LONDON
METROPOLITAN
UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

CC7178NI Cyber Security Management

Advanced Persistent Threat on a Global Scale

50% Individual Coursework

Year

2023/2024 Spring

Student Name: Nishit Koirala

London Met ID: 23057168

College ID: NP01MS7S240061

Assignment Due Date: Monday, May 6, 2024

Assignment Submission Date: Monday, May 6, 2024

Submitted To: Roshan Pokharel

Word Count : 4198

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Nishit Koirala **NP01MS7S240061** 6th May 2024

ABSTRACT

The report delves into the rising threat of Advanced Persistent Threats (APTs) in today's digital landscape, shedding light on their evolving tactics and global impact. Through comprehensive case studies on notable incidents like the SolarWinds supply chain attack and the activities of APT41 (Double Dragon), it elucidates the sophisticated techniques employed by these malicious actors. The study emphasizes the inadequacy of traditional security measures in detecting and mitigating APT attacks, necessitating proactive defense strategies and international collaboration.

Furthermore, it analyzes the current scenario, highlighting significant events and projections in the APT protection market. Regulatory responses and recommendations from cybersecurity agencies like CISA and the FBI are also examined, providing insights into best practices for threat mitigation. By outlining the APT life cycle and discussing risk management and contingency planning, the report offers a comprehensive framework for combating APT threats effectively.

The report underscores the critical need for heightened cybersecurity measures and collective action to counter the persistent threat posed by APT groups. By investing in advanced security technologies, fostering a culture of cyber resilience, and strengthening collaboration among stakeholders, organizations, and nations can fortify their defenses and safeguard against APT attacks.

Keyword: APT, CISA, Double Dragon, Cybersecurity, Solarwinds, Threats, Cyber Resilience

TABLE OF CONTENTS

List of Figures

Abbreviations

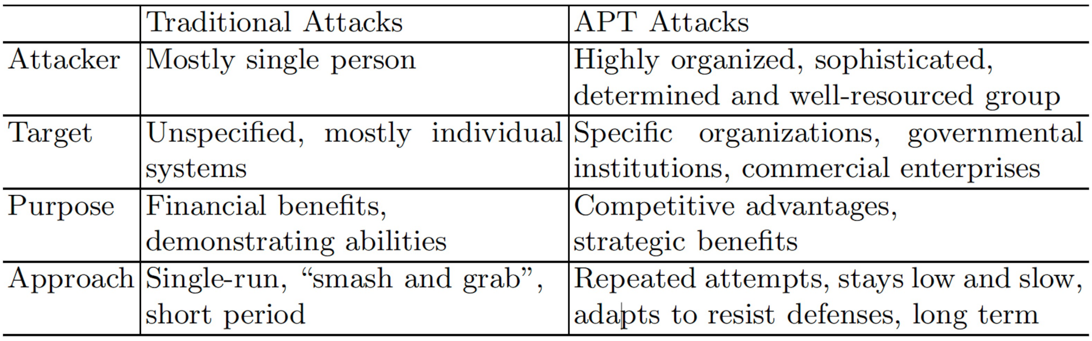
APT	Advance Persistent Threat
TTPs	Tactics, Techniques, and Procedures
CDR	Customer Due Diligence
SIEM	Security Information and Event Management
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
USAF	United States Air Force
C&C	Command and Control
RAT	Remote Access Trojan
CISA	Cybersecurity and Infrastructure Security Agency
FBI	Federal Bureau of Investigation
IOCs	Indicators of Compromise
EU	Europian Union
BFSI	Banking, Financial Services and Insurance
NGFW	New Generation Firewall
CAGR	Compound annual growth rate
DDoS	Distributed Denial of Service
IBM	International Business Machines
CI/CD	Continuous Integration / Continuous Delivery
DOJ	Department of Justice
IOCs	Indicators of Compromise
EDR	Endpoint Detection Response

1 INTRODUCTION

1.1 General Introduction

With rapid digitalization, cybercriminals are constantly evolving with new hacking Tactics, Techniques, and Procedures. In the past few years, there has been a rise in a newly identified class of threats known as the ”Advanced Persistent Threat”(APT). The term persistent means the continued or prolonged existence, Where the attackers gain and maintain an undetected presence in a network for a long period to steal highly sensitive data. APT was originally used to target military organizations, but it has now expanded to become a global issue. “Attackers of this type are typically supported by a nation-state or criminal organization.”

The APT campaign involved highly organized and well-resourced attackers. They had clear objectives and persistently pursued specific targets over a long period. The attackers used stealthy and evasive techniques in their repeated attempts. They usually use a mix of sophisticated techniques. These include advanced malware, social engineering, zero-day exploits, and targeted phishing campaigns. In the past traditional APT attacks were mostly run by a single person, and were usually done for financial benefits, and the approach was smash and grab as of today APTs are highly organized and attempt to stay low and slow to remain undetected and also to evade detection.



	Traditional Attacks	APT Attacks
Attacker	Mostly single person	Highly organized, sophisticated, determined and well-resourced group
Target	Unspecified, mostly individual systems	Specific organizations, governmental institutions, commercial enterprises
Purpose	Financial benefits, demonstrating abilities	Competitive advantages, strategic benefits
Approach	Single-run, “smash and grab”, short period	Repeated attempts, stays low and slow, adapts to resist defenses, long term

Figure 1.1: Comparison between Traditional Attacks and APT Attacks (Chen, et al., 2014).

APT includes cyber criminals such as APT34 from Iran, APT28 from Russia, and various other groups. Attackers can originate from any location globally, which makes

APT a Global Threat. Significant ones often emerge from Iran, other parts of the Middle East, and North Korea. They are currently focusing their efforts on a diverse array of industries and governmental bodies.

