
			DS0009	Process	Process Creation
			DS0005	WMI	WMI Creation
	T1550	Use Alternate Authentication Material	DS0026	Active Directory	Active Directory Credential Request
			DS0015	Application Log	Application Log Content
			DS0028	Logon Session	Logon Session Creation
			DS0002	User Account	User Account Authentication
			DS0006	Web Credential	Web Credential Usage
TA0009: Collection	T1005	Data from Local System	DS0017	Command	Command Execution
			DS0022	File	File Access
			DS0009	Process	OS API Execution
			DS0012	Script	Process Creation
					Script Execution
	T1074	Data Staged	DS0017	Command	Command Execution
			DS0022	File	File Access
					File Creation

			DS0024	Windows Registry	Windows Registry Key Modification
TA0011: Command and Control	T1071	Application Layer Protocol	DS0029	Network Traffic	Network Traffic Content
					Network Traffic Flow
	T1105	Ingress Tool Transfer	DS0017	Command	Command Execution
			DS0022	File	File Creation
			DS0029	Network Traffic	Network Connection Creation
					Network Traffic Content
					Network Traffic Flow
	T1573	Encrypted Channel	DS0029	Network Traffic	Network Traffic Content
TA0010: Exfiltration	T1041	Exfiltration Over C2 Channel	DS0017	Command	Command Execution
			DS0022	File	File Access
			DS0029	Network Traffic	Network Connection Creation
					Network Traffic Content
					Network Traffic Flow
	T1029	Scheduled Transfer	DS0029	Network Traffic	Network Connection Creation
					Network Traffic Flow

Appendix 3. AA23-129A (2023), Snake malware attack techniques

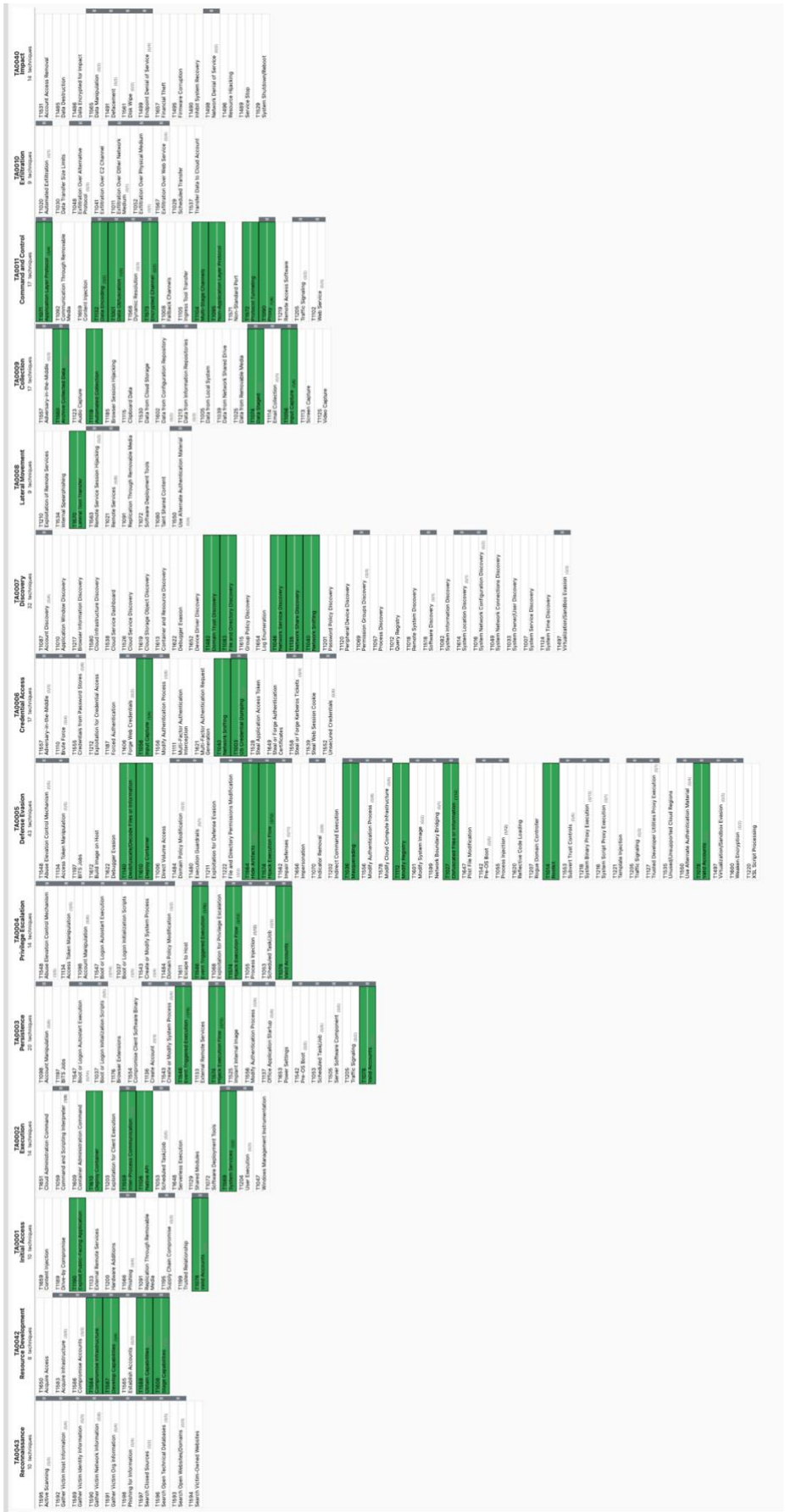
ID	Technique Title	Use
T0840	Network Connection Enumeration	Adversaries may perform network connection enumeration to discover information about device communication patterns.
T1001	Data Obfuscation	Adversaries may obfuscate command and control traffic to make it more difficult to detect.
T1001.003	Protocol Impersonation	Adversaries may impersonate legitimate protocols or web service traffic to disguise command and control activity and thwart analysis efforts.
T1003	OS Credential Dumping	Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software.
T1014	Rootkit	Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components.
T1027	Obfuscated Files or Information	Adversaries may attempt to make an executable or file difficult to discover or analyse by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.
T1027.002	Software Packing	Adversaries may perform software packing or virtual machine software protection to conceal their code.
T1036	Masquerading	Adversaries may attempt to manipulate features of their artefacts to make them appear legitimate or benign to users and/or security tools.
T1040	Network Sniffing	Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network.
T1046	Network Service Discovery	Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation.
T1055.001	Dynamic-link Library Injection	Adversaries may inject dynamic-link libraries (DLLs) into processes to evade process-based defences as well as possibly elevate privileges.

