Complexity of Contemporary Indicators of Compromise

Raymond Andre Hagen and Kirsi Helkala
Norwegian University of Science and Technology, Norway
Norwegian Defence College, Norway
raymohag@stud.ntnu.no
Khelkala@mil.no

Abstract. The cybersecurity landscape has undergone substantial transformation, especially in the sphere of Advanced Persistent Threats (APT). These evolving threats, marked by increased sophistication, scale, and impact, require the critical revaluation of traditional security models and the development of more advanced defensive strategies. This study offers a comprehensive analysis of the progress in APT attack methodologies over the past 30 years, focused on the evolving nature of compromise (IoCs) and their role in shaping future predictive and defensive mechanisms. Using a rigorous methodological approach, this survey systematically reviewed 21 significant APT incidents that span three decades. This includes integrating data from various sources such as academic journals, specialised cybersecurity blogs, and media reports. Using comparative and analytical methods, this study dissects each incident to provide an intricate understanding of the APT landscape and the evolution of IoCs. Our findings indicate a notable change in thinking from isolated hacker activities to organised state-sponsored APT operations driven by complex motives such as political espionage, economic disruption, and national security interests. Advancements in APTs are characterised by sophisticated persistence mechanisms, innovative attack vectors, advanced lateral movement within networks, and more covert data exfiltration and evasion methods. This study emphasises the difficulties in detecting advanced persistent threat (APT) activities due to their sophisticated and secretive nature. This stresses the importance of thoroughly investigating the evidence of such activities and highlights the need for a dynamic and initiative-cybersecurity approach. This study also highlights the crucial role of integrating IoC understanding into AI-driven predictive models and frameworks to predict potential APT. This integration is essential for the development of pre-emptive defence strategies. This study provides valuable information on the evolving dynamics of cyber threats and emphasises the urgent need for forward-thinking adaptive cybersecurity strategies. It offers a framework for understanding the complexities of modern APTs and guides the development of more effective AI-enhanced defence mechanisms against emerging cyber threats.

Keywords: State Actors, APT, IoC, Threats

1. Introduction

Cybersecurity has changed significantly in the past three decades, as malicious actors have refined their strategies and tactics. This evolution has ushered in an era where threats are not only more sophisticated but also highly targeted, leveraging a mix of technological prowess and strategic planning to breach defense. Advanced Persistent Threats (APTs) are among the most formidable. APTs are specialized cyber operation collectives that are primarily associated with nation-state entities or, in some instances, organized crime groups. These entities are characterized by their high level of sophistication, significant resources, and persistent focus on specific targets. Their operations are typically aimed at espionage, data theft, or disruption, leveraging a wide array of tactics, techniques, and procedures (TTPs) over prolonged periods to achieve their objectives.

The identification and analysis of IoCs is an integral aspect of understanding and mitigating the risks posed by APTs involves the identification and analysis of Indicators of Compromise (IoCs). IoCs are observable artefacts or behaviors in a network or system that, alone or aggregated with other IoCs, can suggest a successful cyberattack. These indicators can range from simple indicators, such as known malicious IP addresses or domain names, to more complex patterns of behavior that suggest unauthorized access or data exfiltration. Recognizing IoCs is pivotal for the early detection of cybersecurity breaches, enabling timely response and mitigation actions to limit damage and prevent future attacks.

This study aims to improve and optimize defensive cyber strategies by examining cyber incidents, particularly their IoCs. By dissecting and understanding the nature of APTs and IoCs that characterize their attacks, cybersecurity professionals can enhance their defensive measures. This entails not only deploying technical solutions but also adopting a more strategic approach to defense, considering the sophisticated nature of APT actors and their campaigns. A thorough understanding of APTs and their IoCs is crucial for fortifying the defense against ever-evolving cyber threats. Through detailed analysis and strategic implementation of defense mechanisms, it is possible to build resilience against these advanced adversaries and protect critical information and infrastructure from compromises.

2. Methodology

This chapter describes our systematic research methodology for investigating the development of APTs over the past 30 years. Our approach guarantees transparency and thoroughness, thereby ensuring the empirical validity of the APT observations.

2.1 Evolving Indicators of Advanced Persistent Threats in Cybersecurity

The survey focused on understanding advanced persistent threats (APTs) within the ever-evolving realm of cybersecurity. This addresses the following critical question.

"Dynamic Indicators of APT Incursions: What are the predominant indicators of an APT attack, and how have these indicators evolved to adapt to the changing cybersecurity environment?"

2.2 Research Design

We use a strategic framework to examine the intricate nature of advanced persistent threats (APTs) during a designated period. Therefore, we applied a combination of comparative and analytical methods.

Selection Criteria We conducted a thorough parameter selection process to identify a wide range of standard parameters. We then reviewed each and removed any redundant or challenging information that could be obtained, with the Norwegian Cybersecurity Centre (NCSC) providing valuable input to help us make our final decision. We selected 21 APT attacks that spanned more than three decades, with diversity and importance as the main criteria. Furthermore, we analysed each incident against twenty carefully selected parameters to create a complete dataset. This allowed us to take a multifaceted look at the APT dynamics.

