ISSN 2664-4150 (Print) & ISSN 2664-794X (Online)
South Asian Research Journal of Engineering and Technology
Abbreviated Key Title: South Asian Res J Eng Tech

| Volume-6 | Issue-5 | Sep-Oct- 2024 | **DOI: https://doi.org/10.36346/sarjet.2024.v06i05.004**

Original Research Article

Cybersecurity in Critical Infrastructure: Defending Against Nation-State Groups

Christian Bassey[1*], Success Imakuh[2], Festus Zindozin[3]

[1]Department of Security and Network Engineering, Innopolis University, Russia
[2]Department of Computing, Teesside University, Middlesbrough, United Kingdom
[3]Department of Electrical and Computer Engineering, University of Florida, Gainesville, Florida, United States

***Corresponding Author:** Christian Bassey
Department of Security and Network Engineering, Innopolis University, Russia

Article History
Received: 16.09.2024
Accepted: 21.10.2024
Published: 23.10.2024

Abstract: Cyber-attacks on critical infrastructure can be disastrous and undermine states' national security. Different groups execute these attacks for varying reasons; some may be state-sponsored, and their attack for geopolitical reasons or to achieve strategic national cyber objectives. Regardless of the nation-state actor, it is essential to identify the techniques used and defend critical infrastructure against these attacks. This study evaluated the attack methodology of five nation-state actors based on the MITRE ATT&CK ICS matrix and proposed a multi-layered defense architecture. A virtual organization with critical and enterprise infrastructure domains was created, and the proposed defense architecture and tooling were implemented there. Then, techniques of the nation-state adversaries were emulated against the infrastructure to evaluate the performance of the defense strategies. The results show that the multi-layered approach was sufficient to mitigate all the techniques of the nation-state actors.

Keywords: Critical infrastructure, cybersecurity, nation-state actors, OT/ICS, MITRE, defense.

1. INTRODUCTION

The advances in industrialization, which include automation and digitalization of industrial processes, have brought with it the need to protect these infrastructures from cyber attacks. These infrastructures are crucial for economic, social, and national security. These are known as critical infrastructure. The critical infrastructures of a state are the physical, non-physical, and cyber resources or services that are fundamental to the minimum functioning of a society and its economy (Viganò *et al.*, 2020).

Due to the vital nature of critical infrastructure to a country's national security, adversaries can execute attacks against that infrastructure in cyber warfare campaigns to escalate tensions within the nation. The 2015 Sandworm attack on the Ukrainian electrical grid disrupted electricity supplies from the power grid from one to six hours, depending on location (Pollard, 2024). This attack is an example of the impact cyber-attacks can have on critical infrastructure. Also, due to global interconnectedness in technology, replicating such attacks against other countries by hostile nation-states will have a low barrier to entry. For example, the same type of serial-to-ethernet converters that Ukraine used at the time of the attack are being utilized in the United States power grid (Zetter, 2016).

Cyberattacks are conducted for various reasons. Some reasons may be financial, activist, espionage, or geopolitical reasons. Countries execute cyber attacks against other countries for multiple reasons, such as to shape public opinion, election interference, and other geopolitical concerns. The attack on the Ukrainian power grid was not officially claimed by any threat actor or government. However, the tooling used was attributed to the Sandworm group, and geopolitical circumstances and forensic evidence suggest Russian involvement (Knake, 2017). Sandworm, in particular, has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455 (MITRE.org, 2024a). The groups that execute these attacks may sometimes be officially

attributed, even though publicly attributing cyberattacks to a particular actor remains a core difficulty in cybersecurity, both for law enforcement and nation-states. Also, states use proxy groups to perpetrate cyberattacks, giving them plausible deniability in case of discovery (Baezner, 2018). These groups are referred to as nation-state actors. Nation-state adversaries act on behalf of governments and militaries with significant resources and expertise. They often have dedicated units whose mission is to achieve economic, political, industrial, or military objectives by engaging rivals in cyberspace (Mims, 2017).

