Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume II, 107-113

Leveraging YARA and Sigma Rules to Detect Chinese State-Sponsored Hacking Groups of the "Typhoon" Type

Dimitar Dimitrov
IT Department
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
dimitar@nvna.bg

Dimitar Nikolov
IT Department
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
d.nikolov@naval-acad.bg

Abstract – This study addresses the escalating cyber threat posed by Chinese state-sponsored hacking groups, particularly the "Typhoon" class (Salt Typhoon and Volt Typhoon) which target critical infrastructure through stealthy and persistent techniques. The research aims to enhance detection capabilities against these advanced persistent threats by analysing their tactics, techniques, and procedures and by developing YARA and Sigma rules. The methodology involves mapping observed TTPs to MITRE ATT&CK and designing detection rules that identify key indicators of compromise in both system files and event logs. The main contribution of the study is the implementation of rule-based detection mechanisms that proactively uncover malicious activities often missed by traditional signature-based tools.

Keywords – China, Cyberspace, Salt Typhoon, Sigma rules, Volt Typhoon, YARA rules

I. INTRODUCTION

Cyber threats have become an undeniable reality in the modern digital landscape, with state-sponsored groups playing a critical role in cyber-espionage, sabotage and information warfare. Among the most concerning threats are those originating from Chinese state-sponsored advanced persistent threat groups, which have been implicated in large-scale cyber operations targeting government agencies, critical infrastructure, military entities and private sector organizations across the globe. These groups operate with significant resources, advanced technical capabilities and a strategic focus on long-term objectives, allowing them to execute sophisticated and persistent cyber campaigns. Chinese advanced persistent threat (APT) groups employ a wide range of tactics, techniques and procedures that include credential theft, supply chain compromises, data exfiltration and stealthy network intrusions that remain undetected for extended periods. Their operations align with China's broader geopolitical, economic and military ambitions, making them a persistent and evolving cyber threat.

Within this landscape, the "Typhoon" class of Chinese APTs, particularly Volt Typhoon and Salt Typhoon, has emerged as a significant concern. These groups are distinguished by their emphasis on stealth, persistence and operational security, leveraging advanced techniques to maintain access to victim networks while avoiding detection. Volt Typhoon, for example, has been observed targeting critical infrastructure, including communications networks, energy providers and transportation systems. Rather than relying on traditional malware, this group primarily uses "living off the land" techniques, meaning it exploits built-in system tools and legitimate network functionalities to conduct attacks, making detection exceptionally difficult. Similarly, Salt Typhoon has demonstrated a high degree of adaptability, frequently shifting tactics and using highly customized toolsets to evade security defenses. The ability of these groups to persist within networks for months or even years highlights the inadequacy of traditional security measures and underscores the need for more advanced detection methodologies.

The nature of advanced persistent threats like Volt Typhoon and Salt Typhoon presents a considerable challenge to conventional cybersecurity defenses. Traditional signature-based detection methods, such as antivirus solutions and intrusion detection systems, rely on identifying known malicious signatures, hashes, or predefined attack behaviours. However, Chinese APT groups increasingly employ evasion techniques that render these detection methods ineffective. Their ability to blend

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol2.8617

into normal network traffic, use compromised credentials and exploit legitimate system functions makes it difficult for traditional security tools to recognize their presence. Also, these APTs operate with a long-term strategic mindset, often establishing persistent footholds in networks, allowing them to conduct reconnaissance, data exfiltration and system manipulation over extended periods. Given these challenges, there is a growing need for pattern-based detection mechanisms that focus on behavioural analytics rather than static signatures. Unlike traditional signature-based defenses, pattern-based detection methodologies such as those implemented using YARA [1] and Sigma rules enable security teams to identify suspicious activity based on contextual indicators, anomalous system behaviour and tactics, techniques and procedures (TTPs) associated with APT groups. YARA rules, for instance, are widely used for malware classification and allow analysts to define heuristics that match characteristics of malicious files and processes. By leveraging these rule-based detection methods, organizations can improve their ability to detect and respond to Chinese APT activities proactively.