2.3 Data Collection, Database Selection, and Search Strategy

We sourced our primary data from Oria, a renowned academic database. We adopted a strategic approach, using search terms such as 'Moonlight Maze', 'APT', 'hacking', 'cyberattacks', and ’attribution of APT.’ Information search was conducted using traditional search engines and new AI tools, as specified in the references.

2.4 Inclusion of Non-Traditional Sources

Recognising the rapid evolution of cyberattacks, we have expanded our research beyond traditional academic sources. This included insights from YouTube channels, such as True Spies, Kaspersky, Darknet Diaries, authoritative security blogs, and prompt press releases. Although these sources may deviate from academic norms, their relevance in supplying the current cyber-threat perspectives is crucial. We carefully reviewed each for credibility, ensuring that they complemented our research with practical insight. This approach bridges the gap between academic research and the dynamic cyber landscape, offering a comprehensive understanding of the cyberattack ecosystem. Readers are encouraged to consider these diverse sources holistically from a well-rounded perspective.

2.5 Data Analysis

Comparative analysis. We use comparative analysis as a methodological approach to qualitative research. The goal is to name patterns, similarities, and variances between events and cases. Furthermore, our aim was to figure out the broader patterns and their unique deviations.

Procedure:

Data Categorisation: Data were sorted according to year, type of attack, affected entities, and methods.

Event-by-Event Comparison: Each event was contrasted with others to find similarities and differences.

Thematic Extraction: Emerging themes were documented during these events.

2.6 Analytical Approach

The data were subjected to more in-depth comparative analysis. This stage distils the findings to reveal the changing sides of the APTs throughout the study period. This study aimed to uncover information on the evolution and transformation of APTs.

2.7 Limitations and Mitigation

Although every methodological approach has intrinsic limitations, conscious steps were taken to minimise their potential impact on our research.

Subjectivity: Different researchers interpret the same dataset differently. However, by defining our research question and selecting the parameters, we proved a structured framework that reduced the scope of various interpretations. Furthermore, cross-verification of findings from multiple researchers can further dilute individual biases.

2.8 Overemphasis on Commonalities

Although focusing on standard parameters might lead to overlooking outliers or unique events, these were conscious decisions to ensure a consistent data comparison. However, we know of the potential loss of insight from individual cases. To address this, our analytical approach was designed to be vigilant for significant deviations or outliers with different implications.

To keep the credibility of our research, we used a standardised survey that systematically collected identical data points across the board. This method speeded up the data collection process and significantly minimised the likelihood of introducing inconsistencies or errors in our analysis. Our overarching goal was to support the precision and authenticity of our findings and to accurately reflect the genuine dynamics of APT.

2.9 Ethical Considerations

Finding who is behind cyber threats, particularly those linked to the government, is challenging. We conducted our research cautiously to recognise advanced persistent threat actors and have been transparent about our sources, while considering their limitations. We focus intensely on being explicit to ensure the correctness of our findings.

2.10 Limitations of the Survey

Our research was based on 21 well-known attacks in the cybersecurity community. Although these cases supply valuable information, other APT activities that can reveal various aspects of APT capabilities have not yet been investigated. A more extensive or added set of attacks can lead to varying conclusions, emphasising the need for continuous and diverse studies in this field.

3. Comparative Analysis of APT Attacks Over Two Decades

We comprehensively examined twenty-one major APT attacks over the past two decades.

