Modeling of APT Actors Targeting Healthcare Sector

Muhammad Dikko Gambo [1†] and Dr Talal Mousa Alkharobi [2††],

King Fahad University of Petroleum and Minerals

Abstract
The healthcare sector plays a crucial role in saving lives, storing sensitive patient data, and ensuring public health. Any compromise in this sector can have severe consequences, including patient safety and privacy breaches. Globally, the healthcare industry continues to be the top target for cyberattacks given its role in society and the value of its immense data. Advanced Persistent Threats (APTs) continue to be a major security problem in today's cyberspace. The necessity for up-to-date information is crucial for cybersecurity experts to effectively carry out their responsibilities. This paper presents an in-depth study of Advanced Persistent Threats (APTs) targeting the healthcare sector, focusing on three APT groups: FIN4, Deep Panda, and APT41. The study identifies and examines the Tactics, Techniques, and Procedures (TTPs) employed by these groups, using the Cyber Kill Chain, Diamond Model, and MITRE ATT&CK frameworks. The study reveals how these APT actors gain and maintain access to healthcare systems, highlighting their strategies for exploiting vulnerabilities and evading detection. We also offer a novel ontological breakdown of TTPs, providing a structured approach to understanding these complex cyber attacks. The paper contributes significantly to the cybersecurity field by proposing a comprehensive Cyber Threat Intelligence (CTI) model, which includes actionable CTI reports for each APT group. These reports serve as a strategic resource for healthcare organizations, enabling them to adopt proactive and targeted defense strategies. Finally, we formulate practical recommendations presented in a Course of Action matrix for robust defense against these sophisticated adversaries.
Keywords:
TTP,APT,CKC, CTI

1. Introduction

In nearly every country, healthcare services are one of the most significant areas of the economy and society. The International Labour Organization (ILO) supports the basic concepts of the human right to health and social protection. (Mucaraku & Ali, 2022) The healthcare sector plays a crucial role in saving lives, storing sensitive patient data, and ensuring public health. Any compromise in this sector can have severe consequences, including patient safety and privacy breaches. (Pandey et al., 2020). Globally, the healthcare industry continues to be the top target for cyberattacks, according to IBM's annual report on data breaches. For the 13th straight year, that sector reported the most expensive breaches of any field, averaging $11 million each (Seh et al., 2020).

"In October 2020, for instance, over 5,000 devices were targeted, shutting down the IT systems of the UVM Health Network. The system went down for 40 days and caused a loss of over 1.5 million dollars a day in revenue and expenses (Bardow, 2021) The healthcare sector suffered about 295 breaches in the first half of 2023 alone, according to the HHS Office for Civil Rights (OCR) data breach portal. More than 39 million individuals were implicated in healthcare data breaches in the first six months of the year (HealthITSecurity, 2022)" Notable instances include a cyberattack on a California-based healthcare provider System, which caused emergency rooms across multiple states to be closed and ambulance services to be redirected (CBS News, 2023)

Given the concerning situation we're facing it's clear that the healthcare industry urgently needs an analysis and effective strategies to combat the evolving Advanced Persistent Threats (APTs). To strengthen cybersecurity defenses and protect patients well being as well as protecting sensitive healthcare data, it is essential to understand the tactics, techniques and procedures (TTPs) employed by APT groups when targeting healthcare organizations. This research aims to investigate how each APT group targets the healthcare sector and provide actionable insights and recommendations, for enhancing security against APT threats, in the healthcare industry.

Advanced Persistent Threats (APTs) pose an widespread cybersecurity challenge, for governments, corporations and especially the healthcare sector. APTs are carefully planned cyberattacks carried out by well supported and sophisticated threat actors. These attackers employ techniques and tactics to avoid detection allowing them to maintain access to their targets for extended periods of time. As they continuously adapt their strategies to exploit emerging vulnerabilities APT attacks impose burdens costing companies and government agencies billions of dollars every year. Although APT attacks target industries the healthcare sector is particularly vulnerable due to its

Manuscript received February 5, 2025
Manuscript revised February 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.2.17

societal role and the high value of its data (Mucaraku & Ali 2022). Recent statistics highlight the seriousness of this problem indicating an increase in data breaches and incidents, within the healthcare sector (IBM, 2019).

2. Literature Review

The literature review allowed us to identify the various topics related to APT (Advanced Persistent Threat) attacks that have been studied by other researchers. The data for this review was primarily sourced from Web of Science and Google Scholar. It is evident that the detection and defense against APT attacks have been a significant area of focus in the articles published. Investigating cyber threats is not a new concept; it has been an ongoing research endeavor. Numerous techniques have been documented in the literature to actively detect these threats.

Research in this area has explored aspects of identifying attacks, including game theory, modeling, detection systems, and the utilization of honeypots in networks and defensive mechanisms. Bahrami et al. highlighted the importance of staying updated with information about APTs tactics, techniques, and procedures (TTPs) to develop defense strategies. They emphasized how using taxonomies for categorizing cyberattacks can be valuable. One significant contribution to this field is the Diamond Model of cyber attack modeling introduced by Chapman et al. in 2011. This model simplifies cyber attacks by focusing on four components; the adversary, victim, capability, and infrastructure.