Given the impact attacks on critical infrastructure can have and the resources a nation-state actor has access to, it is crucial that critical infrastructure is defended against attacks from these adversaries. The devices and assets classified as critical infrastructure include SCADA, operational technology and industrial control systems (OT/ICS), and other digital assets used in managing or controlling processes deemed critical. The interconnectivity between the enterprise information technology (IT) and industrial control systems (ICS) environment introduces new attack surfaces for critical infrastructure (CI) operators (Malatji *et al.*, 2022). Critical infrastructure security is typically handled as a domain separate from enterprise infrastructure security because it performs functions different from enterprise networks with other requirements, operational priorities, and security considerations. OT/ICS systems are often more vulnerable to cyber-attacks because they are more difficult to patch due to the extreme uptime and reliability requirements of operational systems (Knapp, 2024). However, more damage is incurred when an intrusion occurs in the critical infrastructure domain due to unpatched systems. The uptime requirements and different operational requirements of these systems mean that any downtime in these systems can be catastrophic.

To defend critical infrastructure from nation-state actors, it is crucial to understand the current state of critical infrastructure security, the threats they face, states capable of wreaking cyber havoc, and the techniques state-sponsored actors utilize to breach CI. Voo *et al.*, in the *National Cyber Power Index 2020: Methodology and Analytical Considerations* policy paper, measured the cyber capabilities and intents of 30 countries as they related to their national objectives and provided a ranking of their capabilities and cyber power (Voo *et al.*, 2020).

Pandey *et al.*, identified the risks to cyber-physical systems that often form part of CI in the paper on *Cyber security risks in globalized supply chains: conceptual framework*. Some risks identified include theft of vendor credentials, breach from the vendor network, modification of the source code through malware, plant interruption, loss of availability, and unauthorized access (Patey *et al.*, 2019).

Dawson *et al.*, identified cybersecurity challenges in critical infrastructure, which spread across hacking groups, nation-states, and other actors seeking to manipulate system functions to disrupt regular operations, steal intellectual property, or cause cascading failures. Nation-state actors are exploiting these challenges (Dawson *et al.*, 2021).

In the paper *Cyber-Attacks Against Critical Infrastructure*, Martti Lehto investigated and identified the motivation of CI attackers and the techniques used. These techniques included exploiting system vulnerabilities, leveraging compromised, weak, or stolen credentials, phishing, exploiting misconfigurations, etc. The author identified attacks against critical infrastructure in the critical manufacturing, information technology, financial services, and energy sectors, among others (Lehto, 2022).

This research investigates the techniques used by nation-state actors, performs adversary emulation using their tooling and tradecraft, and then proposes methodologies for defending critical infrastructure from nation-state groups. The paper is structured as follows: Section 2 introduces the materials and methods for investigating critical infrastructure defense. Section 3 implements a virtual organization with critical and enterprise infrastructure domains and then builds a multi-layered defense against nation-state group techniques. Emulation is conducted to identify the effectiveness of the proposed defense system, and section 4 summarizes the paper's findings and hypothesis for future work.

2. MATERIALS AND METHODS

This section proposes an approach to identifying techniques nation-state threat actors use to attack critical infrastructure. We then set about building the technical and conceptual frameworks for performing adversary emulation based on the behavior of the identified nation-state actors.

2.1 Nation-State Threat Groups and Attack Techniques Identification

This work used the existing attribution work done by the MITRE ATT&CK team (mitre.org - Groups, 2024) to identify nation-state actors and their techniques. The matrix used was the ICS ATT&CK matrix. Five nation-state actor threat groups were chosen from a pool of 15 threat actors that target ICS systems for various reasons. Based on the threat actors chosen, their techniques and tactics were identified using the ATT&CK navigator tool.

2.2 Adversary Emulation

Once the state-sponsored threat actors were identified, the tooling and architectures they use for cyber warfare were identified and set up to prepare for executing these attacks while posing as nation-state adversaries against critical infrastructure. Figure 1 below shows the attack path we used as nation-state actors to compromise our fictitious organization and pivot to attacking its critical infrastructure. This attack path is also similar to the one leveraged by these threat groups.