1.2 Problem Definition

With the advancement in new Tools and Technologies, traditional security measures such as Firewalls, antivirus, Intrusion detection, and prevention systems are unable to detect stealthy and sophisticated attacks. APTs Group typically employ a combination of sophisticated techniques, including advanced malware, social engineering, zero-day exploits, and targeted phishing campaigns. The primary objective of APT groups typically revolves around influencing national security, gathering sensitive information concerning the military plans of the targeted nation, and disrupting the economic stability of the country.

Detecting APT attacks poses a significant challenge due to its sophisticated use of Tactics, Techniques, and Encryption Methods. Mostly the underdeveloped countries like Nepal, people here are unaware of the potential risks in cyberspace. Recently, a Chinese APT group exfiltrated the call records of all Nepali Users from a government-based telecom company. Incident response reports show that the adversary had been seen taking CDR data from the telecom server to APT 41 and APT 71. The data stolen has been put on sale on the Dark web (Economic Times, 2021).

To prevent such incidents and narrow down the attack surface proper incident response framework should followed. Protective measures should be kept in place such as Threat sharing platforms, and performing vulnerability assessments simulating adversary tactics, techniques, and procedures.

So, proactive measures should be applied to prevent breaches. This report aims to provide insights into the APT's rising concern on a global scale and focuses on the life cycle of APT groups. It also covers the methods and strategies these groups employ to execute successful attacks, along with recommendations to mitigate or identify such sophisticated threats.

1.3 Current Scenario

Well-known events, like the SolarWinds supply chain breach and the Colonial Pipeline ransomware attack, have shown how APTs, with their advanced methods, affect both national security and economic stability.

Attacks conducted by APTs on EU institutions, bodies, and agencies increased by 30% in 2021. By 2025 the advanced persistent threat protection market will be worth an estimated $12.5 billion annually. These groups usually escalate threats to government agencies, financial institutions, and critical infrastructure providers. The cost of the tools needed for a banking attack would start at $55,000. A cyberespionage campaign would be much more expensive, running at least $500,000 to start. The BFSI sub-segment for APT protection is in extensive demand and is further expected to register a noteworthy revenue of $2,624.3 million by 2027. The global advanced persistent threat protection market is projected to reach $ 20 billion by 2027. The professional services for the advanced persistent threat (APT) protection market shall have notable growth and is projected to register a revenue of $9,387.7 million by 2027, surging from $1,619.5 million in 2019. The NGFW software for the advanced persistent threat (APT) protection market will be a rapidly growing segment and is further projected to register a revenue of $3,938.2 million by 2027. SIEM shall have a dominating market share in the global market and is expected to generate a revenue of $3,811.7 million, during the analysis timeframe (PURPLESEC, 2022).

The government and defense sub-segment for the advanced persistent threat (APT) protection market will have a dominating share in 2020 and is expected to generate a revenue of $2,631.1 million by 2027, with a CAGR of 19.3%.In 2015, several Ukrainian power companies were attacked, which led to blackouts. The attack involved spear-phishing emails to gain network access, followed by DDoS attacks (Tinney, 2024)

According to the ‘Cost of a Data Breach 2023’ report by IBM, the global energy sector set a new record in 2022, with an average data breach cost of $4.72 million (Allan, 2023).

It is anticipated that the global market revenue for APT Protection solutions will more than double, exceeding $12.4 billion by 2025 from its 2021 figure of over $5.9 billion (Radicati Group, 2021).

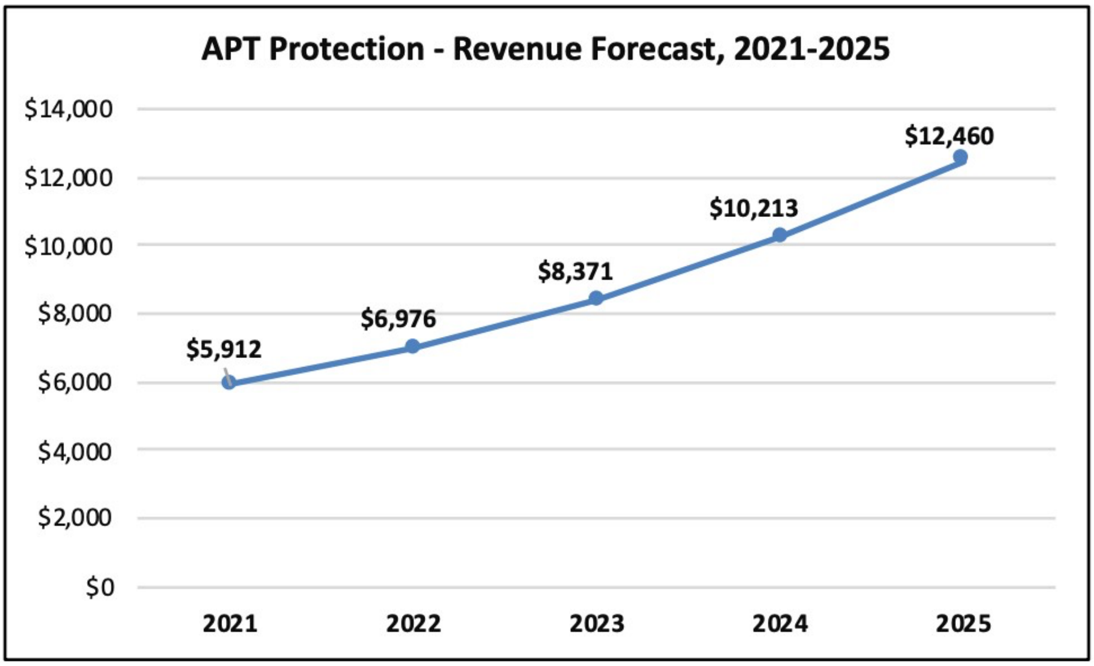


Figure 1.2: APT Protection Market Revenue Forecast, 2021 – 2025 (Radicati Group, 2021)