Different methods of modeling, such as Attack Graphs or Trees, play a role in analyzing cyber threats. Caltagirone et al. have emphasized the significance of these techniques especially when it comes to modeling Advanced Persistent Threats (APTs) to improve detection methods and strengthen cybersecurity measures (Caltagirone et al., 2013). Atapour et al. took a theoretical approach by utilizing the kill chain framework to model four well-known APTs and identify common behavior. They highlighted that APTs actors can be detected at one or more stages of operation (Atapour et al., 2018).

For a comprehensive cyber threat intelligence, we must interpret attack data collected from network events. This analysis involves identifying various cyber attack artifacts, such as IP addresses, domain names, tools and techniques, usernames, passwords, and the geographical location of the attacker. Al-Mohannadi et al. have highlighted the significance of using cloud-based web services as a honeyport to enhance cyber threat intelligence by understanding the indicators of compromise of the attackers (Al-Mohannadi et al., 2020).

In their research, Bahrami et al. examined classifications used to analyze APT actors. We have included a table derived from their work, which outlines the taxonomies utilized by various researchers and their respective strengths and limitations.

Method	Authors	Strength	Limitations
Multi-dimensional	Hansan et al.,	Enables the comprehensive categorization of attack. Examines attack from a variety of angles.	Specified APTs; limited in scope. Real evaluation of cyber attack are not taken into account.
Based on attack type	Chapman et al.,	Explains how an attacker might go about carrying out an attack.	Not meant to record complex attacks. For complex attacks, no suitable protection method can be suggested. Not based on actual attack.
Initial infection vector	Virvilis et al.,	Shows the typical behavior patterns and methods used by APT actors. Recommends defenses against attacks.	Other attacks cannot be classified using this taxonomy since it only considers four APT actors. Attack stages or an APT group's campaign lifespan are not taken into account.
CKC	Chen et al.,	Examining the strategies used often in APT attacks.	The taxonomy cannot be generalized since there have been few real-world attacks evaluated. The results do not provide specific information.

CKC	Yadav et al.,	Methodologies, tactics, and resources used in the CKC model's many stages are organized into categories.	There is a lack of specificity in the classification of technologies utilized throughout each stage of an attack. The taxonomy lacks a real-world APT attack foundation; categorization is too broad and constrained.
CKC	Ussath et al.,	An examination of 22 APT campaigns' tactics suggests using a detection and prevention strategy.	Concentrate solely on the CKC model's three phases. There are only a few defenses. For each campaign, only one report is used in the study of APT attacks. The technological aspects of the attack are not taken into account.
APT actors	Lemay	Emphasizes the operations of the APT.	There are no defensive measures present.
CKC	Bahrami et al.,	Analysing 40 APT groups, decompose complex attacks and identify the relevant characteristics of such attacks	do not provide a systematic way to extract and classify the objective of APTs attack.
CKC & Damond Model	Taylor et al.	provides a comprehensive and systematic representation of the adversary's actions, capabilities, infrastructure, and objectives outlines defensive strategies for each stage of the Cyber Kill Chain	do not fully accommodate the dynamic and adaptive nature of certain APT groups, which might employ alternative paths to evade detection

3. Methodology

Our research commenced with a comprehensive literature review, aimed at understanding the methodologies employed by other researchers in analyzing APT actors. This review was critical in identifying existing gaps, particularly in the systematic categorization of cybersecurity data, which is essential for effective and efficient analysis by cybersecurity professionals.

The APT actors analyzed in this study are briefly described below:

- **FIN4**: Notable for its financial motivations, FIN4 has primarily targeted information critical to financial markets, especially focusing on the healthcare and pharmaceutical sectors since at least 2013. This group is distinguished by its strategy of capturing credentials for accessing confidential email communications rather than deploying typical persistent malware (MITRE, n.d. -a).
- **Deep Panda**: Suspected to be a Chinese threat group, Deep Panda has targeted various industries, including healthcare. This group's involvement in the Anthem healthcare breach underscores its capability to penetrate sensitive health data networks. Known by several aliases, Deep Panda's diverse operations highlight the need for comprehensive cybersecurity measures in the healthcare sector (MITRE, n.d.-b).
- **APT41**: Considered a Chinese state-sponsored group, APT41 conducts both espionage and financially motivated operations. Active since at least 2012, this group has targeted sectors including

healthcare, telecommunications, and technology, demonstrating the necessity for multifaceted defense strategies in the healthcare industry (MITRE, n.d.-c).

-

To analyze the TTPs of these APT actors, we utilized the MITRE ATT&CK framework, an accessible knowledge base framework, built upon real-world observations of adversary tactics and techniques. It served as our foundation for understanding and categorizing these APT actors.

To extract the Tactics, Techniques, and Procedures (TTPs) employed by our selected APT groups effectively, we used the ATT&CK Navigator tool. This tool is very helpful in extracting and visualizing ATT&CK vectors, enabling us to develop an understanding of how each group carries out their attacks.