Table 1: Table 1 of the 8 of the comparative analysis

No.	Incident	Year	References
1	The Cuckoo's Egg	1988	Stoll, C (2000); Stoll, C (1988)
2	Operation Aurora	2009	McAfee (2009); Rosenberg, J (2017)
3	Stuxnet	2009	Ilmoi, S. (2019); Cole, E. (2016)
4	Stuxnet computer worm	2005-2007	Shakarian, P, Shakarian, J, and Ruef, A. (2013); Langner, R. (2012); Bencsáth, B., Pék, G., Buttyán, L., and Félegyházi, M. (2012); Hajek, K., Milenkoski, P.H., and Sinclair, C. (2020); Revivo, B. (Unknown); Shakarian, P., Shakarian, J., and Ruef, A. (2013)
5	Flame	2012	What is Flame and How Does It Work? (2024); Bencsáth, B., Pék, G., Buttyán, L., and Félegyházi, M. (2012)
6	Red October	2008	Red October Cyber Attack, 8 Minute Profile' (2024); Barakos, A. (2018); Iranian, E. and Stockpol, A.B. (2022)
7	Deep Panda	2011	Chinastrike (2018); Cole, E. (2016)
8	World Anti-Doping Agency Attack	2016	News, V. (2016); Revivo, B. (Unknown)
9	Ukraine's artillery app	2016	Schwartz, M.J. (2016)
10	WannaCry attack	2017	'WannaCry: The World's Largest Ransomware Attack' (2023); Akbanov, M., Vassilakis, V.G., and Logothetis, M.D. (2019); et al, T. (2020); Andrex, D. (2017)
11	Bureau 121 - Sony Pictures Attack	2014	FireEye (2016); Holm, L. (2017); Resnick, F.Y. (2017)
12	SolarWinds supply chain attack	2020	'The SolarWinds Hack: The Largest Cyber Espionage Attack in the United States' (2021); Lazarovitz, L. (2023); Oladimeji, S. and Kerner, S.M. (2024)
13	Anonymous attack on Russia state television	2022	Portilla, J. (2022)
14	Mirai	2016	'A Study on the Mirai Attack' (2017); Zhang, X., Upton, O., Beebe, N.L., and Choo, K.K.R. (2020); Zou, Q., Sun, X., Liu, P., and Singhal, A. (2020)
15	Yahoo data breach	2016	'Data Breaches: Deloitte Suffers Serious Hit While More Details Emerge About Equifax and Yahoo' (2017); Krause, R. (2017)
16	Defacement of Le Monde	2017	'Defacement of Le Monde - Anatomy of an Attack' (2022); Reuters.com (2017)
17	Saudi Aramco Hacking	2012	Brooks, C. and Thiel-Rogers, E. (2016); Pagliery, J. (2015)
18	Deep Panda of Ukraine President Zelenskii	2022	Miller, J.R. (2022); Buchanan, B. (2020)
19	Equifax data breach	2017	'Data Breaches: Deloitte Suffers Serious Hit While More Details Emerge About Equifax and Yahoo' (2017); Pitz, G.H. (2017)
20	Moonlight Maze	1998	Ansari, J.R., Chari, V., Heren, M., Refiq, O., and Simon, D. (1998)
21	NotPetya	2017	Paj, S.Y.A. (2018); Zou, Q., Sun, X., Liu, P., and Singhal, A. (2020)

Table 1b: Table 1b of the 8 of the comparative analysis

No.	Incident	Year	References
16	Defacement of Le Monde	2017	'Defacement of Le Monde - Anatomy of an Attack' (2022); Reuters.com (2017)
17	Saudi Aramco Hacking	2012	Bronk, C. and Tikk-Ringas, E. (2013); Pagliery, J. (2015)
18	Deep Fake of Ukraine President Zelenskii	2022	Miller, J.R. (2022); Buchanan, B. (2020)
19	Equifax data breach	2017	'Data Breaches: Deloitte Suffers Serious Hit While More Details Emerge About Equifax and Yahoo' (2017); Pike, G.H. (2017)
20	Moonlight Maze	1996	Ansart, J.P., Charl, V., Neyer, M., Rafiq, O., and Simon, D. (1983)
21	NotPetya	2017	Fayi, S.Y.A. (2018); Zou, Q., Sun, X., Liu, P., and Singhal, A. (2020)

Table 2: Table 2 of 8 of the comparative analysis

No.	Aspect	Description
1	Confidentiality	German hacking group that broke into American universities, government, and military computer systems.
2	Confidentiality	A series of attacks on around 30 large companies.
3	Confidentiality	Malware that uses different methods to steal credentials.
4	Availability	Worm used to stop Iran's nuclear program.
5	Availability and Confidentiality	A highly sophisticated tool that allows for customization-based tools in relation to the attacker's needs.
6	Confidentiality	Espionage programmed.
7	Confidentiality	Espionage programmed.
8	Confidentiality	APT hacked into WADA and accessed information about WADA athletes that leaked to the media.
9	Availability	Russian APT managed to change a target calculating app for howitzers that allowed GPS coordinates to be sent to Russia, Ukraine lost 60% of howitzers in one day.
10	Availability	Using zero-day exploits, the ransomware spread around the world in 18 hours.
11	Availability	Due to the Hollywood movie "The Interview," where the North Korean leader was depicted in a nonflattering way, DPRK launched a cyberattack on Sony Pictures.
12	Confidentiality and Integrity	Supply chain attack where the popular SolarWinds Orion Software update server was compromised, giving the attackers access to more than 18,000 systems.
13	Integrity	Hacktivism group 'Anonymous' got access to Russian state television and sent a pro-Ukraine video.
14	Availability	A massive botnet took advantage of insecure IoT devices.
15	Confidentiality	The largest data breach in history up to that point.
16	Integrity	Attack that killed several French media outlets.
17	Integrity	35,000 computers from the world's largest oil company were wiped out.
18	Integrity	A deep fake trying to claim Zelenskiy wanted Ukraine to surrender.
19	Confidentiality	The credit bureau was breached.
20	Confidentiality	Different US government agencies, defence contractors, and research institutions were compromised.
21	Confidentiality and Availability	NonPetya was a destructive malware attack on 27 June 2017. Although disguised as a ransomware attack similar to the notorious Petya ransomware, it was identified as a more damaging wiper attack designed to cause destruction.