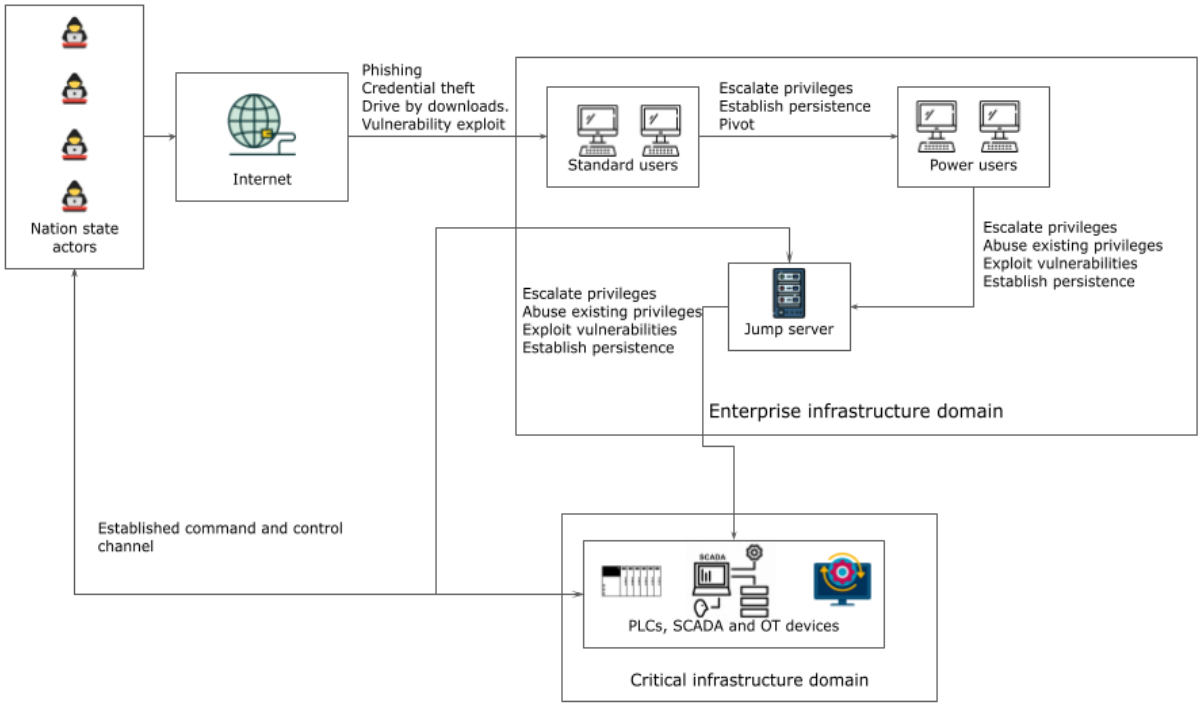

Fig. 1: Nation-state actors attack path

Attacks were executed from a virtual machine running the Kali Linux operating system. It had 2 GB of RAM, 2 vCPUs, and 50 GB of storage space.

2.3 Critical Infrastructure Emulation

A virtual organization with enterprise and critical infrastructure domains was built to emulate the critical infrastructure environment. The virtual organization consisted of the following assets:

Enterprise infrastructure domain:

1. A Windows Active Directory domain controller.
2. One standard non-privileged user Windows workstation.
3. One power privileged user Windows workstation.
4. One Windows server serving as a jump host.
5. One Ubuntu 22.04 Linux server.

Critical infrastructure domain:

1. One Ubuntu 20.04 Linux server serving as a PLC.
2. One CentOS 7 Linux server serving as an OT device.
3. One FreeBSD Linux server serving as a SCADA device.
4. One Windows Active Directory domain controller.

Networking and interconnectivity between devices and the domains are achieved using a Mikrotik router with OS 7.13. The jump host serves as the only source of entry into the critical infrastructure domain from the outside world. All the resources were run on virtual machines in a server farm running Proxmox. Figure 2 shows the theoretical architecture of the emulation environment.