2 LITERATURE REVIEW

2.1 History of Advance Persistent Threats

On January 10 google disclosed, that it had been targeted by the sophisticated attack that marked the beginning of the APT era. Although Google's disclosure put APT into the spotlight, law enforcement, intelligence, and counterintelligence communities had already been using the term for several years. The United States Air Force (USAF) coined the phrase Advanced Persistent Threat back in 2006 because teams working within the service needed a way to communicate with counterparts in the unclassified public world (Radzikowski, 2015). Some of the most famous Advanced persistence threats are Cuckoo's Egg, Moonlight Maze, Titan Rain, and GhostNet (SailPoint, 2023). Today's organizations can't assume that they will fly under the radar of APTs. As exploits and methods propagate within the hacker community, more organizations will fall victim to targeted attacks and suffer potentially irrecoverable losses.

There's a suggestion that highly skilled attackers, no matter their motivations, financial resources, or oversight, often follow a specific cycle when targeting their victims. The below figure represents the evolution of APTs and the APT life cycle.

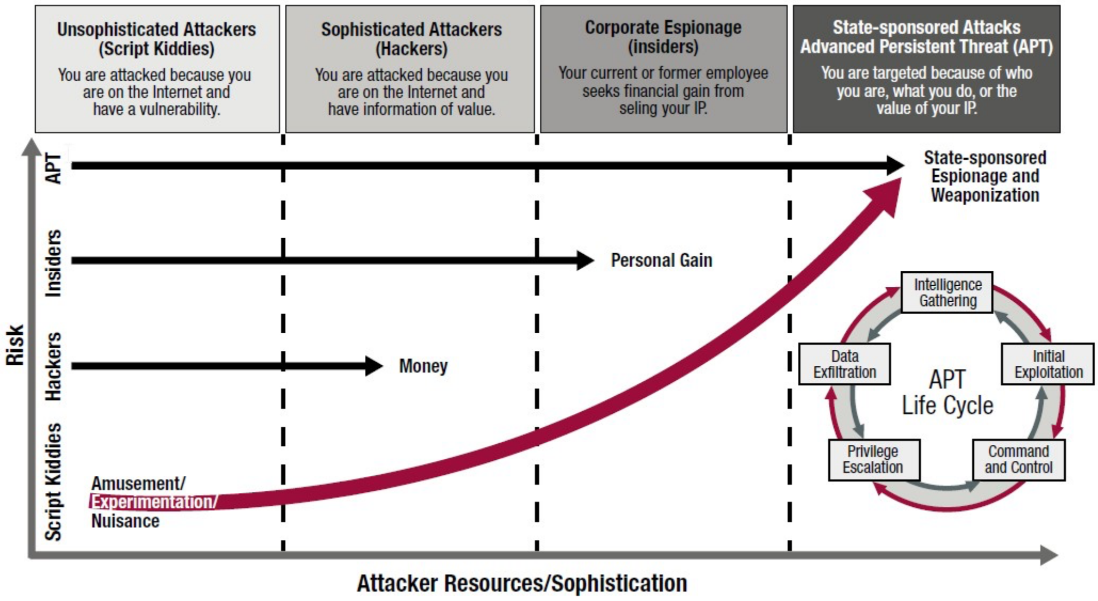

Unsophisticated Attackers (Script Kiddies)
You are attacked because you are on the Internet and have a vulnerability.
Sophisticated Attackers (Hackers)
You are attacked because you are on the Internet and have information of value.
Corporate Espionage (insiders)
Your current or former employee seeks financial gain from seling your IP.
State-sponsored Attacks Advanced Persistent Threat (APT)
You are targeted because of who you are, what you do, or the value of your IP.
Risk
APT
Insiders
Hackers
Script Kiddies
State-sponsored Espionage and Weaponization
Personal Gain
Money
Amusement/ Experimentation/ Nuisance
Intelligence Gathering
Initial Exploitation
Command and Control
Privilege Escalation
Data Exfiltration
APT Life Cycle
Attacker Resources/Sophistication

Figure 2.1: Evolution of APTs and APT life cycle (Radzikowski, 2015)

2.2 APT Life cycle

The cyber kill chain is based on the military's kill chain concept and was developed by Lockheed Martin in 2011. It's a structured approach that breaks down cyberattacks into stages, helping information security teams understand when and how they can prevent, detect, or disrupt attackers. This framework is particularly useful against advanced persistent threats (APTs), which involve highly skilled adversaries who carefully plan and execute attacks over an extended period. Below are the Cyber Kill chain phases (Bergmans, 2022) used by APT group for completely taking over the network.

Reconnaissance: Reconnaissance is when attackers collect information, like details about an organization, its systems, or its people, to plan their attacks. Normally APT groups gather information via active and passive scanning to get into the system, decide what they want to do next, or learn more about their target.

Weaponization: During an APT attack, attackers inject malicious software with ways to exploit system weaknesses. They do this to create unwanted files or links that can trick people into opening them. Attackers also use sneaky techniques like obfuscating code or making it look different to avoid getting caught by security systems. This helps them stay hidden and do more damage once they're inside a computer network.

Delivery: APTs use advanced social engineering to deliver weaponized content, often through phishing emails, watering hole attacks on frequented websites, or exploiting supply chain weaknesses. These tactics exploit human trust and vulnerabilities, allowing attackers to bypass defenses and successfully compromise targets with malicious payloads.