Table 3: Table 3 of 8 of the comparative analysis

Nr	Duration	Aggressor	Who did Attribution?
1	3 years	(Group of countries / APT) KGB by proxy of a West-German hacker group	The parties involved in the case
2	2 years	China	Google
3	3 years	Russia	USA
4	5 years	USA	Several public and private IT-security companies
5	1994-2012	USA / Israel / China	The Washington Post
6	2008 - 2012	China	Russia / England
7	2008-dd	China	CrowdStrike
8	2016	Russia	FireEye / Mandiant
9	2016	Russia	Armed forces of Ukraine
10	2 days	North Korea	USA
11	1 month	North Korea	USA
12	6 months	Russia	USA
13	2 hours	Anonymous hacking collective	Russia
14	Constantly adjusted; ongoing in some form	USA	USA
15	22.09.2016	Russia	USA
16	2017	Russia	France
17	6 months	The group "Cutting sword of justice"	Saudi Arabia
18	1 day	Russia	Ukraine
19	3 months	China	USA
20	3 years	Russia	USA
21	From a few hours up to six months	Russia	ESET, Kaspersky, and Microsoft

Table 4: Table 4 of 8 of the comparative analysis

Nr	Country that was attacked	Time to Mitigate Attack	Method Used
1	USA	3.5 years	Credential stealing
2	USA	1.5 years until Microsoft had a patch ready	Exploiting operating systems vulnerability
3	USA, Canada, UK, India, Mexico	Six months	Credential stealing
4	Primary objective Iran, but the worm spread worldwide	2 years	Custom malware to attack Siemens SCADA systems
5	Different Countries in the World, Middle East and Africa	Shortly after attack	Modular-based malware
6	Global attack	2012	Error in the MS Office file format
7	American companies, most famous Adobe Breach	2 years	Custom malware
8	Canada	1 month	Custom malware
9	Ukraine	Instantly	Custom malware
10	500,000 companies around the world	18 hours	Custom malware
11	Japan	2 days	Custom malware
12	Global attack	Ongoing	Custom supply chain attack malware
13	Russia	2 hours	Intrusion of broadcast system
14	Global attack	Estimate 1 day for each attack	Password hacking, HTTP flooding, wipers and other malware from infected IoT devices
15	USA	4 months	Hackers got access to Yahoo's main site user database
16	France	6 months	Phishing emails
17	Saudi Arabia	6 months	Phishing emails
18	Ukraine	1 day	Deep fake video (AI GAN method)
19	USA, UK, and Canada	76 days	Exploiting nonpatched systems
20	USA	3 years	Social Engineering and Exploitation vulnerabilities
21	Ukraine initially and then globally	Short-lived due to destructive operation	Wiper malware hidden as ransomware

Table 5: Table 5 of the 8 of the comparative analysis

Nr	Complexity Assessment	Attack Surface	Targeted or Random (Opportunistic)
1	Low	Software vulnerability	Targeted
2	High	Operating system	Targeted
3	Medium	Internet Browsers	Targeted
4	High	PLC controllers of Siemens SCADA systems	Targeted
5	High	Rootkits	Targeted
6	High	Exploits	Random
7	High	Exploits	Targeted
8	High	Exploits	Targeted
9	Medium	Exploits	Targeted
10	High	Exploits	Random
11	High	Destructive malware	Targeted
12	High	Update server	Targeted
13	Medium	Exploits	Targeted
14	Medium	IoT devices	Random
15	Medium	Exploits	Targeted
16	Low	Exploits	Targeted
17	Low	Exploits	Targeted
18	High	Video and social networks	Targeted
19	High	Apache Struts framework	Targeted
20	High	Exploits and social manipulation	Targeted
21	High	Malware	Targeted

Table 6: Table 6 of 8 of the comparative analysis

Nr	Motivation	Consequence	Specially Adapted Malware
1	Bragging rights	KGB got access to some US systems, but very little data was stolen.	Yes
2	Political	Several high-value targets got exposed and lost data	Yes
3	Economic gain	Further development of the malware used in this attack	Yes
4	Political	Managed to negotiate the Iran nuclear treaty	Yes
5	Political	Espionage	Yes
6	Research and development	Espionage	Yes
7	Political	Espionage	Yes
8	Political / Show of force	Hacktivism	Yes
9	Political / War	State actor	Yes
10	Economic gain	Many billions to restore and fix the attack, many Eastern European companies went down	Yes
11	Political	Show of force	Yes
12	Persistent access and stealing of data	18,000 companies were infected	Yes
13	Hacktivism	Tried to create civil unrest due to the Russian war in Ukraine	Yes
14	Hacktivism	Have been used in state actors to try and stop root DNS servers, tough attack to negotiate	Yes
15	Economic gain	The market value of Yahoo was severely reduced	Yes
16	Hacktivism	Le Monde had to rebuild their entire IT system infrastructure, no cost has been publicly disclosed	Yes
17	Hacktivism	Cost of rebuilding and protecting the infrastructure	Yes
18	Political / War	None	Yes
19	Economic gain / Political	Lost a lot of sensitive data	Yes
20	Political	Loss of sensitive information and showed vulnerabilities in national infrastructure	Yes
21	Political	Parties were hit. The initial spread was in Ukraine, affecting much of the Ukrainian infrastructure	Yes