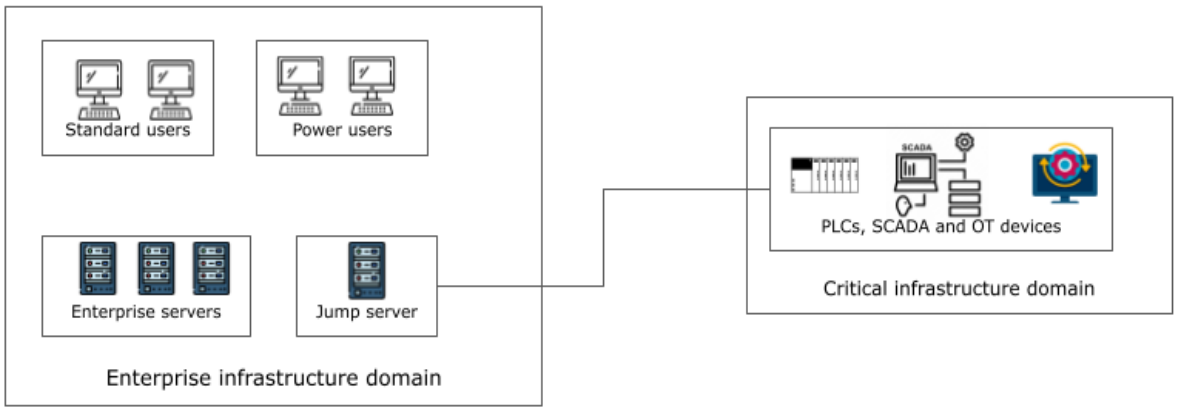

Fig. 2: Emulation theoretical architecture

2.4 Defense Infrastructure

Defense tooling was inserted at various stages of the virtual organization infrastructure to protect against emulated nation-state attacks and detect malicious activity. When evaluating the defense tooling, considerations were made for ease of use, scalability, and licensing, with robust open-source tooling favored above other solutions. Based on these considerations, the defense infrastructure was as follows:

1. Wazuh was chosen as the security information and event management (SIEM) and extended detection and response (XDR) tool.
2. ClamAV, in combination with YARA rules and Wazuh's FIM and XDR, was used for endpoint detection and response (EDR).
3. Mikrotik native firewalls were used for ACLS and firewall management.
4. Suricata was used as the network IDS.
5. Squid was installed as the proxy server.
6. Other security solutions were used on a theoretical basis.

Based on the defense tooling, we propose an approach for defending organizations from nation-state groups and their techniques.

2.5 Safety Precautions

To ensure that our research does not impact the real-world environment, this research was executed in a virtual environment with a dedicated internet connection not used by any other individuals in the laboratory. Additionally, a kill switch was added to the internet infrastructure for ease of termination in the case of escalated scenarios.

3. RESULTS AND DISCUSSIONS

3.1 Nation-State Threat Groups

Based on the attribution work and filtering methodology in section 2.1, the results of the nation-state threat groups, their targets, and their origin country have been listed in Table 1 below.

Table 1: Nation-state threat groups, targets, and origin country

S/N	Group	Targets	Origin country
1.	ALLANITE	Electric utility sector in the United States and the United Kingdom.	Russia (RU)
2.	APT33	Aviation and energy sectors in the United States, Kingdom of Saudi Arabia, and South Korea.	Iran (IR)
3.	CyberAv3ngers	Water, energy, manufacturing, and healthcare in Israel.	Iran (IR)
4.	Dragonfly	Defense, aviation, industrial control system manufacturers, and government entities worldwide.	Russia (RU)
5.	Lazarus Group	Electric grid companies in the United States.	North Korea (NK)

Russia and Iran each had two threat groups, while North Korea was represented by one threat group. The source of the attribution data is the MITRE ATT&CK group website (MITRE.org, 2024b).

3.2 Attack Techniques of the Nation-State Actors

Once the threat groups were identified and attributed to a nation-state, we identified their techniques, tactics, and procedures. Table 2 below shows the tactics and associated techniques used by the nation-state groups to compromise critical infrastructure. The techniques have been grouped based on the tactics.

Table 2: Nation-state actor techniques and state affiliation (MITRE.org, 2024c)

S/N	Tactic	Techniques	Nation-state group
1.	TA0108 - Initial access	T0862 - Supply chain compromise T0865 - Spearphishing attachment T0833 - Internet accessible device T0817 - Drive-by compromise	ALLANITE (RU) APT33 (IR) CyberAv3ngers (IR) Dragonfly (RU) Lazarus Group (NK)
2.	TA0104 - Execution	T0853 - Scripting	APT33 (IR)
3.	TA0110 - Persistence	T0859 - Valid accounts	ALLANITE (RU) Dragonfly (RU)
4.	TA0109 - Lateral movement	T0859 - Valid accounts T0812 - Default credentials	ALLANITE (RU) CyberAv3ngers (IR) Dragonfly (RU)
5.	TA0109 - Collection	T0852 - Screen capture	ALLANITE (RU) APT33 (IR) Dragonfly (RU)
6.	TA0101 - Command and control	T0885 - Commonly used ports	Dragonfly (RU)
7.	TA0107 - Inhibit response function	T0814 - Denial of service	CyberAv3ngers (IR)
8.	TA0105 - Impact	T0829 - Loss of view T0828 - Loss of productivity and revenue T0826 - Loss of availability	CyberAv3ngers (IR)

The tactics and techniques used by the threat groups significantly overlapped, suggesting that state-sponsored actors have similar operational methodologies and exploit identical vulnerabilities. Figure 3 below shows the MITRE ATT&CK ICS matrix map generated for these nation-state actors.