Exploitation: Upon execution, the weaponized content capitalizes on vulnerabilities, granting unauthorized access or control within the targeted system or network. This exploitation enables attackers to maneuver stealthily, compromise critical assets, and execute further malicious actions to achieve their objectives within the compromised environment.

Installation: After successfully exploiting vulnerabilities, attackers advance to the installation phase within the Cyber Kill Chain. During this stage, they strategically establish persistent access and control within the compromised system or network. This involves deploying malicious software or backdoors, altering system configurations, creating unauthorized user accounts, and establishing communication channels for command and control purposes.

Command & Control: Command and Control refers to methods that attackers employ to communicate with systems they control within a targeted network. C&C provides means of upgrading the malware, performing further attacks, and facilitating during the data exfiltration stage. A very sophisticated C&C is usually used by skilled and well-sponsored APT groups who want to keep their campaign very stealthy for a long time. In any case, C&C is a crucial part of the attack carried out by these adversaries.

Action on objectives: After gaining a solid foothold within the compromised system, attackers carry out actions that are in line with their specific goals. These goals could involve stealing data, altering system functions, causing service disruptions, gathering intelligence for future attacks, or engaging in other malicious activities to achieve their desired outcomes.

2.3 CISA & FBI Recommendations against Advance Persistent Threats

Cybersecurity and infrastructure security agencies and the Federal Bureau of Investigation regularly release advisories, alerts, and recommendations related to Advanced Persistent Threats (APTs) and cybersecurity in general. These organizations provide valuable insights, best practices, and guidance to help organizations protect against APTs and other cyber threats. Below listed are some of the recommendations from CISA and the FBI:-

- Segment network to restrict access and follow the least privilege policy.
- Regularly monitor network traffic as APT often blends the malicious traffic with legitimate network traffic to remain undetected.

- Implement multi-factor authentication across the system to add an extra layer of security.
- Assess and secure the supply chain from adversaries to prevent exploitation of third-party vulnerabilities and gaining unauthorized access to the network.
- Regularly collaborate with the industry partner to share threat intelligence and stay informed about the latest APT's TTP.
- Proactive Threat hunting should be done to detect unusual behavior across the system.
- A proper incident response plan should be developed and regularly updated. Simulated exercises must be done to test the effectiveness of the plan.
- Updating Use cases in the SIEM environment with the latest IOCs.

Regular cybersecurity training must be done to aware employees of phishing techniques, social engineering attacks, and some of the APT techniques. Moreover, encourage them to report the suspicious activity to the concerned department (MITRE Corporation, 2024).

2.4 Regulatory and Policies responses to APT threats on Global and National scale

Some of the regulatory and policy responses regarding APT threats on National and International levels are as follows:

❖ According to the Cybersecurity Bylaw 2020 (Nepal Telecommunications Authority, 2020)passed by the Nepal Telecommunications Authority:

- Telecommunication and internet service providers have to make use of national and international cyber risk information sharing platforms to receive and share information regarding security issues, Vulnerabilities, and cyber threat intelligence.

- Telecommunication and internet service provider are required to form an incident response team or computer emergency response team ('CERT') within their organizations. The minimum number of members in a CERT, or qualifications required to be a member of such team are not defined.

❖ The Budapest Convention on Cybercrime treaty, also known as the Council of Europe Convention on Cybercrime, facilitates international cooperation in combating cybercrime. It includes provisions for information sharing, mutual legal assistance, and establishing effective incident response mechanisms (Hitchens & Goren, 2017).

❖

ISO International Organization for Standardization develops and publishes cybersecurity standards (e.g., ISO/IEC 27001) that provide guidelines for implementing cybersecurity controls, managing information security risks, and promoting best practices globally (Hitchens & Goren, 2017).

❖ United Nations Office on Drugs and Crime (UNODC) Cybercrime Program: UNODC provides technical assistance, capacity building, and training programs to strengthen cybersecurity capabilities, enhance law enforcement cooperation, and combat cybercrime at the international level (Hitchens & Goren, 2017).

Risk management and Contingency planning

Some of the risk management plans are (Landman, 2023):

- Collaborative efforts among countries to share threat intelligence, indicators of compromise (IOCs), and attack patterns related to APTs enable better risk assessment and proactive threat detection.

- Coordinated incident response frameworks at the international level help manage APT-related incidents efficiently, minimize impact, and prevent further spread of attacks.

- Adherence to international norms, principles, and best practices in cyberspace, including responsible state behavior, cybersecurity standards (e.g., ISO/IEC 27001), and incident response guidelines, contributes to effective risk management against APTs.

- Collaborative agreements and initiatives between governments and the private sector, such as public-private information-sharing partnerships, joint cybersecurity exercises, and sector-specific cybersecurity alliances, enhance risk management capabilities against APTs.

Some of the contingency planning regarding APT are (LinkedIn community, 2023):

- Conduct a thorough risk assessment to identify potential APT targets, entry points, and critical assets.

- Define roles and responsibilities within the team and establish clear lines of communication.

- Conduct regular security assessments, penetration testing, and vulnerability scans to identify and remediate weaknesses.

- Implement secure backup solutions with regular backups stored in offsite locations to ensure data availability in case of APT-induced disruptions.

- Coordinate with legal advisors to understand the legal implications of APT incidents and develop appropriate responses.

- Conduct post-incident reviews and lessons-learned exercises to identify areas for improvement and update contingency plans accordingly.

2.5 Research Paper Review

A.IcojocaruandA.Gulyás. (2021), in “LAZARUS ”THE NORTH KOREAN HACKER GROUP, concluded that it poses a great threat to the financial system, education, and telecommunication on a global scale. It also states that the North Korean government or policy can’t be stopped as they have been backed up by strong nations. Malicious intentions shouldn’t be supported and therefore, technological assistance should not be provided to endorse such government policies. Geo-political biases shouldn’t be brought into the digital space. Emulating APT groups can be challenging due to their dynamic nature. We tried to cover the latest tactics and tools used by the APTs group with relevant data sources (GULYÁS, 2021).