Table 7: Table 7 of 8 of the comparative analysis

Nr	Total Number of Users Affected?	Social Engineering Used?	How Was the Attack Discovered?
1	Estimate of 15 companies attacked by the group	No	A billing error in the accounting system
2	More than 20 companies	No	McAfee discovered zero days
3	Unknown	No	Security Companies
4	200,000 companies worldwide	Yes	A company was hired to do an audit and found the malware
5	1,000 computers	No	Kaspersky Labs, Iranian National CERT and CrySYS investigated Iranian systems on behalf of the UN
6	Around 300 systems had the trojan	No	Cybersecurity files
7	Unknown	No	Security Companies
8	Unknown	No	Observed data were extracted from WADA servers
9	Unknown	No	70% of the Ukrainian howitzers were destroyed in one day
10	500,000 at least	Unknown	Security companies
11	Unknown	No	Leaked documents
12	Unknown	No	Mandiant (FireEye) investigated their breach and found a modified DLL that was used
13	Unknown	No	N/A
14	Unknown	No	Instantly
15	Between 500 million and 3 billion user accounts	No	No public information suggested that management knew about the attack for four months before publishing it
16	N/A	Yes (Phishing)	Employees noticed the system acted "abnormal"
17	N/A	Yes	N/A
18	N/A	Yes. Played on feelings	It was a terrible job and it was easy to see that it was fake
19	160 million users	No	Equifax disclosed the breach themselves
20	Several hundred systems, classified and unclassified networks	Yes	The US DoD discovered the attack and alerted the different targets
21	Unknown	No	The malware was so destructive that the impact was imminent

Table 8: Table 8 of 8 of the comparative analysis

No.	Political Situation at the Time of the Attack (Both Local and Global)
1	Cold War and a divided Germany
2	Tensions between the United States and China
3	Normal
4	Global worry over Iran getting nuclear weapons
5	The "normal" tensions between different states in the Middle East
6	Normal
7	Normal
8	Normal, but there was some tension when WADA decided not to let Russian athletes compete internationally
9	At the start of the still ongoing war between Russia and Ukraine
10	Normal, North Korea was looking for cash due to sanctions
11	North Korea was under pressure to stop their rocket and missile tests
12	A part of the ongoing tensions between Russia and the USA
13	Full-scale war in Ukraine
14	This has become a tool of different groups; amongst others, the Russian-affiliated APT group "Killnet" used a derived version towards countries that help Ukraine in their ongoing war with Russia
15	Normal
16	Some social tension in France at the time before the attack
17	Some protests against the Royal Family of Saudi Arabia
18	War in Ukraine
19	Some protests against the US financial system. Most famous was the "Occupy Wall Street" movement
20	Several regional conflicts and evolving security threats, including cyber
21	The attack was considered part of the ongoing war between Russia and Ukraine, which began in 2014

Working with the Norwegian Cybersecurity Centre (NCSC), we carefully selected these attacks to ensure their relevance to cybersecurity. To understand the dynamics of APTs, we collected data from various sources, including academic databases, blogs, and media outlets. This approach supplies a detailed exploration of this topic.

3.1 Observations from Notable APT Attacks

During the past two and a half decades, the post-Cold War era and aspirations for technological dominance have prompted a significant increase in cyberattacks, reshaping the cyber warfare landscape. The digital age, while empowering, has allowed governments to conduct secret operations, making it challenging to assign definitive blame for online assaults. This anonymity, especially the use of zero-day vulnerabilities and deceptive tactics by APT groups, complicates the attribution process (Tables 3 and 5).

APT groups vary in their motivations: Chinese factions are linked to industrial espionage, Russian groups to military objectives, and US entities to political cyber activities. Countries such as India, Pakistan, and North Korea also demonstrate APT capabilities, with North Korea focusing on national pride and financial gains (see Table 6).

Since the late 1980s, the evolution of individual hackers into state-sponsored APT entities has become notable. The Mandiant identification of China Unit 61398 and the activities of the Equation Group and Russia APT29 illustrate this change (Table 6).

3.2 Categorising the Attacks

Attacks can be classified according to their motivation and consequences. We divide the attacks into four categories.

Early Espionage: These attacks prove the development of cyber espionage, which focuses on obtaining confidential data and the growth of state-sponsored cyber operations. Examples include Cuckoo's Egg incident (1986), Operation Aurora (2009), Flame (2012), Red October (2007-2013), and Moonlight Maze (mid-1990s), which illustrate the stages of collecting classified information and increasing participation in state-sponsored cyber activities (see relevant citations).