Applying the Cyber Kill Chain framework, which outlines the phases of a cyberattack, from gathering information to stealing data, allowed us to analyze and understand the tactics, techniques, and procedures (TTPs) used. This analysis helped us uncover the motives and progression of each stage in an attack.

We used the Diamond Model to delve deeper into understanding malicious activities, focusing on comprehending the attackers' motivations and the specific steps they undertake to achieve their objectives. This model offered an enhanced perspective, enabling us to dissect the intricacies of each attack and the strategic intent behind the actions of these APT groups.

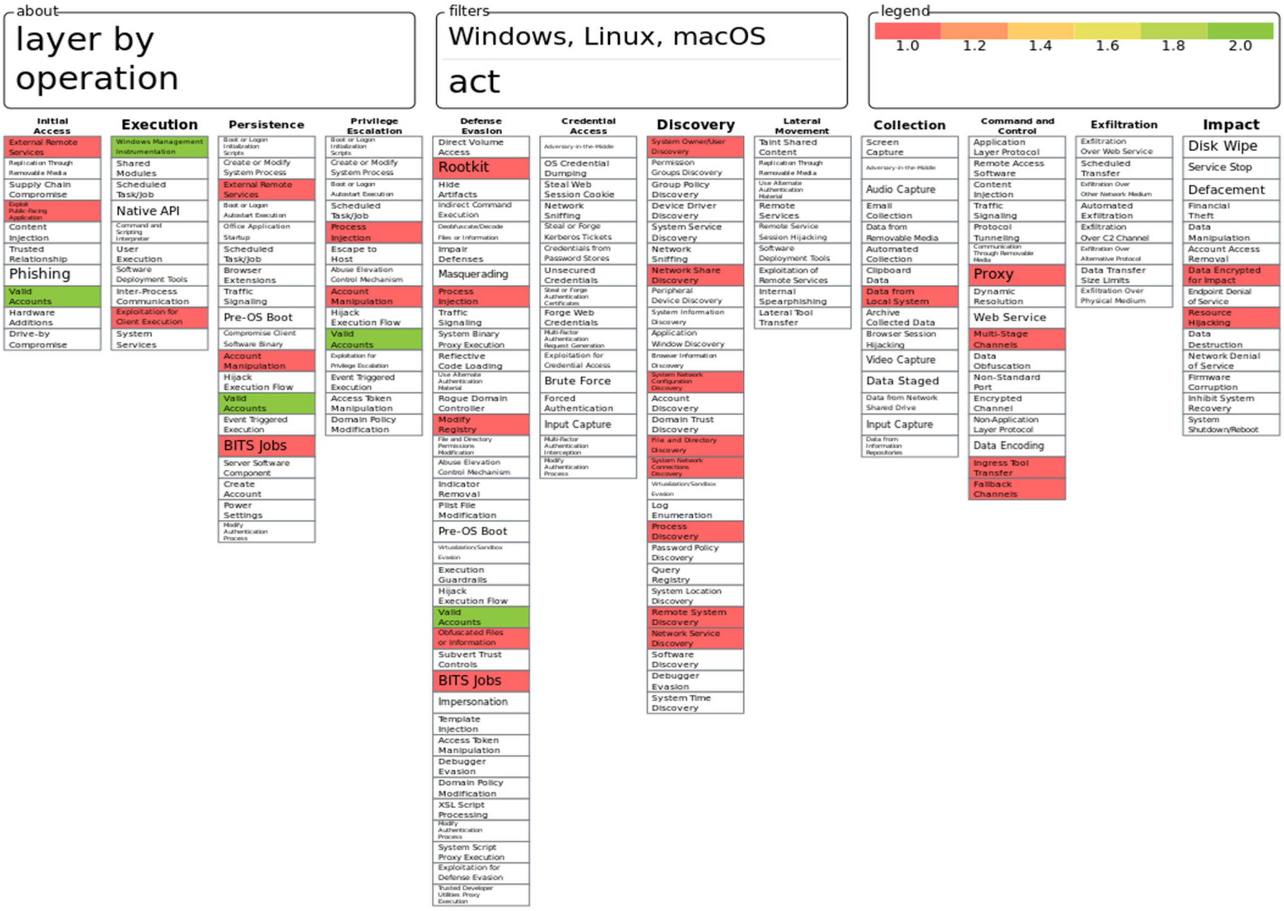
To distill the complexity of the attacks into a structured format, we developed a TTP ontology. This process highlighted the abstract concepts within the attack patterns, such as vulnerabilities exploited and potential paths an attacker could employ to evade detection.

Drawing from our ontological analysis, we designed a TTP chain that organizes cybersecurity data into actionable intelligence. Taxonomy is intended to facilitate quick and informed decision-making for cybersecurity analysts.

Finally, we formulated a Course of Action Matrix to provide healthcare organizations with potential strategies to detect, prevent, and counteract adversarial actions at each stage of the Cyber Kill Chain, thereby bolstering their defensive capabilities.