One of the primary objectives of this study is to conduct analysis of the tactics, techniques and procedures used by Typhoon APT groups. By examining their attack methodologies, exploitation techniques, command and control infrastructures and persistence mechanisms, this research aims to provide a structured understanding of their operational behaviours. This analysis will be mapped to established threat intelligence frameworks such as MITRE ATT&CK to contextualize their activities within the broader cyber threat landscape. Understanding these TTPs is crucial for developing effective countermeasures, as it allows security teams to anticipate potential attack vectors and enhance their defensive capabilities. Additionally, this study will focus on the development and implementation of YARA and Sigma rules to improve threat detection capabilities against these APT groups. Traditional signature-based detection methods often fail to identify the stealthy and adaptive techniques used by Typhoon APTs. To address this challenge, this research will design customized YARA and Sigma rules that target specific behavioural indicators associated with these groups.

II. MATERIALS AND METHODS

YARA, introduced in 2008 by Victor Álvarez of VirusTotal [2], was originally designed to assist malware analysts in classifying threats through flexible, rule-based signatures. Unlike hash-based antivirus solutions, YARA enabled the definition of heuristic patterns such as byte sequences or strings offering adaptability to emerging malware variants. Its open source nature let to rapid adoption within the cybersecurity community, evolving from a research tool into a cornerstone of forensic investigations, threat hunting and real time detection by the mid-2010s. Key developments, including integration with tools like Volatility and the addition of parsing modules for PE and executable and linkable format (ELF) files, enhanced its capability to dissect complex threats. Over the years, YARA [3] has evolved into a critical component of malware analysis, forensic investigations and advanced threat detection. It has been integrated into security solutions such as endpoint detection and response (EDR), intrusion detection systems (IDS) and network traffic analysis tools. These integrations enable security analysts to conduct deep malware scans on endpoints, detect malicious activity within network traffic and perform forensic analysis on compromised systems. Given that Typhoon APT groups frequently use custom malware and advanced obfuscation techniques, YARA rules serve as a vital detection mechanism, allowing defenders to identify malicious payloads even when traditional antivirus solutions fail.

YARA operates by scanning files, memory and process execution data for predefined signatures that match known malware characteristics. These signatures are structured using logical conditions, metadata and string patterns, allowing for a highly granular approach to malware detection. Security researchers develop YARA rules by analyzing malware samples, extracting distinguishing byte sequences and defining detection parameters that minimize false positives while maintaining high accuracy.

In the context of state-sponsored cyber threats [4], YARA is critical for identifying sophisticated malware that exhibits polymorphic or stealthy behaviours. APT groups such as Volt Typhoon use advanced obfuscation techniques, fileless malware and encrypted command-and-control (C2) communications to evade detection. YARA rules can be tailored to detect not only static file signatures but also behavioural markers, memory-resident threats and unique encryption algorithms used by such adversaries. By applying these rules within forensic investigations, security teams can identify malware variants linked to specific threat actors, enabling effective countermeasures and attribution.

In the context of Typhoon type of APTs, YARA rules provide a robust framework for detecting the stealthy malware by enabling analysts to define tailored heuristics that address specific characteristics of these threats. These rules can target unique byte sequences or API calls embedded within malware payloads, such as those used by Volt Typhoon to inject code into legitimate processes. Additionally, YARA excels at identifying encryption methods and obfuscation techniques, which are hallmarks of Chinese APT operations designed to thwart reverse-engineering efforts. For example, rules can be crafted to detect proprietary C2 encryption algorithms or memory-resident artifacts like those deployed by Salt Typhoon to maintain persistent access by scanning process memory or network traffic for anomalous patterns. By focusing on these granular indicators, YARA bridges the gap left by traditional defenses, offering a proactive means to pinpoint malware variants that evade conventional detection systems. Beyond static analysis, YARA's application extends to uncovering broader indicators of compromise associated with Typhoon APTs, enhancing both forensic investigations and real-time threat hunting. Rules can be designed to identify malicious processes, registry

modifications, or behavioural markers such as Volt Typhoon's use of wmic process call create for remote execution providing a comprehensive view of an adversary's footprint. This capability is particularly valuable in detecting memory-only implants, which lack disk-based signatures and require memory forensics to expose.