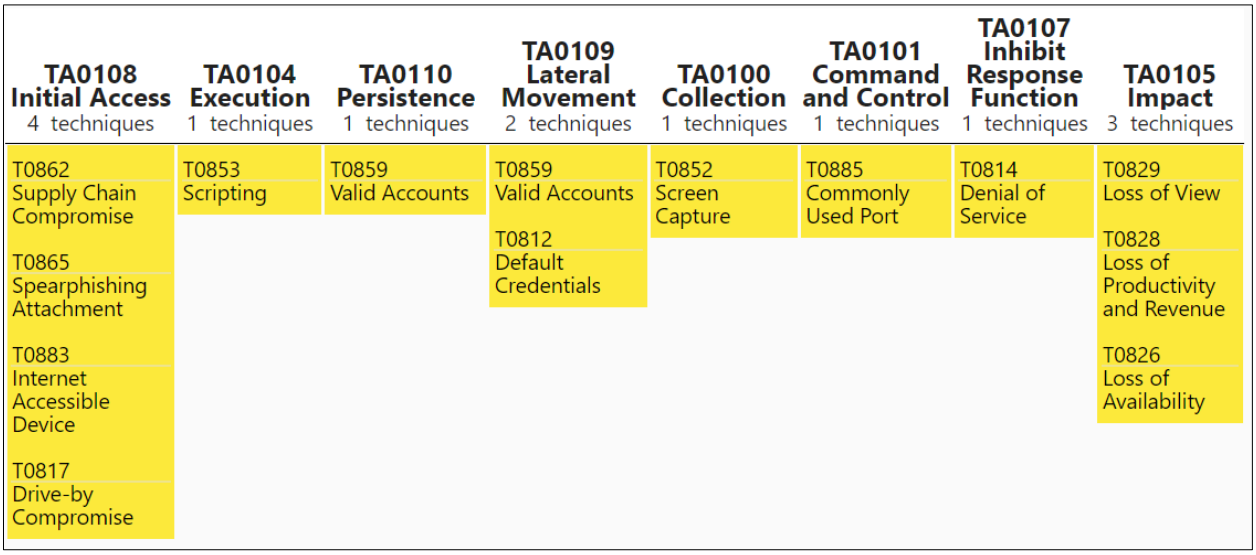

Fig. 3: MITRE ICS matrix mapping of techniques and tactics used by the nation-state groups

3.3 Defense Architecture

To defend against these nation-state attackers, the security tooling identified in section 2.4 was utilized. We utilized a multi-layered approach to implementing security in the infrastructure. The layers are as follows:

1. **Shell layer:** This layer was the outer security layer. It consisted of an outer Mikrotik firewall filtering traffic from the internet, implementing ACLs for inbound and outbound traffic, and performing traffic inspections.
2. **Core layer:** This layer was the inner security layer for the entire enterprise including parts of the critical infrastructure. It consisted of an internal firewall filtering traffic between networks, workstations, and servers. Suricata was used as an intrusion detection system, and traffic analysis was performed. The primary enterprise security tooling also resides in the core layer.

The Wazuh SIEM and XDR were focal points of the defense infrastructure, playing a key role in detecting malicious activities. Logs from all servers, workstations, network devices, SCADA, OT, PLC, and other security tooling were ingested into the SIEM, where they were analyzed and correlated to identify nation-state techniques and activities. In collaboration with the Wazuh XDR functions, ClamAV was utilized to detect malware. Wazuh's vulnerability detection function was used to detect unpatched vulnerabilities.

All traffic within the enterprise domain had to flow through the internal firewall, while traffic to destinations on the Internet was tunneled through the Squid proxy and onto the external firewall. This method allowed tight control over the URLs visited from the enterprise environment.

A Windows active directory was used to manage users and maintain their privileges. Power users who require more elevated privileges for technical tasks were separated into a different group from standard non-power users. A theoretical email gateway solution was used to control emails and filter out phishing and spam emails.