4. Defensive Gap Assessment

Ideally, an organization would protect against all threat actors within the MITRE ATT&CK framework, but it is more practical to prioritize those that pose a direct threat to your specific data and systems. Allocating resources across all adversary groups is resource-intensive and may not align with a cost-benefit analysis. Focusing on the most relevant threats enables a more efficient and tailored security strategy.



In the above figure, we have provided the TTPs used by APT actors targeting health care organizations allowing the healthcare organization to conduct Defensive Gap assessment. This will empower healthcare organizations to pinpoint which tactics and techniques of those adversary groups they are currently equipped to detect and which remain blind spots. By understanding the specific TTPs used by FIN4, Deep Panda, and APT41, healthcare organization can direct their resources towards bolstering defenses where they are most vulnerable, thereby adopting a proactive and focused security posture. This targeted defense strategy, inspired by the principles of knowing one's capabilities and adversary's methods as advocated by Sun Tzu.

3. Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) is information that enables an organization to respond to cyber threats in a proactive and timely manner. Cyber Threat Intelligence (CTI) equips security operators with essential information to safeguard against cyber threats and respond effectively to attacks . When organized in a structured manner, we can utilized it with automated tools and for threat hunting and analysis. The Diamond Model, which consists of four components the adversary, victim, capability and infrastructure offers a simplified approach, to understanding complex cyber attacks (Chapman et al., 2011). This model provides us with an effective framework for comprehending the dynamics of cyber threats and their impact, on targets. In order to aid our understanding of the steps taken by attackers to achieve their objectives, Lockheed Martin created a Cyber Kill Chain which outlines the sequence of activities that adversaries need to complete in order to successfully compromise a system. By combining these two modeling styles, we can present a visual representation of adversary activity (Taylor et al., 2018).

- **Component of a Diamond model**

The Diamond model consist of four components:

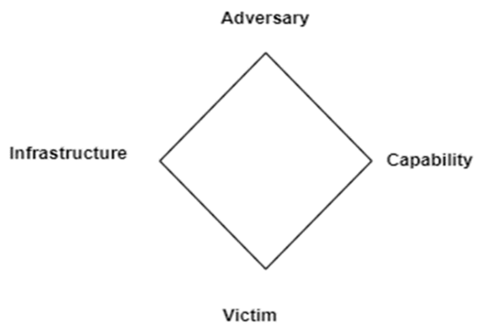


Figure 1 Diamond Model (Adopted from [3])

1. **Adversary:** the adversary component refers to the individual, group, or organization responsible, for carrying out an attack. Here we focus on understanding their identity, capabilities, motivations, and intentions. This understanding is vital in determining who the adversary is, their objectives, and how skilled they are which in turn helps us in defending against their attacks.

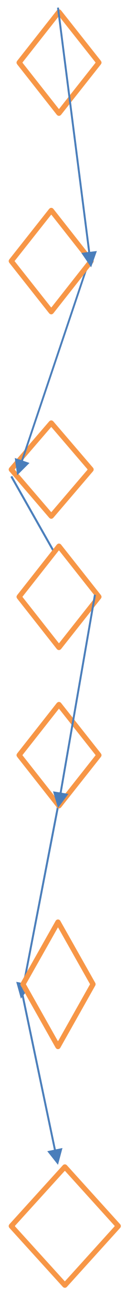
2. **Capability**: This component refers to the tools, techniques and resources employed by the adversary to execute their attacks. It allows us to gain insights into the types of malware utilized by these persistent threat (APT) groups, their tactics and the methods they employ to exploit vulnerabilities, within a target system.

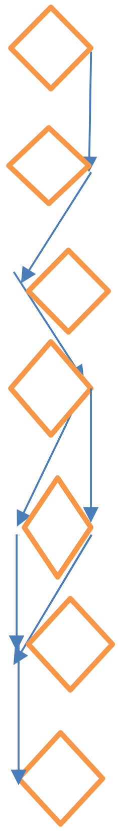
3. **Infrastructure**: the infrastructure component refers to the physical and digital means by which attackers utilized to conduct their attacks. This includes command and control (C2) servers, domains, IP addresses, network assets used by APT groups to execute their attacks as well as any additional potential attack vectors identified during analysis of infrastructure assets.

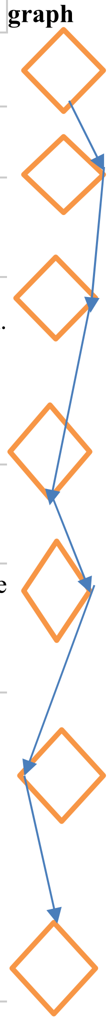
4. **Victim**: The victim component refers to the target of the attack. It can be an individual, an organization, or a system. This component helps us examine the victim's vulnerabilities that were exploited, the impact of the attack, and the data or assets compromised. Understanding the victim is crucial for improving defenses and for response and recovery efforts.