P. Chen, L. Desmet, and C. Huygens (2014), “A study on advanced persistent threats” concluded how APT groups are complex and always changing, but they follow certain patterns. Regular security measures aren’t enough to stop them. To defend against APTs, we need to understand how they work and develop new ways to fight them. By looking at real cases and industry insights, the paper offers a broad view of APTs to help the security community work together on better defenses. Oversimplifying APT behaviors by only focusing on common patterns, and potentially missing out on unique tactics and techniques is a risk. Relying only on publicly available cases and industry insights might also limit the depth of analysis and overlook undisclosed APT activities (Chen, et al., 2014).

3 Critical Analysis

3.1 Case Study 1: SolarWinds Supply Chain Attack

3.1.1 Background

In 2020, one of the largest and most sophisticated supply chain breaches took place at SolarWinds known as SolarWinds cyberattack or SolarWinds supply chain attacks. It was a major attack in U.S. history because it didn't just breach SolarWinds infrastructure but caused a bigger problem across many organizations including the U.S. government, through a supply chain attack. This attack was carried out by skillful APT groups where they inserted malicious code into the network monitoring platform of SolarWinds "Orion", which resulted in the attackers gaining access to sensitive data and systems within the affected organization (Oladimeji & Kerne, 2023).

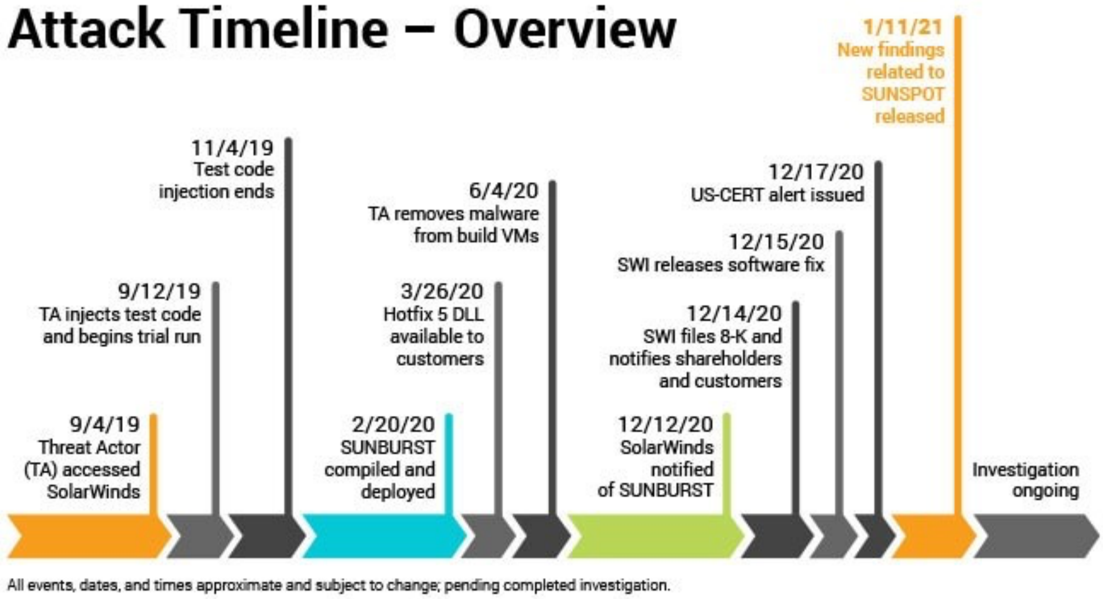

Attack Timeline – Overview
9/4/19 Threat Actor (TA) accessed SolarWinds
9/12/19 TA injects test code and begins trial run
11/4/19 Test code injection ends
2/20/20 SUNBURST compiled and deployed
3/26/20 Hotfix 5 DLL available to customers
6/4/20 TA removes malware from build VMs
12/12/20 SolarWinds notified of SUNBURST
12/14/20 SWI files 8-K and notifies shareholders and customers
12/15/20 SWI releases software fix
12/17/20 US-CERT alert issued
1/11/21 New findings related to SUNSPOT released
Investigation ongoing
All events, dates, and times approximate and subject to change; pending completed investigation.

Figure 3.1: SolarWinds attack timeline (Ramakrishna, 2021)

3.1.2 Objectives

The objective behind the SolarWinds attack was to breach the SolarWinds Orion platform by poisoning software updates with malicious code. This results in gaining unauthorized access to the networks of thousands of organizations that used the poisoned software. This allowed them to conduct espionage, steal sensitive information, and potentially disrupt operations within these targeted entities.

3.1.3 Issue Identification

FireEye was the first to detect the breach, confirming their exposure to the malware upon observing its presence within customer systems. To gain initial access to the organization's systems, the attacker targeted the core of the CI/CD pipeline, where code undergoes testing, packaging, containerization, and signing. They successfully altered SolarWinds' source code and introduced malware, famously dubbed "SunSpot," which operated with elevated privileges. This malware was designed to scan for Orion builds (CyberArk, 2021). The attackers chose Orion because it's connected to many parts of a company's network, like switches, routers, and more. This means it has access to important passwords and information. So, by targeting Orion, they could get into many different areas of a company's network easily.

The compromised software then spread to impact a minimum of nine U.S. federal agencies, including the Department of Justice (DOJ), the Department of Defense, the Department of Homeland Security, and the Treasury Department. Additionally, it affected leading technology and security companies such as Microsoft, Mandiant, Intel, Cisco, and Palo Alto Networks.