3. **Root layer:** This layer contains the security for the critical infrastructure (CI) domain. It consisted of an OT firewall filtering traffic from the enterprise infrastructure domain. Only the jump server was permitted to connect to the OT firewall and given access to the CI domain. Similarly, all devices in this domain were not allowed to communicate with other devices outside of it except for outbound-only connectivity from a log collector server in the CI domain to the SIEM on port 514/TCP, and bidirectional connectivity was allowed from the SIEM/XDR to the CI domain on port 1514 for security management. Internet access from the CI domain was restricted entirely. Wazuh XDR features were utilized to perform device scanning, anomaly detection, and vulnerability management.

Figure 3 below shows the operational defense architecture to protect the virtual organization's critical infrastructure and enterprise infrastructure domains from nation-state groups.

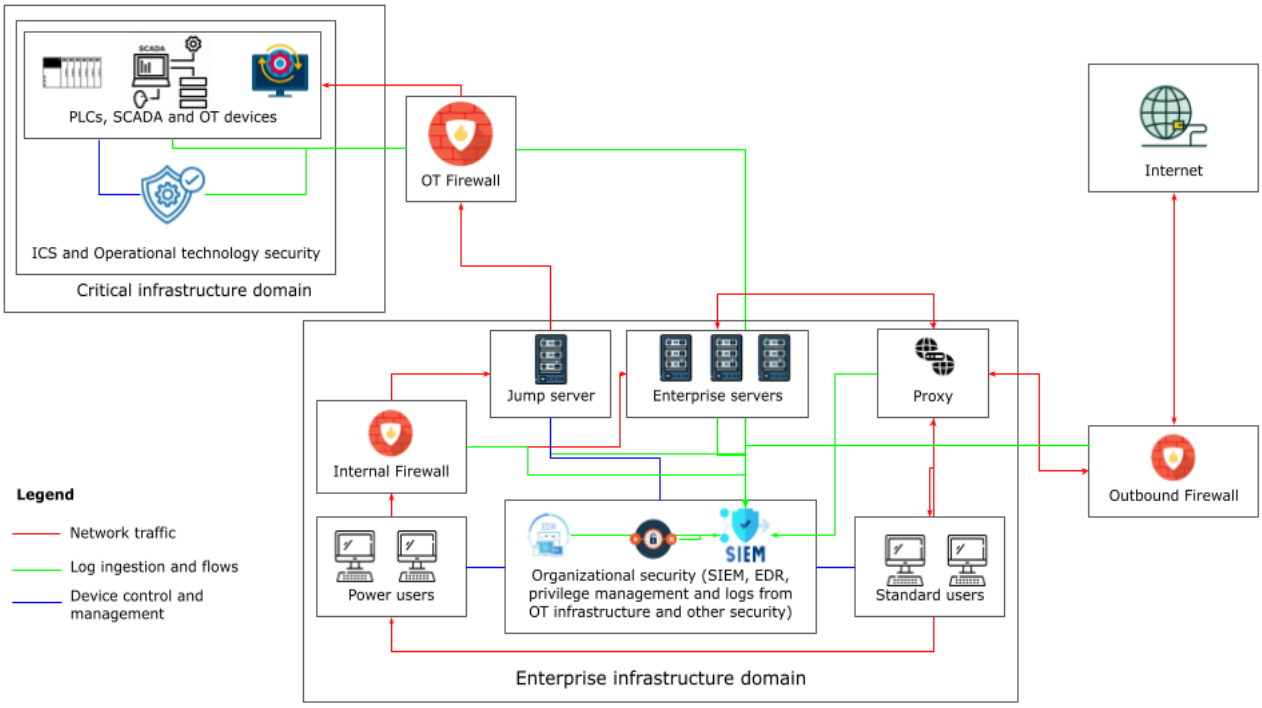

Fig. 4: Operational defense architecture for defending critical infrastructure

3.4 Results of the Adversary Emulation of the Nation-State Groups and the Defenses

Adversary emulation using the tooling and attack path in section 2.2 was executed for all the identified techniques of the five (5) nation-state groups, and the defense layers were evaluated to determine their responses to the attacks.

T0862 - Supply chain compromise

This technique involved distributing trojan files through compromised vendor websites. To emulate this behavior, we spun up a dummy web server and downloaded a trojan copy of ICS software. Dragonfly uses this technique as an initial access tactic, and the malware scanner successfully detected and mitigated it.