4. Threat Modeling

Threat modeling is a systematic method of identifying, prioritizing, and addressing potential security threats. For each APT groups we have identified their complete attack pattern expression by mapping their threat actions and TTPs to The Cyber Kill Chain. The diamond model is used as activity threat graph to identify the adversaries, their capabilities and infrastructures

CKC PHASE	**Activity**	**Activity attack graph**
Reconnaissance	This is where adversaries are gathering information on targets to prepare for an attack. • External Remote Services (APT41 compromised an online billing/payment service using VPN access). • Network Service Discovery (Conducted port scans). • Network Share Discovery (Used for network reconnaissance).	
Weaponization	This phase involves creating remote access malware weapons tailored to the target. • Access Token Manipulation (BADPOTATO exploit used for local privilege escalation). • Account Manipulation (Added user accounts for access). • Application Layer Protocol (Used HTTP, FTP, DNS for initial payload download). • Archive Collected Data (Data packaging for exfiltration).	
Delivery	How the weapon is transmitted to the victim. • BITS Jobs (Used BITSAdmin to download and install payloads).	
Exploitation	This phase takes advantage of a vulnerability. • Exploit Public-Facing Application (Exploited CVEs for initial access). • Exploitation for Client Execution (Leveraged exploits for execution on clients). • Exploitation for Privilege Escalation (Abused named pipe impersonation for privilege escalation).	
Installation	Installing malware on the victim's system for persistence. • Boot or Logon Autostart Execution (Created and modified startup files for persistence). • Create or Modify System Process (Modified Windows services to install malware backdoors).	
Command and Control (C2)	This phase involves establishing a command and control channel to control the malware remotely. • Exfiltration Over C2 Channel (Used Cloudflare services C2 channels for data exfiltration). • Exfiltration Over Web Service (Used Cloudflare services for data exfiltration). • Fallback Channels (Used Steam community page as a fallback for C2). • Multi-Stage Channels (Used BEACON backdoor to download secondary backdoor).	
Actions on Objectives	This is where the adversary achieves their end goal. • Data Encrypted for Impact (Used ransomware for impact). • Data from Local System (Uploaded files and data from compromised host).	

CKC PHASE	**ATIVITY**	**Activity Attack Graph**
Reconnaissance	This phase typically involves collecting information that will facilitate the attack. • Process Discovery (Uses Tasklist utility to list processes). • Remote System Discovery (Used ping for identifying machines).	
Weaponization	This phase involves creating a deliverable malicious payload. • Obfuscated Files or Information: Indicator Removal from Tools (Updated and modified malware).	
Delivery	The phase where the attacker transmits the weapon to the victim. • Command and Scripting Interpreter: PowerShell (Used PowerShell scripts to download and execute programs).	
Exploitation	Taking advantage of vulnerabilities or features to execute code. • System Binary Proxy Execution: Regsvr32 (Used regsvr32.exe to execute malware).	
Installation	Setting up a persistent presence on the victim's system. • Server Software Component: Web Shell (Uses Web shells for persistent access). • Event Triggered Execution: Accessibility Features (Sticky-keys technique for persistence).	
Command and Control (C2)	Establishing a channel to control the malware and possibly exfiltrate data. • Windows Management Instrumentation (WMI used for lateral movement, which often includes C2 activities).	
Actions on Objectives	Conducting actions to achieve their end goals. • Remote Services: SMB/Windows Admin Shares (Uses net.exe for network share access). • Hide Artifacts: Hidden Window (Used to conceal PowerShell windows).	

CKC PHASE	**Activity**	**Activity Attack graph**
Reconnaissance	Seeking information about the target to prepare for an attack. • Email Collection: collect victims email	
Weaponization	The creation of malware designed to exploit the victim's system. • Command and Scripting Interpreter: Visual Basic (Used VBA macros).	
Delivery	Sending the weaponized bundle to the victim. • Phishing: Spearphishing Attachment (Spearphishing with attachments). • Phishing: Spearphishing Link (Spearphishing with malicious links).	
Exploitation	Taking advantage of a vulnerability or feature to execute code on the victim's system. • Application Layer Protocol: Web Protocols (Used HTTP POST requests). • User Execution: Malicious Link (Lured victims to click malicious links). • User Execution: Malicious File (Lured victims to launch malicious attachments).	
Installation	Installing malware to maintain presence on the victim's system. • the use of VBA macros and keylogging suggests that FIN4 may have installed malicious software as part of their operations.	
Command and Control (C2)	Managing a connection back to the attacker's infrastructure to control the malware and possibly exfiltrate data. • Proxy: Multi-hop Proxy (Used Tor for anonymizing login to victim's email).	
Actions on Objectives	Performing actions to achieve their goals, such as data theft or disruption. • Email Collection: Remote Email Collection (Accessed and hijacked email communications). • Hide Artifacts: Email Hiding Rules (Created Outlook rules to hide their activities). • Input Capture: Keylogging (Captured credentials via keylogging). • Input Capture: GUI Input Capture (Collected credentials through spoofed prompts). • Valid Accounts (Used legitimate credentials for hijacking email communications).	

5. TTP Ontology Graph

The necessity for up-to-date information is crucial for cybersecurity experts to effectively carry out their responsibilities. The increasing complexity and economic importance of cybersecurity have resulted in a rise, in the amount of threat information available, making its management and practical application more challenging. As a result it is crucial to make efforts to organize cybersecurity data systematically to support the work of analysts and automated systems in this expanding field (Iannacone et al., 2015).