The Department of Justice (DOJ) initially discovered the operation six months earlier, in late May 2020. They became suspicious when they noticed unusual activity originating from a server running a trial version of SolarWinds' Orion software suite. This software, utilized by system administrators for network management, was communicating externally with an unfamiliar internet system. To investigate further, the DOJ sought assistance from security firm Mandiant and engaged with Microsoft, though the exact reason for involving Microsoft in the investigation remains unclear. The DOJ publicly disclosed that the SolarWinds hackers may have breached approximately 3 percent of its Office 365 mailboxes (ZETTER, 2023).

3.1.4 Mitigation

Some of the mitigation measures recommended by CISO are:

- **Assume Compromise and Activate Incident Response Plan:**

  - If using the affected version of SolarWinds, assume compromise and activate a full incident response plan immediately.

  - Conducted a comprehensive forensic analysis to understand the attack vector, and to identify compromised systems.

- **Rebuild Affected Devices and Update SolarWinds Orion Platform:**

  - Rebuild affected devices using trusted SolarWinds sources and ensure the latest versions of the SolarWinds Orion platform are installed.

- **Enhance Security Measures:**

  - Include all known Indicators of Compromise (IoCs) in the block list.

  - Run up-to-date Endpoint Detection and Response (EDR) and antivirus solutions to detect compromised libraries

  - Disable/remove unnecessary services and applications (Smeaton, 2020).

Some additional security policies and practices to prevent future data breaches include:

- **Enhanced Access Control:** Implement strict access controls to limit access to sensitive systems and data.

- **Regular Security Audits:** Conduct regular security audits and assessments to identify vulnerabilities, misconfigurations, and potential risks in the IT infrastructure.

- **Network Segmentation:** Segment the network using VLAN so that different groups of users can be separated from each other.
- **Continuous Monitoring:** Implement continuous monitoring of network traffic, system logs, and user activities using security information and event management (SIEM) tools to detect and respond to suspicious activities in real-time.
- **User Awareness Training:** Provide comprehensive cybersecurity awareness training to employees to recognize phishing attacks, suspicious activities, and best practices for data protection.

The SolarWinds cyberattack led to an increased focus on national cybersecurity. A forthcoming executive order will require federal contractors to report cyber incidents, list software details for important programs sold to the government, and work with law enforcement. It also encourages sharing information between public and private sectors and may improve security with measures like two-factor authentication and data encryption for federal agencies (Morrison & Foerster LLP, 2021).

3.1.5 Case Study Summary

From the case study, We learned cyberattack happened at SolarWinds, carried out by a skilled hacker group. They got into SolarWinds' Orion platform using corrupted software updates, causing problems for many organizations like U.S. government agencies and big tech firms. FireEye caught the breach first, which led to actions to fix it, like making response plans, fixing devices, improving security, and planning new cybersecurity rules for government contractors.

3.2 Case Study 2: APT41 (Double Dragon)

3.2.1 Background

APT41, also known as Double Dragon, is a significant cyber threat group engaging in both Chinese state-sponsored espionage and financially motivated cybercrime activities. This group has been active since 2012 and is known for its sophisticated tactics, including the use of a wide range of malware families like HIGHNOON, HOMEUNIX, PHOTO, SOGU, and ZXSHELL. APT41 conducts activities across diverse industries, with particular attention given to healthcare, telecommunications, and technology sectors. The group's activities involve a blend of espionage for political purposes and financial gain, showcasing a dual nature in its cyber operations. Additionally, APT41 has been observed using techniques like DLL side-loading and exploiting vulnerabilities to establish footholds in victim environments. The group's operations demonstrate a high level of sophistication, adaptability, and persistence in carrying out cyber attacks (MANDIANT , 2022).