A. UNDERSTANDING SIGMA RULES

Sigma rules represent a transformative approach to threat detection by providing a standardized, YAML-based framework that enables security analysts to define detection logic applicable across diverse Security Information and Event Management (SIEM) platforms. Introduced in 2017 by Florian Roth and Thomas Patzke [5], Sigma addresses the heterogeneity of SIEM query languages by offering a vendor-neutral format that can be translated into dialects such as Splunk's Search Processing Language (SPL), ElasticSearch's Event Query Language (EQL) and Kibana Query Language (KQL), Microsoft Sentinel's Kusto Query Language (KQL), IBM QRadar's AQL and Micro Focus ArcSight's query syntax, among others. This cross-platform compatibility ensures that organizations with varied SIEM deployments common in enterprise settings can implement a unified detection strategy without the need for extensive customization. By leveraging log data from sources such as Windows Event Logs, Sysmon, network traffic and authentication records, Sigma empowers security teams to monitor for early indicators of advanced persistent threat activity, a capability critical to countering the stealthy operations of Chinese state-sponsored groups like Volt Typhoon and Salt Typhoon.

The relevance of Sigma rules is particularly pronounced in detecting the behavioural patterns of Typhoon APTs, which exploit system logs and legitimate functionalities to establish persistence and evade traditional malware-focused defenses. Volt Typhoon, for example, is known to manipulate authentication logs through brute-force attacks or credential dumping, while Salt Typhoon has been observed altering process execution data to facilitate lateral movement within compromised telecommunications networks. Sigma rules enable granular detection of such activities by defining logic that flags anomalies—such as unusual login patterns, suspicious command-line executions. or unexpected registry changes—in real time.

Sigma's real-time monitoring capabilities [6] enhance SIEM effectiveness by correlating disparate log events into actionable intelligence, a critical advantage against the prolonged dwell times characteristic of Typhoon APTs. By integrating with frameworks like MITRE ATT&CK, Sigma rules map detected behaviours to specific TTPs such as persistence (T1090) or discovery (T1087) enabling precise attribution and contextual understanding of adversary actions. This adaptability allows security teams to refine rules based on evolving threat intelligence, reducing false positives and mitigating alert fatigue. For instance, a Sigma rule might correlate a spike in failed logins with subsequent PowerShell execution, a pattern observed in Salt Typhoon's initial access strategies, providing early warning of a potential compromise. When deployed within security operations centers, Sigma's standardized approach streamlines threat hunting across enterprise environments, ensuring that defenders can proactively disrupt the attack lifecycle of sophisticated state-sponsored actors like those driving China's aggressive cyber campaigns

B. Primary distinction between yara and sigma rules

YARA, originally developed as a pattern-matching tool for malware classification and detection, operates at the file, memory and process execution level, making it particularly effective for identifying static and dynamic artifacts associated with APTs [7]. By scanning binary files, memory dumps and running processes, YARA detects predefined signatures that include unique byte sequences, string patterns and API call behaviours, which are essential for identifying malicious code deployed by sophisticated adversaries. YARA's ability to define heuristic-based rules allows cybersecurity analysts to pinpoint these sophisticated attack vectors, even in post-compromise forensic investigations. The flexibility of YARA, which supports complex logical conditions and modular parsing of executable formats, makes it an indispensable tool in threat-hunting frameworks, forensic analysis and automated malware detection within EDR and SOAR platforms.

In contrast, Sigma serves as a log-centric detection framework [8], focusing on the behavioural analysis of system, network and application logs to identify anomalies indicative of cyber threats. Sigma employs a standardized YAML-based format that allows security teams to define platform-independent rules, which can then be translated into specific SIEM query languages to facilitate real-time threat detection. Given its ability to correlate log-based activity across multiple data sources, Sigma enables security analysts to track adversarial TTPs in alignment with frameworks such as MITRE ATT&CK, thereby enhancing its applicability in proactive threat hunting, SOC workflows and automated incident response processes.