One essential step in building a knowledge graph for cybersecurity involves developing an ontology. This ontology includes concepts like vulnerabilities, attackers, attack patterns and the consequences of these attacks. It acts as a tool for representing, consolidating and sharing cybersecurity information while also providing a set of terms, within the domain of information security (Li et al., 2023).

To address Tactics, Techniques and Procedures (TTPs) employed by APT groups FIN4, Deep Panda and APT41 we have created a cybersecurity ontology. This ontology systematically. Structures the characteristics and methods used by these groups to provide a clearer understanding of their attack strategies.APT41 Ontology Graph

The ontology for APT41 illustrates a sophisticated series of interlinked cyberattack strategies and potential actions adversaries may perform following one another, starting from initial access through SQL injection and spear-phishing. It demonstrates how each completed action can be a gateway to further malicious activities, such as deploying ransomware or establishing persistent access. The sequence of actions reflects APT41's ability to exploit vulnerabilities, steal credentials, masquerade their presence, and exfiltrate data to C2 servers.

Figure 4. APT41 TTP Ontology

or to log into the victim's accounts using anonymizing services like Tor. The attacker's actions end in the encryption of data and exfiltration to a command and control server, illustrating a multi-stage cyberattack aimed at information theft and espionage.

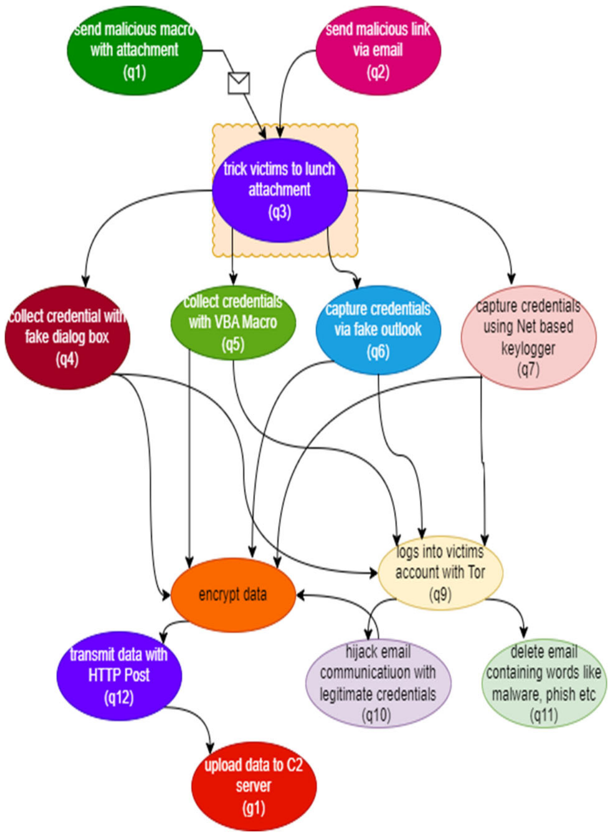


Figure 5. FIN4 TTP Ontology

This ontology illustrates how FIN4 target healthcare organizations through social engineering tactics, primarily via email. After tricking victims to engage with a malicious macro attachment or link, the attacker moves on to credential harvesting through various methods, including fake dialog boxes and fake Outlook login screens. These credentials can then be leveraged to hijack legitimate email communications

The ontology for Deep Panda captures a series of interconnected actions, reflecting the attacker's ability to progress from one technique to the next. Initiating with reconnaissance, the attacker can progress to compromising the network using web shells, then systematically evading detection. Subsequent steps involve exploiting system features for access and lateral movement within the network, all converging towards deploying ransomware and exfiltrating data to a command and control server.

Figure 6. Deep Panda Ontology

5. Cyber Threat Intelligence Report

Cyber threat intelligence (CTI) reports are unstructured text reports written by experts to describe an attack (e.g., malware or APT) based on deep analysis. Based on the analyzed APTs in this paper, we have generated (CTI) reports for the three APT actors targeting the Health Care organizations. These reports serve as a strategic blueprint for healthcare organizations in bolstering their defenses against FIN4, APT41, and Deep Panda actors. Utilizing the detailed information within these reports, the healthcare security specialist can configure firewall rules to block known malicious traffic patterns. Moreover, red teams can leverage the insights to emulate real-world attacks, testing the robustness of current security measures. By simulating the TTPs of these APT groups, healthcare organizations can critically assess and refine their defense mechanisms, ensuring that their cybersecurity infrastructure can withstand actual attack scenarios.