T1056.001	Keylogging	Adversaries may log user keystrokes to intercept credentials as the user types them.
T1059.001	PowerShell	Adversaries may abuse PowerShell commands and scripts for execution.
T1071	Application Layer Protocol	Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic.
T1071.001	Web Protocols	Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic.
T1071.003	Mail Protocols	Adversaries may communicate using application layer protocols associated with electronic mail delivery to avoid detection/network filtering by blending in with existing traffic.
T1071.004	DNS	Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic.
T1074	Data Staged	Adversaries may stage collected data in a central location or directory prior to Exfiltration.
T1078	Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Défense Evasion.
T1083	File and Directory Discovery	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.
T1090.003	Multi-hop Proxy	To disguise the source of malicious traffic, adversaries may chain together multiple proxies.
T1095	Non-Application Layer Protocol	Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network.
T1104	Multi-Stage Channels	Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions.
T1106	Native API	Adversaries may interact with the native OS application programming interface (API) to execute behaviours.

T1112	Modify Registry	Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.
T1119	Automated Collection	Once established within a system or network, an adversary may use automated techniques for collecting internal data.
T1132	Data Encoding	Adversaries may encode data to make the content of command-and-control traffic more difficult to detect.
T1132.002	Non-Standard Encoding	Adversaries may encode data with a non-standard data encoding system to make the content of command-and-control traffic more difficult to detect.
T1135	Network Share Discovery	Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement.
T1140	Deobfuscate/Decode Files or Information	Adversaries may use Obfuscated Files or Information to hide artefacts of an intrusion from analysis.
T1190	Exploit Public-Facing Application	Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network.
T1482	Domain Trust Discovery	Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments.
T1546.016	Installer Packages	Adversaries may establish persistence and elevate privileges by using an installer to trigger the execution of malicious content.
T1547.006	Dynamic Linker Hijacking	Adversaries may execute their own malicious payloads by hijacking environment variables the dynamic linker uses to load shared libraries.
T1559	Inter-Process Communication	Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution.
T1560.003	Archive Collected Data	An adversary may compress and/or encrypt data that is collected prior to exfiltration.
T1564	Hide Artefacts	Adversaries may attempt to hide artefacts associated with their behaviours to evade detection.

T1569.002	Service Execution	Adversaries may abuse the Windows service control manager to execute malicious commands or payloads.
T1570	Lateral Tool Transfer	Adversaries may transfer tools or other files between systems in a compromised environment.
T1572	Protocol Tunneling	Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems.
T1573	Encrypted Channel	Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.
T1573.001	Symmetric Cryptography	Adversaries may employ a known symmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.
T1573.002	Asymmetric Cryptography	Adversaries may employ a known asymmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.
T1574.002	DLL Side-Loading	Adversaries may execute their own malicious payloads by side-loading DLLs.
T1584	Compromise Infrastructure	Adversaries may compromise third-party infrastructure that can be used during targeting.
T1587.001	Malware	Adversaries may develop malware and malware components that can be used during targeting.
T1588	Obtain Capabilities	Adversaries may buy and/or steal capabilities that can be used during targeting.
T1608	Stage Capabilities	Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting.
T1610	Deploy Container	Adversaries may deploy a container into an environment to facilitate execution or evade defences.

Appendix 4. Snake malware attack techniques (AA23-129A, 2023) presented with MITRE ATT&CK Navigator -tool



Appendix 5. Example of the heatmap with MITRE ATT&CK Navigator -tool