Beyond their differing operational domains, YARA and Sigma exhibit distinct technical architectures and application scopes, offering complementary strengths that enhance threat detection when deployed in tandem. YARA's rule-based structure allows analysts to specify precise pattern-matching conditions, including hexadecimal sequences, regular expressions and system API calls, making it highly effective for static and memory-resident malware identification. However, because YARA relies [9] on discrete artifacts physically present or executable within a system, its utility is inherently constrained when it comes to detecting multi-stage attack sequences or adversarial movements across a network. Conversely, Sigma adopts a high-level, event-driven detection methodology, leveraging log correlation,

behavioural analytics and adversary attribution to identify stealthy APT activities across enterprise environments. By analyzing command-line executions, lateral movement attempts and unauthorized authentication patterns [10], Sigma provides a broader operational view that enables security teams to track and mitigate adversarial campaigns in real time.

Together, YARA and Sigma create a synergistic detection and response framework, addressing both forensic and proactive security challenges. YARA provides depth in malware detection, uncovering specific artifacts that indicate the presence of an APT within a system, while Sigma provides breadth in threat hunting, illuminating the adversary's operational footprint across an organization's IT infrastructure. The integration of these tools is essential for countering Chinese state-sponsored Typhoon groups, whose tactics involve blending into legitimate network activity, leveraging compromised credentials and executing LotL techniques to evade detection.

C. Technical overview of Volt typhoon and Salt typhoon

Volt Typhoon and Salt Typhoon are integral components of a broader, coordinated effort by the People's Republic of China to establish strategic dominance in cyberspace. As cyber operations continue to play a critical role in the ongoing US-China strategic competition, these two APTs demonstrate China's evolving cyber warfare strategy, which extends beyond conventional espionage to infrastructure pre-positioning, coercion and power projection. Volt Typhoon primarily focuses on infiltrating and embedding itself within critical infrastructure, ensuring access to essential networks that can be disrupted during geopolitical crises, effectively serving as a deterrent mechanism and a means of strategic leverage. Salt Typhoon, on the other hand, operates within the telecommunications sector, providing China with a comprehensive intelligence-gathering capability while also allowing for the potential disruption of communications in key strategic moments

III. RESULTS AND DISCUSSION

Volt Typhoon, active since at least 2017, primarily targets US critical infrastructure, including telecommunications, energy, transportation and water systems, with a strategic focus on pre-positioning for potential sabotage during geopolitical conflicts, particularly involving Taiwan. Its operations, documented in reports from Microsoft and CISA [11, 12, 13], extend to military bases in Guam and key infrastructure, aiming to disrupt US military mobilization. The group's emphasis on OT systems and SCADA networks, reflects its intent to compromise energy grids and communication hubs, aligning with China's cyber warfare strategy.

The group exploits vulnerabilities in public-facing network appliances, including Fortinet FortiGate firewalls, Ivanti Connect Secure VPNs, Citrix NetScaler and Cisco routers. Often, these attacks leverage known CVEs, such as CVE-2021-40539, while also employing brute-force attacks against administrator accounts with weak or default passwords. By focusing on unpatched systems, Volt Typhoon ensures successful entry into targeted environments. To maintain long-term access within compromised networks, Volt Typhoon utilizes built-in Windows administrative tools, including wmic (Windows Management Instrumentation Command-line), ntdsutil (Active Directory manipulation), netsh (network configuration) and PowerShell. These tools enable the APT to blend into normal system activities, avoiding EDR alerts. Additionally, Fast Reverse Proxy clients are deployed to establish covert command-and-control channels, ensuring continuous remote access to infiltrated systems. Volt Typhoon's use of compromised Small Office/Home Office routers as proxy nodes, creating botnets for relay points to mask network traffic. This tactic complicates attribution and detection efforts, enhancing operational security and amplifying the group's ability to maintain covert footholds. A key aspect of Volt Typhoon's tradecraft is its reliance on Fast Reverse Proxy (FRP) clients to establish covert command-and-control (C2) channels. This technique ensures continuous remote access while obfuscating traffic patterns. Additionally, the group utilizes compromised Small Office/Home Office (SOHO) routers as proxy nodes, creating botnets that relay malicious network traffic through legitimate infrastructure. This tactic significantly complicates attribution and detection, enhancing operational security and resilience against takedown efforts. Upon successfully infiltrating a network, Volt Typhoon employs [14] Remote Desktop Protocol (RDP), VPN tunnels and credential-dumping tools such as Mimikatz to escalate privileges and achieve lateral movement. The group has also been observed leveraging Volume Shadow Copy Service (VSS) for offline password cracking, facilitating deeper penetration into domain controllers and administrative systems. Analysis of historical intrusions suggests that Volt Typhoon often maintains network access for over 300 days before detection, exemplifying its long-term infiltration strategy.