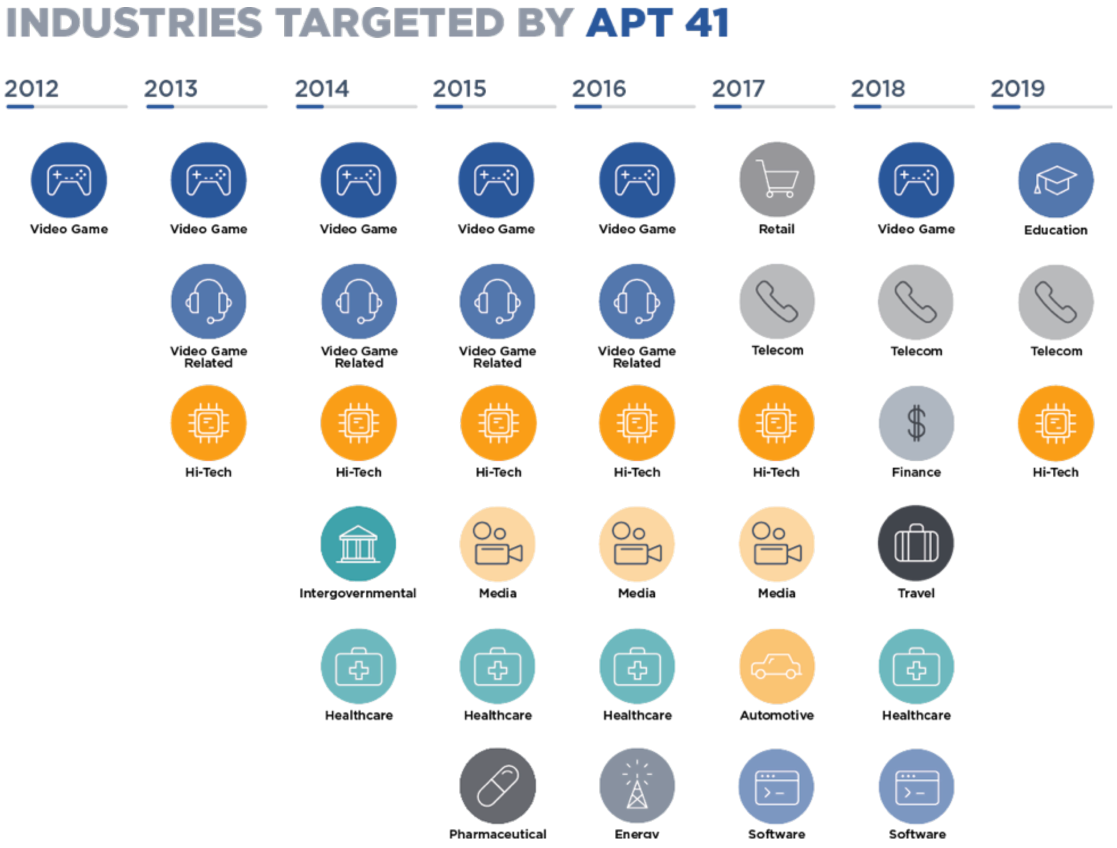


Figure 3.2: Timeline of industries directly targeted by APT41 (Mandiant, 2019).

3.2.2 Objectives

APT41 is a Chinese cyber group that does two main things: spying and cybercrime. They want to keep accessing systems and data to do more attacks, mess up enemy activities, and make people unsure. They go after industries like healthcare, technology, and gaming to get money or political benefits. APT41's actions show they are after both spying and making money, using a variety of cyber tactics.

3.2.3 Issue Identification

APT41 represents a unique and complex threat landscape due to its simultaneous engagement in both cyber espionage and cybercrime activities. Between July 2014 and May 2016, APT41 targeted a medical devices subsidiary of a large corporation. A keylogger dubbed GEARSHIFT was first deployed at the medical device company.
A digital certificate from the victim was compromised and used to sign malware used in an operation against a separate biotech company. A biotech company undergoing acquisition was targeted by APT41 in May 2015. Highly sensitive information about corporate operations, including human resources data, tax information, and acquisition-related documents, were targeted. Clinical trial data of developed drugs, academic data, and R&D funding-related documents were exfiltrated.APT41 is well-known for leveraging compromised digital certificates from video game studios to sign malware. The group has abused at least 19 different certificates in this way. APT41 has used several malware families that have also been used by other Chinese espionage operators, including variants of HIGHNOON, HOMEUNIX, PHOTO, SOGU, and ZXSHELL (MANDIANT , 2022).

3.2.4 Mitigation

Some of the mitigation measures related to APT41 are given below:

- Employ endpoint protection systems equipped with advanced threat detection features, such as behavioral analysis and machine learning, to detect and thwart APT41's sophisticated malware.

- Partition of the network to isolate critical medical devices, patient records, and sensitive data from other network segments.
- Deploy email security solutions, such as filtering and anti-phishing tools, to identify and block malicious emails used by APT41 for initial infiltration or lateral movement within the medical sector's network.
- Develop and routinely update an incident response strategy tailored to the specific threat profile posed by APT41 in the medical sector.
- Employ security monitoring systems to continuously surveil network traffic and system operations for indications of APT41's presence.
- Establish strict procedures for managing digital certificates to prevent them from being compromised or misused.

Mitigating an Advanced Persistent Threat involves two main approaches: reactive methods and proactive analysis. Reactive methods focus on identifying potential attack paths and scenarios based on existing vulnerabilities. Proactive analysis involves analyzing metrics within graphs to detect attacks and predict possible pathways. In summary, APT mitigation involves both reacting to current vulnerabilities and analyzing data to anticipate and prevent future attacks (Brandao & Limonova, 2021).

3.2.5 Case Study Summary

From the case study, it is clear that APT41 is a sophisticated cyber threat group engaging in both state-sponsored espionage and financially motivated cybercrime. Active since 2012, their tactics include deploying various malware families across industries like healthcare, telecommunications, and technology. Their objectives span spying and financial gain, using advanced techniques like DLL side-loading. Mitigation strategies involve advanced threat detection, network partitioning, email security, incident response planning, and digital certificate management to counter cyber attacks.

4 CONCLUSION

The examination of the APT Group on a global scale underscores the urgent need to boost cybersecurity measures and foster international cooperation. Their sophisticated tactics, abundant resources, and sustained targeting of high-profile assets across various sectors highlight the ever-evolving cyber threat landscape. Their infiltration of government agencies, critical infrastructure, and private enterprises poses a severe risk to national security, economic stability, and individual privacy.

This report highlights the importance of proactive defense strategies, such as sharing robust threat intelligence, implementing advanced network security protocols, and maintaining constant alertness for suspicious activities. It also emphasizes the crucial role of fostering collaboration among governments, law enforcement agencies, cybersecurity firms, and other stakeholders to effectively detect, disrupt, and mitigate APT group operations.

As the global cybersecurity landscape continues to evolve, it’s crucial for organizations and nations to remain alert, adaptable, and united against the persistent threat of APT groups. By investing in cutting-edge technologies, promoting a cybersecurity-conscious culture, and prioritizing collaboration and information sharing, we can secure our defenses and shield ourselves from the ongoing threat posed by APT groups.

REFERENCES

Chen, P., Huygens, C. & Desmet, L., 2014. *A Study on Advanced Persistent Threats.* [Online] Available at: https://doi.org/10.1007/978-3-662-44885-4_5 [Accessed 4 March 2024].

Economic Times, 2021. *Nepal telecom call details stolen by chinese hackers.* [Online] Available at: https://ciso.economictimes.indiatimes.com/news/nepal-telecom-call-details-stolen-by-chinese-hackers/84366159 [Accessed 6 March 2024].