We developed a TTP ontology for creating cyber threat intelligence reports that categorize the APT groups Tactics, Techniques, and Procedures in a structured manner. This transforms the analysis of cyber threats into actionable intelligence, facilitating healthcare organizations in deploying effective and efficient countermeasures. Leveraging these insights, healthcare organizations can enhance firewall configurations, empower red teams to emulate threat actors for testing their security measures, and configure their intrusion detection systems with signatures patterns of adversary behavior. This can enable the Healthcare organizations to respond to cyber threats in a proactive and timely manner

APT41 Cyber Threat Intelligence Report

ID	Technique	Tactic	What (Action)	Where (Object1)	Relation	Where (Object2)	Manner (Tools)	When (Pre-condition)	Why (intent)
T1071	Application Layer Protocol	Command and Control	use	HTTP protocol	to	Download malware	User action	User receives email	Gain access
T1560	Archive	Exfiltration	archive	collected data	using	RAR utility	User action	User receives email	Trick user to click on malicious link
T1547	Boot or Logon Autostart Execution	Persistence	modify	startup files	of	operating system	Remote access tool	Victim's credentials are collected	Collect sensitive communications
T1134	Access Token Manipulation	Privilege Escalation	manipulate	access token	using	BADPOTATO exploit	Configuration change	Access to victim's email client	Hide malicious activities
T1543	Create or Modify System Process: Windows Service	Persistence	Create	Windows Service	using	Malware	Discretely	Administrative Access	Maintain Access
T1071	Application Layer Protocol: Web Protocols	Command and Control	Communicate	C2 Server	Using	Web Protocol	Via HTTP/HTTPS	Network Reachability	Control Compromised System
T1560	Archive Collected Data: Archive via Utility	Exfiltration	Package	Collected Data	Using	RAR/ZIP	Covertly	Data Harvested	Prepare for Exfiltration
T1547	Boot or Logon Autostart Execution	Persistence	Configure	Autostart Mechanism	With	Malware	Automatically	System Startup	Ensure Persistence

6. Recommendation for Mitegation

This Course of Action matrix provides a structured approach for healthcare organizations to consider when planning their defense strategies against these specific APT groups. It aligns with the actions of detect, deny, disrupt, degrade, deceive, and destroy from DoD information operations doctrine. Each column represents a phase in the cyber kill chain, and each row under the APT group columns represents potential mitigation strategies or actions to take in response to the identified threats.

Cyber Kill Chain Phase	**Action**	**FIN4**	**Deep Panda**	**APT41**
Reconnaissance	Detect	Threat Intelligence Analysis	Advanced Network Analytics	Continuous Network Monitoring
	Deny	-	-	-
	Disrupt	-	-	-
	Degrade	-	-	-
	Deceive	-	-	-
	Destroy	-	-	-
Weaponization	Detect	Email Scanning	Application Whitelisting Alerts	Endpoint Protection Alerts
Delivery	Detect	Phishing Detection Systems	Suspicious Traffic Isolation	Spear-Phishing Detection Systems
	Deny	User Training and Email Filtering	Proxy Filtering	Email Filtering
	Disrupt	User Awareness Training	-	Targeted User Training
	Degrade	-	-	Network Segmentation
	Deceive	-	Honeypot	Decoy Email Accounts
	Destroy	-	-	-
Exploitation	Detect	Patch Management Verification	Host Intrusion Detection Systems	SIEM Alerts
	Deny	Patching Software Vulnerabilities	Patch Distribution Enforcement	Vulnerability Scanning and Patching
	Disrupt	Data Execution Prevention	-	Privilege Restriction
	Degrade	-	Data Execution Prevention	-
	Deceive	-	Fake Network Shares	-
	Destroy	-	-	-
Installation	Detect	Log Monitoring	Log Monitoring	Log Monitoring
	Deny	Application Whitelisting	Application Control	Application Whitelisting
	Disrupt	-	Endpoint Malware Protection	-
	Degrade	-	-	-
	Deceive	-	-	Decoy Systems and Services
	Destroy	-	-	
C2	Detect	Network Intrusion Detection Systems	Network Intrusion Detection Systems	Network Intrusion Detection Systems
	Deny	Firewall ACLs	Firewall ACLs	Firewall ACLs
	Disrupt	DNS Filtering	-	Real-time SIEM Response
	Degrade	-	-	-
	Deceive	-	DNS Sinkholes	-
	Destroy	-	-	-
Actions on Objectives	Detect	Audit Log Analysis	Audit Log Analysis	Audit Log Analysis
	Deny	Encryption	Encryption	Encryption
	Disrupt	-	Queuing	-
	Degrade	-	-	-
	Deceive	-	DNS Sinkholes	-
	Destroy	DNS Sinkholes	-	Adaptive Zone Defence

7. Conclusion and Feature Work

This study offers a modeling of three Advanced Persistent Threat (APT) groups FIN4, APT41, and Deep Panda focusing on their attack tactics against the healthcare sector. We have proposed a set of methodologies for thorough TTP investigations that result in actionable cyber threat intelligence. We aimed to mitigate risk exposure within healthcare organizations by providing up-to-date insights into these APT TTPs and highlighting vulnerabilities and potential attack vectors. This enables a strategic allocation of defensive resources.

By implementing our findings, healthcare organizations are better positioned to refine firewall configurations, conduct red team exercises to simulate these APT attacks to test their security posture, and enhance intrusion detection systems with these signatures to recognize adversarial behavior. Our study ends with a recommendations presented in a Course of Action Matrix, offering mitigation strategies against each APT group, guiding healthcare entities to adopt a proactive defense posture.