Salt Typhoon, linked to Ministry of State Security of China[15, 16] and active since at least 2022, targets telecommunications infrastructure, focusing on US providers like Verizon, AT&T, T-Mobile and Lumen Technologies, as well as global networks, for long-term espionage. Its operations aim to steal sensitive data, including government communications, law enforcement wiretaps and call logs, aligning with China's intelligence-gathering strategy. It also targets government and technology sectors, compromising political figures' communications, including those from the 2024 US presidential campaigns, reflecting its broad scope [17].

In order to infiltrate, Salt typhoon exploits vulnerabilities in network devices, particularly Cisco routers such as CVE-2018-0171, as well as systems such as

Ivanti Connect Secure VPN - CVE-2023-46805 and CVE-2024-21887, Microsoft Exchange – ProxyLogon and CVE-2021-26855 and Fortinet FortiClient EMS. It frequently targets misconfigured systems and employs spear-phishing and credential harvesting to gain initial entry through public-facing endpoints. This group utilizes PsExec, WMIC and PowerShell for stealthy movement within networks. The deployment of the GhostSpider [18] backdoor enables persistent access, facilitating long-term surveillance. Additionally, the group modifies router configurations, such as altering routing tables, to reroute traffic for espionage, effectively blending its actions with legitimate administrative activity. A critical aspect of their Modus operandi is the ability to capture TACACS, SNMP and RADIUS traffic, extracting authentication details to gain access to privileged accounts, thereby securing long-term operational control over compromised systems. alt Typhoon has demonstrated expertise in modifying router configurations to enable port forwarding and traffic rerouting, allowing for the interception of sensitive communications, including wiretap systems. This capability compromises law enforcement surveillance operations, granting the APT unprecedented access to critical data.

Volt Typhoon's stealth-oriented tactics make traditional security measures ineffective, as they leverage built-in system utilities rather than deploying detectable malware. By using Sigma rules, security teams can identify suspicious behaviours and flag adversarial tactics before they escalate into serious breaches. On fig.1 we present Sigma rule tailored to detect key tactics of Volt Typhoon. NTDS file dumping for credential theft and internal port forwarding for lateral movement and persistence.

The purpose of the rule is to detect abuse of the built-in ntdsutil command-line utility for credential dumping from Windows domain controllers. Adversaries target the Active Directory database (NTDS.dit) because it stores password hashes and other credential data for the entire domain. By creating a copy of this database, often via ntdsutil or Volume Shadow Copy services, attackers can obtain credentials for all users and computers in the domain. The rule's primary goal is to catch any attempt to illicitly copy or export the NTDS.dit file using such built-in tools before an attacker can leverage the stolen credentials.

Detection logic of the rule is to monitor process creation events and command-line parameters indicative of NTDS dumping activity, focusing on ntdsutil, vssadmin and wmic usage. It employs multiple detection selections to cover the variations in how this technique can be executed:

- NTDSutil Invocation - Flags any process execution of ntdsutil.exe with arguments suggesting an Active Directory instance activation and data export. For example, an attacker running ntdsutil "activate instance ntds" ifm "create full C:\Windows\Temp\pro" to generate a copy of the AD database would trigger this rule. Such usage of ntdsutil, often with the "Install From Media" ifm command to create a full NTDS backup, is uncommon outside of planned domain maintenance and is a strong indicator of credential dumping attempts.
- Shadow Copy Creation, VSSAdmin/WMIC - Detects the creation of Volume Shadow Copies via command-line utilities. Adversaries frequently create a shadow copy of the system drive, which contains the AD database, to bypass file locks and copy NTDS.dit safely. This selection looks for commands like vssadmin create shadow /for=C: or the equivalent WMI command, wmic.exe shadowcopy call create Volume=C:\, being executed on a domain controller. The presence of "create" and "shadow" in a process command-line, especially associated with vssadmin.exe or wmic.exe, is a red flag for this technique.
- NTDS.dit File Copying - Monitors for any command-line that attempts to copy or save the NTDS.dit file from its default location to another path. For instance, after making a shadow copy, an attacker might run a command to copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\NTDS\ntds.dit to a local folder. The Sigma rule's logic includes patterns like copy ntds.dit to catch such file transfer attempts. This covers variations of the extraction process, whether using copy, xcopy, or even tools like esentutl, any attempt to read or move the AD database file via command-line.
- Associated Utilities – In some cases, the rule may also watch for use of auxiliary commands such as reg.exe to export the SYSTEM hive, since dumping NTDS alone is not enough, attackers also need the system's registry hive for decrypting password hashes. While the focal point is the ntdsutil/VSS sequence, security logs may show concurrent use of reg save HKLM\\SYSTEM commands, which can be correlated with the NTDS.dit dump attempt.

```
status: experimental
description: Volt Typhoon uses ntdsutil to exfiltrate the ntds.dit file and the SYSTEM registry hive from Windows domain controllers
author: Dimitar Nikolov, Dimitar Dimitrov - Bulgarian Naval Academy
references:
    - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
tags:
    - attack.credential-access #TA0006
    - attack.t1003 #OS Credential Dumping NTDS
logsource:
    category: process_creation
    product: windows
detection:
    selection1:
        CommandLine|contains|all:
            - 'cmd /c vssadmin create shadow /for=C: > C:\Windows\Temp\'
            - 'cmp cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\NTDS\ntds.dit C:\Windows\Temp > C:\Windows\Temp\'
    selection2:
        CommandLine|contains|all:
            - 'wmic process call create "ntdsutil \"ac i ntds\" ifm \"create full C:\Windows\Temp\pro'
    selection3:
        CommandLine|contains|all:
            - 'wmic process call create "cmd.exe /c ntdsutil \"ac i ntds\" ifm \"create full C:\Windows\Temp\Pro"'
    selection4:
        CommandLine|contains|all:
            - 'wmic process call create "cmd.exe /c mkdir C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm \"create full C:\Windows\Temp\tmp\""'
    selection5:
        CommandLine|contains|all:
            - "cmd.exe" /c wmic process call create "cmd.exe /c mkdir C:\Windows\Temp\McAfee_Logs & ntdsutil \"ac i ntds\" ifm \"create full C:\Windows\Temp\McAfee_Logs\""
    selection6:
        CommandLine|contains|all:
            - 'cmd.exe /Q /c wmic process call create "cmd.exe /c mkdir C:\Windows\Temp\tmp & nidsutil \"ac i nids\" ifm \"create full C:\Windows\Temp\tmp\" 1> \\127.0.0.1\ADMIN$\ 2>&1'
    condition: 1 of selection*
falsepositives:
    - Administrative use.
level: high
```

Fig.1. Sigma rule for Volt Typhoon NTDS file dumping

All these detection criteria leverage process creation logs - windows Security Event ID 4688 or Sysmon Event ID 1 with full command-line logging. By correlating events that involve ntdsutil, shadow copy utilities and file copy actions, the rule ensures that multiple methods of

performing an NTDS dump are caught. Notably, Volt Typhoon's tradecraft has involved exactly these patterns - using WMIC to run ntdsutil for an AD database export and vssadmin to create volume shadows which this rule is tailored to detect.