Vairav Technology, 2023. *Apt sidewinder: Targeted incursions aimed at nepal's governmental entities.* [Online] Available at: https://vairav.net/assets/backend/uploads/Files/APT%20Sidewinder-TARGETED%20INCURSIONS%20AIMED%20AT%20NEPAL'S%20GOVERNMENTAL%20ENTITIES.pdf?fbclid=IwAR3Ijf2p7SfM5bI7HNcQ6lx9XaIOwH4dkLnE_FrzqaFFmr1JOnMaj15u2MA [Accessed 10 March 2024].

Seals, T., 2020. *SideWinder APT Targets Nepal, Afghanistan in Wide-Ranging Spy Campaign.* [Online] Available at: https://threatpost.com/sidewinder-apt-nepal-afghanistan-spy-campaign/162086/ [Accessed 10 March 2024].

Radicati Group, 2021. *Advanced Persistent Threat (APT) Protection Market, 2021-2025.* [Online] Available at: https://www.radicati.com/wp/wp-content/uploads/2021/03/APT-Protection-Market-2021-2025-Executive-Summary.pdf [Accessed 11 March 2024].

Radzikowski, S., 2015. *CyberSecurity: Origins of the Advanced Persistent Threat (APT).* [Online] Available at: https://drshem.com/2015/10/08/cybersecurity-origins-of-the-advanced-persistent-threat-apt/ [Accessed 12 March 2024].

SailPoint, 2023. *Advanced persistent threat (apt).* [Online] Available at: https://www.sailpoint.com/identity-library/advanced-persistent-threat/ [Accessed 4 March 2024].

MITRE Corporation, 2015-2024. *Mitre att&ck groups.* [Online] Available at: https://attack.mitre.org/groups/ [Accessed 13 March 2024].

GULYÁS, A., 2021. *"LAZARUS" THE NORTH KOREAN HACKER GROUP.* [Online] Available at: https://revista.unap.ro/index.php/XXI_CSSAS/article/download/1354/1314/4735 [Accessed 14 March 2024].

Oladimeji, S. & Kerne, S. M., 2023. *SolarWinds hack explained: Everything you need to know.* [Online] Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know [Accessed 17 March 2024].

Ramakrishna, S., 2021. *New Findings From Our Investigation of SUNBURST.* [Online] Available at: https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/ [Accessed 17 March 2024].

CyberArk, 2021. *The Anatomy of the SolarWinds Attack Chain.* [Online] Available at: https://www.cyberark.com/resources/blog/the-anatomy-of-the-solarwinds-attack-chain [Accessed 19 March 2024].

ZETTER, K., 2023. *The DOJ Detected the SolarWinds Hack 6 Months Earlier Than First Disclosed.* [Online] Available at: https://www.wired.com/story/solarwinds-hack-public-disclosure/ [Accessed 19 March 2024].

Smeaton, A., 2020. *A CISO's Perspective - SolarWinds Hack and Mitigation Measures.* [Online] Available at: https://www.linkedin.com/pulse/cisos-perspective-solarwinds-hack-mitigation-andrew/ [Accessed 20 March 2024].

Morrison & Foerster LLP, 2021. *U.S. Government Responds to SolarWinds Hack.* [Online] Available at: https://www.mofo.com/resources/insights/210419-us-government-responds-solarwinds-hack [Accessed 20 March 2024].

MANDIANT, 2022. *APT41 (Double Dragon): A Dual Espionage and Cyber Crime Operation.* [Online] Available at: https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf [Accessed 22 March 2024].

Mandiant, 2019. *Timeline of industries directly targeted by APT41.* [Online] Available at: https://www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation [Accessed 22 March 2024].

Brandao, P. R. & Limonova, V., 2021. *Defense Methodologies against Advanced Persistent Threats.* [Online] Available at: https://thescipub.com/pdf/ajassp.2021.207.212.pdf [Accessed 25 March 2024].

PURPLESEC, 2022. *Advanced Persistent Threat (APT) Statistics.* [Online] Available at: https://purplesec.us/resources/cyber-security-statistics/#APTs [Accessed 10 April 2024].

Tinney, M., 2024. *Cybersecurity Solutions for the Energy Sector.* [Online] Available at: https://www.linkedin.com/pulse/cybersecurity-solutions-energy-sector-safeguarding-critical-tinney-j2vtc/ [Accessed 20 April 2024].

Allan, K., 2023. *Protecting the energy sector using proactive intelligence.* [Online] Available at: https://cybermagazine.com/articles/protecting-the-energy-sector-using-proactive-intelligence [Accessed 10 April 2024].

Bergmans, B. L., 2022. *WHAT IS THE CYBER KILL CHAIN? PROCESS & MODEL.* [Online] Available at: https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/ [Accessed 14 April 2024].

Nepal Telecommunications Authority, 2020. *Cyber Security Byelaw, 2077 (2020).* [Online] Available at: https://nta.gov.np/uploads/contents/Cyber-Security-Bylaw-2077-2020.pdf [Accessed 13 April 2024].

Hitchens, T. & Goren, N., 2017. *International Cybersecurity Information Sharing Agreements.* [Online]
Available at:
https://www.jstor.org/stable/resrep20426?searchText=&searchUri=&ab_segments=&searchKey=&refreqid=fastly-default%3Ac883a644623c434e2f046ab67fd219df&seq=4 [Accessed 15 April 2024].

Landman, C., 2023. *Cybersecurity Risk Management Fundamentals.* [Online] Available at: https://www.auditboard.com/blog/cybersecurity-risk-management/ [Accessed 16 April 2024].

LinkedIn community, 2023. *What are the best cybersecurity practices for contingency planning?* [Online]
Available at: https://www.linkedin.com/advice/3/what-best-cybersecurity-practices-contingency [Accessed 17 April 2024].