Economic Infiltration: This category looks at cyberattacks that have significantly affected global financial systems, highlighting the economic weaknesses of these incidents. Examples of such attacks include SpyEye (2009-2011), Yahoo Data Breach (2013-2014), Equifax Data Breach (2017), and Saudi Aramco Hacking (2012), all of which have had considerable monetary impacts on the world economy (see relevant citations).

Political Disruption: These examples demonstrate the increasing prevalence of cyber warfare in political disputes, with incidents such as the Stuxnet Worm (2010), WADA Hack (2016), SolarWinds Attack (2020), Anonymous Attack on Russian State TV (2022), Le Monde Newspaper Defacement (2015), Deep Panda Operations (2014), and NotPetya Attack (2017) serving as evidence. Cyberattacks have been used to disrupt political processes and institutions, highlighting the growing importance of cyber warfare in geopolitical conflicts (see citations).

Unique Cases: This wide range of cyberattacks encompass various methods and targets, displaying various threats and creative tactics in the cyber world. Examples include the WannaCry attack (2017), Bureau 121 Sony Pictures attack (2014), Deep Fake Attack on President Zelensky (2022), Mirai attack (2016), and 2014 Russian cyberattack on a Ukrainian artillery app, each of which proves distinct threats and approaches (see the respective citations).

4. Results

This section explores the dynamic and constantly evolving domain of cybersecurity, with an emphasis on advanced persistent threats (APTs). Our study focused on the expansion and transformation of the indicators of compromise (IoC) associated with these threats.

An analysis of 21 different APT attacks revealed that APT activity is more complex and sophisticated. This development in IoCs reflects the increasing skill and sophistication of attackers. APTs are "a group involved in specialised cyber operations, often linked to national-state entities or organised crime." As outlined below, a transition in IoCs has been seen from the primary signs of persistence and stealth to more intricate strategic behaviour.

Enhanced Persistence: APT groups show a persistent effort to keep access to target networks, evident in repeated infiltration attempts and continuous communication with command-and-control centres.

Advanced Attack Methods: These threats employ sophisticated tactics, including zero-day exploits, custom malware, and complex multi-tier strategies, providing a detailed understanding of the vulnerabilities of their

targets.

Lateral Movement: Indicators such as unusual network activities, unanticipated privilege increases, and system interconnection exploitation suggest APT strategies to navigate within systems for increased control or access to critical data.

Strategic data exfiltration: APTs are characterised by unauthorised data transfers that involve abnormal data movement to unknown IP addresses or at unusual times.

Evasion Techniques: APTs use advanced techniques to avoid detection, including hidden network traffic, encrypted communications, and alterations in system logs.

APT Group-Specific IoCs: Certain IP addresses, domain names, malware signatures, or known tactics, techniques, and procedures can be used to propose APT.

Unusual User Activities: Signs such as logging in during odd hours, multiple failed access attempts, or unauthorised data access can indicate APT activities.

Resource utilisation: Abnormal system resource usage, such as increased CPU activity, unexpected network traffic, or sudden disk space consumption, may indicate an APT incident.

Detection of APTs is challenging because of their sophisticated and covert nature. Although these IoCs supply crucial information, they do not offer definitive proof of the presence of APT. Therefore, a complete and thorough investigation is essential when these signs are detected. A comprehensive and initiative-based approach for detection and analysis is necessary to counteract the covert and complex activities of APTs effectively.

5. Conclusions

This study extensively examines the development of advanced persistent threat actors (APT) over the past three decades. Studies have shown these actors have become increasingly complex and influential in cybersecurity. The transformation from isolated cyberattacks to well-structured state-sponsored operations, fuelled by a complex interplay of geopolitical, economic, and security interests, has led to a growing concern that traditional cybersecurity approaches are becoming less effective against the evolving tactics of APT actors.

Our analysis of twenty-one major APT incidents revealed a worrisome trend: changing tactics outpaced traditional cybersecurity strategies. Our findings emphasise the need for a dynamic and initiative-taking approach to cybersecurity that can adapt to constantly evolving threats posed by APTs. This includes enhancing indicators of compromise (IoCs) to be more responsive to advanced tactics, such as stealthy network infiltration, sophisticated data exfiltration techniques, and evasive manoeuvres that challenge conventional detection frameworks.

The increasing complexity and stealth of APTs require an equally sophisticated and vigilant cybersecurity posture. Organisations must adopt a multifaceted approach, focusing on detecting and mitigating attacks while emphasising preventive measures through continuous learning and adaptation. As APTs evolve, strategies must be developed to defend against them and ensure that cybersecurity measures are dynamic and resilient to threats they seek to combat.