The second rule we created and shown on Fig. 2 is designed to catch the abuse of the Windows netsh interface portproxy command, which attackers use to establish covert internal port forwarding tunnels. Such tunnels effectively turn a compromised host into an internal proxy, allowing adversaries to pivot within a network and maintain persistent access while blending in with legitimate traffic. Chinese state-sponsored groups like Volt Typhoon have been observed using the built-in netsh portproxy utility to create hidden proxies on victim systems as part of their living off the land techniques, enabling lateral movement and stealthy command-and-control (C2) communication without deploying custom malware. By detecting these netsh portproxy commands, the rule aims to alert defenders to the presence of unauthorized internal communication tunnels before attackers can fully leverage them.

Detection Logic of the rule is to monitor Windows process creation logs - Sysmon Event ID 1 or Security 4688 events, for the specific patterns that indicate a port proxy is being configured. In particular, it looks for any process execution of netsh.exe with command-line arguments related to PortProxy setup. The detection logic is broken into several conditions to cover different syntax variants of the netsh portproxy command:

- Standard PortProxy Addition: The command line contains the keywords interface, portproxy, add and v4tov4 together, which is the typical syntax for adding an IPv4-to-IPv4 port forwarding rule. This indicates a new port forwarding rule is being created.
- Abbreviated Command Syntax: Attackers may use abbreviated forms of the netsh command. Netsh allows using just the first letters of subcommands in place of interface portproxy add v4tov4. The rule accounts for this by checking for the sequence of i , p , a , v in the command line, which would appear if the shorthand notation for interface, portproxy, add, v4tov4 is used. This ensures that even non-standard or compact usage of the command is detected.
- Port Proxy Parameters: The presence of port forwarding parameters in the command is another strong indicator. The rule looks for connect, part of connectport and c=, the beginning of a connectaddress= value, in the netsh command line. These tokens appear when a portproxy rule is being defined, for example: listenaddress=0.0.0.0, connectport=3389, connectaddress=10.0.0.5. Detecting these substrings helps catch variations in argument order or spacing, for instance, whether or not an attacker uses quotes or shorthand for the parameters.

```
title: Enable port forwarding on host
status: experimental
description: Volt Typhoon uses the following commands to enable port forwarding on the host
author: Dimitar Nikolov, Dimitar Dimitrov - Bulgarian Naval Academy
references:
    - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
tags:
    - attack.attack.t1090.001 #Proxy: Internal Proxy
logsource:
    category: process_creation
    product: windows
detection:
    selection1:
        CommandLine|contains|all:
            - 'cmd.exe /c "netsh interface portproxy add v4tov4 listenaddress=0.0.0.0 listenport=9999 connectaddress= connectport=8443
protocol=tcp"'
    selection2:
        CommandLine|contains|all:
            - 'cmd.exe /c netsh interface portproxy add v4tov4 listenport=50100 listenaddress=0.0.0.0 connectport=1433 connectaddress='
    condition: 1 of selection*
falsepositives:
    - Administrative use.
level: high
```

Fig.2. Sigma rule for abuse of the Windows netsh interface portproxy

IV. CONCLUSION

This study demonstrates the effectiveness of using YARA and Sigma rules to detect and mitigate the cyber threats posed by Chinese state-sponsored advanced persistent threat groups, particularly Volt Typhoon and Salt Typhoon. By analyzing their tactics, techniques, and procedures and translating them into rule-based detection logic, the research provides concrete tools to improve early threat identification in critical infrastructure networks.

The implementation of custom Sigma rules can successfully identify key adversarial behaviours such as NTDS file dumping and covert port forwarding, which are often used to gain persistence and escalate privileges within compromised systems. Meanwhile, YARA rules can enabled deep inspection of memory and file artifacts, helping analysts detect malware variants and stealthy implants commonly used by Typhoon groups. These detection strategies have shown that combining behavioural log analysis with heuristic-based signature detection significantly enhances an organization's ability to uncover sophisticated intrusions that evade traditional security solutions.

The research confirms that a dual-layered approach, integrating YARA for static and memory-level detection with Sigma for real-time behavioural monitoring, offers a comprehensive defense against advanced state-sponsored cyber threats. The proposed methodology can strengthen the capabilities of security operations centers and threat hunters in detecting, attributing, and responding to the evolving tactics of Typhoon-class APTs.