The analysis identified that different APT groups have distinct motive; for instance, FIN4 is primarily driven by the theft of credentials and sensitive information. Therefore, vigilant monitoring for keylogging attempts is crucial to prevent FIN4's ambitions. Additionally, user awareness training is imperative to counter social engineering tactics, a common initial vector for such threats.

For APT41, whose strategy often includes payloads encryption to download malware for advancing their attacks, the deployment of stateful inspection firewalls has been suggested as an effective countermeasure.

Looking ahead, future research should embark on a detailed analysis of all known and emerging APT actors, continually investigating their up-to-date TTPs . This ongoing process is vital to stay abreast of the ever-changing cyber threat landscape, ensuring that organizations can swiftly adapt and fortify their defenses against the APT actors.

References

[1] F. Gioulekas et al., “A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures,” Healthcare, vol. 10, no. 2, p. 327, Feb. 2022, doi: 10.3390/healthcare10020327.

[2] Mucaraku, L., & Ali, M. (2022). Importance of Information Systems in the Healthcare Sector. In 2022 International Conference on Computing, Electronics & Communications Engineering (iCCECE) (pp. 112-117). Southend, United Kingdom. doi:10.1109/iCCECE55162.2022.9875083.

[3] Pandey, A. K., et al. (2020). Key Issues in Healthcare Data Integrity: Analysis and Recommendations. IEEE Access, 8, 40612-40628. doi:10.1109/ACCESS.2020.2976687

[4] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. Healthcare (Basel), 8(2), 133. doi:10.3390/healthcare8020133. PMID: 32414183; PMCID: PMC7349636.

[5] CBS Interactive. (2023, August 4). Cyberattack causes multiple hospitals to shut emergency rooms and divert ambulances. CBS News. https://www.cbsnews.com/news/prospect-medicalcyberattack-california-pennsylvania-hospital/.

[6] Barlow, E. (2021, June 3). Attacks on Healthcare Industry Continue to Thrive, despite Increased Security Measures. SecurityHQ. https://www.securityhq.com/blog/attacks-on-healthcareindustry-continue-to-thrive-despite-increased-security-measures/.

[7] HealthITSecurity. (2022, September 2). Biggest Healthcare Data Breaches Reported This Year, so Far. http://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-sofar#:~:text=The%20healthcare%20sector%20suffered%20about.

[8] IBM. (2019, November 25). Cost of a Data Breach Report. https://www.ibm.com/downloads/cas
Al-Mohannadi, H., Awan, I., & Al Hamar, J. (2020). Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence. SOCA 14, 175–187. DOI: https://doi.org/10.1007/s11761-019-00285-7.

[9] Atapour, C., Agrafiotis, I., & Creese, S. (2018). Modeling Advanced Persistent Threats to enhance anomaly detection techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 9(4), 71–102.

[10] Bahrami, P.N., Dehghantanha, A., Dargahi, T., et al. Cyber Kill Chain Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures. Journal of Information Processing Systems, 15(4), 865-889. DOI: 10.3745/JIPS.03.0126.

[11] Caltagirone, S., Pendergast, A., & Betz, C. (2013). The diamond model of intrusion analysis. Threat Connect, 298(0704), 1-61.

[12] Chapman, I. M., Leblanc, S. P., & Partington, A. (2011, April). Taxonomy of cyber attacks and simulation of their effects. In Proceedings of the 2011 Military Modeling & Simulation Symposium (pp. 73-80).

[13] Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15 (pp. 63-72). Springer Berlin Heidelberg.

[14] Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24(1), 31-43.

[15] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), 80.

[16] Lampis AlevizosMax Hashem Eiza, Vinh Thong TaQi Shi & Janet Read. (2022). Blockchain-Enabled Intrusion Detection and Prevention System of APTs Within Zero Trust Architecture. IEEE Access 10, 89270-89288.

[17] Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. Computers & Security, 72, 26-59.
MITRE. "MITRE ATT&CKTM." Mitre.org, 2023, attack.mitre.org.

[18[Taylor, P. J., Dargahi, T., & Dehghantanha, A. (2019). Analysis of apt actors targeting IoT and big data systems: Shell_crew, nettraveler, projectsauron, copykittens, volatile cedar and transparent tribe as a case study. Handbook of big data and iot security, 257-272.

[19] Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. (2016, March). Advanced persistent threats: Behind the scenes. In 2016 Annual Conference on Information Science and Systems (CISS) (pp. 181-186). IEEE.

[20] Virvilis, N., & Gritzalis, D. (2013, September). The big four-what we did wrong in advanced persistent threat detection?. In 2013 international conference on availability, reliability and security (pp. 248-254). IEEE.

[21] Iannacone, M., Bohn, S., Nakamura, G., Gerth, J., Huffer, K., Bridges, R., ... & Goodall, J. (2015, April). Developing an ontology for cyber security knowledge graphs. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference* (pp. 1-4).

[22] Li, H., Shi, Z., Pan, C., Zhao, D., & Sun, N. (2023). Cybersecurity knowledge graphs construction and quality assessment. *Complex & Intelligent Systems*, 1-17.