The identification of Indicators of Compromise (IoCs) for advanced persistent threats (APTs) in this study significantly contributes to cybersecurity measures in the era of Artificial Intelligence (AI) and machine learning. This study catalogues and analyses IoCs associated with APT attacks by supplying a dataset that can be used to train AI systems. Understanding IoCs enables the development of more sophisticated AI-driven security tools capable of recognising subtle patterns and anomalies indicative of APT activities. Given the evolving nature of APTs, which often employ complex and stealthy strategies, AI and machine learning algorithms trained on comprehensive IoC data can adapt and improve over time, improving their ability to predict, detect, and respond to APT incidents with greater precision and speed. Integrating these IoCs into AI models transforms cybersecurity from reactive to initiative-taking, equipping systems with the foresight needed to thwart advanced threats before they manifest full-blown attacks. Thus, the study's insights into IoCs are not just retrospective analyses but are instrumental in shaping a more resilient and dynamic defense against future cyber threats.

In conclusion, our analysis of Compromise Indicators (IoCs) in the context of Advanced Persistent Threats (APTs) has yielded valuable insights into cybersecurity strategies. This research provides a robust dataset that can enhance the effectiveness of AI and machine-learning algorithms in threat detection and response. Our study

provides a nuanced understanding of IoCs, enabling advanced technologies to identify and respond to the complex patterns associated with APT activities. As APTs continue to employ sophisticated tactics, integrating AI-driven tools informed by our findings is essential. These tools are expected to evolve and enhance predictive accuracy and responsiveness to appearing threats. We contribute to advancing cybersecurity from a reactive approach to a more initiative-taking and adaptive framework. Using the power of AI and machine learning, we can remain ahead of APTs, ensuring that our defense mechanisms are as sophisticated and dynamic as those of the adversaries.

Acknowledgments

I extend my deepest gratitude to Professor Lasse Øverlier at Norwegian University of Science and Technology for his invaluable guidance and inspiration throughout my research. His expertise and encouragement have been pivotal in shaping my work, offering both challenges and support in equal ways.

Similarly, my sincere thanks go to Professor Kirsi Helkala at Norwegian Defence College, whose critical insights and contributions have significantly enriched my research. Her thoughtful feedback and encouragement were instrumental in pushing the boundaries of my work.

Together, Professors Øverlier and Helkala guided my academic path and profoundly impacted my professional development and personal growth. Their mentorship is the cornerstone of my journey, for which I am eternally grateful. As part of my ongoing research, this article is a testament to their invaluable support and belief in my potential.

References

Akbanov, M., Vassilakis, V.G. and Logotetis, M.D. (2019) 'Ransomware Detection and Mitigation Using Software-Defined Networking - The Case of WannaCry', Computers Electrical Engineering.

Ansart, J.P., Chari, V., Neyer, M., Rafiq, O. and Simon, D. (1983) 'Description, Simulation and Implementation of Communication Protocols Using PDIL', Computer Communication Review, 13(2), pp. 112-120.

Anstee, D. (2017) 'The Great Threat Intelligence Debate', Computer Fraud Security, 2017(9), pp. 14-16.

Bawaba, A. (2013) ''Red October' Cyber Espionage Network Discovered', InformationWeek.

Bencs, B., Pek, G., Buttyan, L. and Felegyhazi, M. (2012) 'The Cousins of Stuxnet: Duqu, Flame, and Gauss'. Available at: www.mdpi.com/journal/futureinternet [Accessed 5 January 2024].

Bitchkey, S. (2016) 'The Yahoo Data Breach and Its Repercussions'. Available at: https://hitachi-systems-security.com/the-yahoo-data-breach-and-its-repercussions/ [Accessed 5 January 2024].

Bronk, C. and Tikk-Ringas, E. (2013) 'The Cyber Attack on Saudi Aramco', Survival.

Buchanan, B. (2020) The Hacker and the State, Cambridge: Harvard University Press.

Cole, E. (2013) 'Author Biography', in Advanced Persistent Threat, Boston: Syngress, p. xiii. Available at: https://doi.org/10.1016/B978-1-59-749949-1.00018-8 [Accessed 5 January 2024].

Crowdstrike (2013) 'Deep Panda - Intelligence Team Report Ver 1.0'.

Fayi, S.Y.A. (2018) 'What Petya/NotPetya Ransomware Is and What Its Remediations Are', in Latifi, S. (ed.) Information Technology - New Generations, Cham: Springer International Publishing, pp. 93-100.

FireEye (2018) 'APT38: Un-usual Suspects'. Available at: https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html [Accessed 5 January 2024].

Haga, K., Meland, P.H. and Sindre, G. (2020) 'Breaking the Cyber Kill Chain by Modelling Resource Costs', in Graphical Models for Security, Lecture Notes in Computer Science, vol. 12419, Cham: Springer International Publishing, pp. 111-126.

Holm, L. (2017) 'Cyber Attacks Coercion in the Digital Era - A Qualitative Case Analysis of the North Korean Cyber Attack on Sony Pictures'.