REFERENCES

[1] Z. Wang, "A systematic literature review on cyber threat hunting," arXiv, 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2212.05310

[2] What Is a YARA Rule?, Oct. 23, 2023. [Online]. Available: https://www.picussecurity.com/resource/glossary/what-is-a-yara-rule. [Accessed: Feb. 18, 2025].

[3] G. Canfora et al., "About the robustness and looseness of Yara rules," ICTSS 2020, pp. 104–120, 2020, https://doi.org/10.1007/978-3-030-64881-7_7.

[4] S. Saeed et al., "A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," Sensors, vol. 23, art. 7273, 2023, https://doi.org/10.3390/s23167273.

[5] What Are SIGMA Rules: Beginner's Guide, May 16, 2022. [Online]. Available: https://socprime.com/blog/sigma-rules-the-beginners-guide/. [Accessed: Feb. 21, 2025].

[6] Introduction to Sigma Rules and Detection of Credential Harvesting, Mar. 8, 2021. [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2021-0308.pdf. [Accessed: Feb. 21, 2025].

[7] K. Yildirim et al., "A YARA-based approach for detecting cyber security attack types," Firat University Journal of Experimental and Computational Engineering, vol. 2, no. 2, pp. 55–68, 2023, https://doi.org/10.5505/fujece.2023.09709.

[8] IDS for Logs: Towards Implementing a Streaming Sigma Rule Engine, Oct. 2020. [Online]. Available: https://ccdcoe.org/uploads/2020/10/Markus-Kont-Mauno-Pihelgas-IDS-for-logs-Towards-implementing-a-streaming-Sigma-rule-engine.pdf. [Accessed: Feb. 22, 2025].

[9] Detecting Malicious Files with YARA Rules as They Traverse the Network, Aug. 7, 2019. [Online]. Available: https://i.blackhat.com/USA-19/Wednesday/us-19-Bernal-Detecting-Malicious-Files-With-YARA-Rules-As-They-Traverse-the-Network-wp.pdf. [Accessed: Feb. 22, 2025].

[10] E. Koleva et al., "Development of an algorithm for calculating the stability of a ship, applied in OBSS," International Journal on Information Technologies and Security, vol. 14, no. 3, pp. 25–36, 2022. [Online]. Available: http://ijits-bg.com/2022.v14.i3.03.

[11] PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, Feb. 7, 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. [Accessed: Feb. 22, 2025].

[12] People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection, May 24, 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a. [Accessed: Feb. 23, 2025].

[13] Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques, May 24, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/. [Accessed: Feb. 23, 2025].

[14] Volt Typhoon and the Disruption of the U.S. Cyber Strategy, Mar. 5, 2024. [Online]. Available: https://www.lawfaremedia.org/article/volt-typhoon-and-the-disruption-of-the-u.s.-cyber-strategy. [Accessed: Feb. 18, 2025].

[15] RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers, Feb. 13, 2025. [Online]. Available: https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices. [Accessed: Feb. 23, 2025].

[16] US Adds 9th Telecom Company to List of Known Salt Typhoon Targets, Dec. 27, 2024. [Online]. Available: https://therecord.media/nine-us-companies-hacked-salt-typhoon-china-espionage. [Accessed: Feb. 20, 2025].

[17] Governments, Telcos Ward Off China's Hacking Typhoons, Dec. 11, 2024. [Online]. Available: https://www.darkreading.com/cyberattacks-data-breaches/governments-telcos-chinas-hacking-typhoons. [Accessed: Feb. 24, 2025].

[18] Salt Typhoon Hackers Backdoor Telcos with New GhostSpider Malware, Nov. 25, 2024. [Online]. Available: https://www.bleepingcomputer.com/news/security/salt-typhoon-hackers-backdoor-telcos-with-new-ghostspider-malware/. [Accessed: Feb. 24, 2025].

[19] Weathering the Storm: In the Midst of a Typhoon, Feb. 20, 2025. [Online]. Available: https://blog.talosintelligence.com/salt-typhoon-analysis/. [Accessed: Feb. 24, 2025].