Irinco, B. (2011) 'Trend Micro Researchers Uncover SpyEye Operation'. Available at: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/87/trend-micro-researchers-uncover-spyeye-operation [Accessed 5 January 2024].

Irshad, E. and Siddiqui, A.B. (2023) 'Cyber Threat Attribution Using Unstructured Reports in Cyber Threat Intelligence', Egyptian Informatics Journal, 24(1), pp. 43-59. Available at: https://doi.org/10.1016/j.eij
.2022.11.001 [Accessed 5 January 2024].

Krause, R. (2017) 'Verizon Surprise - Yahoo Data Breach Hit All 3 Billion Accounts'. Available at: https://www.investors.com/news/technology/verizon-surprise-yahoo-data-breach-hit-all-3-billion-accounts/ [Accessed 5 January 2024].

Langer, R. (2012) Robust Control System Networks - How to Achieve Reliable Control After Stuxnet, New York: Momentum Press.

Lazarovitz, L. (2021) 'Deconstructing the SolarWinds Breach', Computer Fraud Security, 2021(6), pp. 17-19. Available at: https://doi.org/10.1016/S1361-3723(21)00065-8 [Accessed 5 January 2024].

Lemay, A., Calvet, J., Menet, F. and Fernandez, J.M. (2018) 'Survey of Publicly Available Reports on Advanced Persistent Threat Actors', Computers Security, 72, pp. 26-59. Available at: https://doi.org/10.1016/j.cose.2017.08.005 [Accessed 5 January 2024].

McAfee (2024) 'Operation Aurora Overview'. Available at: https://www.youtube.com/watch?v=AEVbd5thokU [Accessed 5 January 2024].

Miller, J.R. (2022) 'Deepfake Video Shows Volodymyr Zelensky Telling Ukrainians to Surrender'. Available at: https://nypost.com/2022/03/17/deepfake-video-shows-volodymyr-zelensky-telling-ukrainians-to-surrender/ [Accessed 5 January 2024].

News, V. (2016) 'Wada Confirms Cyberattack by Russian Hackers'. Available at: www.voanews.com [Accessed 5 January 2024].

Oladimeji, S. and Kerner, S.M. (2024) 'SolarWinds Hack Explained: Everything You Need to Know'. Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know [Accessed 5 January 2024].

Pagliery, J. (2015) 'CNN Business'. Available at: https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html [Accessed 5 January 2024].

Pike, G.H. (2017) 'Equifax - Yet Another Data Breach', Information Today.

Purtill, J. (2022) 'Hacker Collective Anonymous Declares 'Cyber War' Against Russia, Disables State News Website: Hackers Launch Cyber Attacks Against Russian Government Websites, Including State-Controlled Russia Today, in Response to the Ukraine Crisis', ABC Science Online.

Rashid, F.Y. (2017) 'Old Attack Code is New Weapon for Russian Hackers', InfoWorld.com.

Research, C.P. (2018) 'APT37: Inside the Laziest Yet Most Effective North Korean APT Group'. Available at: https://blog.checkpoint.com/security/twisted-panda-check-point-research-unveils-a-chinese-apt-espionage-campaign-against-russian-state-owned-defense-institutes/ [Accessed 5 January 2024].

Review, B. (Unknown) 'Breaking the Cyber Kill Chain by Modelling Resource Costs'.

Rosenberg, J. (2017) 'Operation Aurora - Security in Embedded Systems', Rugged Embedded Systems.

Schwartz, M.J. (2016) 'Russian DNC Hackers Tied to Ukrainian Artillery App Hack', Bankinfosecurity.

Shakarian, P., Shakarian, J. and Ruef, A. (2013) 'Chapter 13 - Attacking Iranian Nuclear Facilities: Stuxnet', in Advanced Persistent Threat, USA: Syngress, 1st ed.

Shakarian, P., Shakarian, J. and Ruef, A. (2013) 'Chapter 8 - Duqu, Flame, Gauss, the Next Generation of Cyber Exploitation', in Introduction to Cyber-Warfare, Boston: Syngress, pp. 159-170. Available at: https://doi.org/10.1016/B978-0-12-407814-7.00008-7 [Accessed 5 January 2024].

Stoll, C. (1989) The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, USA, 1st ed.

Stoll, C. (2020) The Cuckoo's Egg, New York: Gallery Books.

Willett, M. (2021) 'Lessons of the SolarWinds Hack', Survival.

Zhang, X., Upton, O., Beebe, N.L. and Choo, K.K.R. (2020) 'IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers', Forensic Science International: Digital Investigation, 32, 300926. Available at: https://doi.org/10.1016/j.fsidi.2020.300926 [Accessed 5 January 2024].

Zou, Q., Sun, X., Liu, P. and Singhal, A. (2020) 'An Approach for Detection of Advanced Persistent Threat Attacks', Computer, 53(12), pp. 92-96. Available at: https://doi.org/10.1109/MC.2020.302154 [Accessed 5 January 2024].