T0865 - Spearphishing attachment

To emulate this technique, the GoPhish software package was used to send phishing emails to specific users in the enterprise infrastructure domain. This was detected by leveraging the email logs and events sent to the SIEM and email analysis functionality to identify malicious emails. The Lazarus group, APT33, and ALLANITE use this technique as an initial access technique.

T0833 - Internet accessible device

This technique involves accessing critical infrastructure by exploiting systems directly exposed to the internet for remote access and management. This technique was mitigated and could not be exploited because the root security layer projecting the CI domain ensures that no asset from the CI domain is exposed directly to the internet. For continuous assurance that the configuration state is unchanged, the command monitoring module of Wazuh was configured to run periodic Nmap scans for open ports. These mitigations thwart the use of this technique for initial access by the CyberAv3ngers nation-state group.

T0817 - Drive-by compromise

Emulating this used by ALLIANTE and Dragonfly involved compromising a fictitious trusted vendor website and plating malware on it that auto-executed when users from the critical infrastructure organization visited the compromised website. The mitigation our security architecture provided for this was identifying vulnerable applications that can be compromised using the Wazuh vulnerability scanning module and enforcing all requests to external URLs to pass through the proxy. Additionally, our detection rules successfully identified known malicious destinations by ingesting the logs for application and URL access from the proxy to the SIEM, then analyzing and correlating those logs.

T0853 - Scripting

The scripting technique executes commands and code in a victim's infrastructure to gain elevated privileges. APT33 leverages this technique to ingress additional payloads to instantiate command and control for further malicious activity. The scripting technique was emulated by executing PowerShell scripts downloaded after clicking a link in the spearphishing email in technique T0865. Once the script was executed, a command and control channel was established back to our C2 server, where further commands and techniques were executed in the victim environment. Given that these scripts can be of any format (PowerShell, VBS, Bash), this technique was detected by leveraging the Windows and Linux event logs to detect process creations and downloads of scripts to suspicious locations. Figure 5 below shows the detection of PowerShell scripts the nation-state actors used during the execution phase.

T0859 - Valid accounts

The ALLANITE, Dragonfly, and CyberAv3ngers nation-state groups use this technique to establish persistence and perform lateral movement in a compromised critical infrastructure environment. This technique involves dumping valid operational credentials from key stores, utilizing malware to steal them, or creating additional user accounts, then using them to gain and maintain a foothold in the compromised infrastructure. To emulate valid accounts, we brute-forced user credentials until we found the correct one. The SIEM solution detected this activity by leveraging its log analysis module. Figure 5 below shows an event detected by the SIEM solution during the emulation process where a user account was enabled to establish persistence.

T0812 - Default credentials

The default credentials techniques refer to when systems use their devices out of the box without changing the credentials. These default credentials are well-known and not a secret. CyberAv3ngers have been known to compromise critical infrastructure using default credentials extracted from data dumps. Our multi-layered security system detects this issue by utilizing the security configuration assessment module of the Wazuh XDR to detect the use of default credentials and settings. Figure 6 below shows a configuration assessment check that detects the use of blank credentials for console logons and ensures it is disabled.

T0852 - Screen capture

To detect screen capture techniques used to collect sensitive configuration and data by ALLANITE, APT33, and Dragonfly, we utilized script logging functions in the defense architecture to identify when screen capture functions were called. This successfully detected PowerShell scripts calling the *[Drawing.Graphics]::FromImage(*and *New-Object Drawing.Bitmap* or *.CopyFromScreen* PowerShell functions. Additionally, we successfully detected image file creation events in directories commonly used by malware like *C:\Users\Public* and *temp* directories.

T0885 - Commonly used ports

The commonly used ports technique refers to threat actors leveraging standard ports to communicate with their C2 servers to bypass firewalls and traffic inspection detection tooling. To emulate this technique, we initiated a reverse

shell connection over port 443 in the CI domain, a commonly used port for HTTPS communications. The OT firewall at the root layer blocked the connection because all inbound and outbound traffic is tightly controlled on the firewall.

T0814 - Denial of service, T0826 - Loss of availability, and T0828 - Loss of productivity and revenue

Denial of service techniques interrupt the expected normal operation of a device or software. Some execution methods involve overwhelming the target with a huge amount of traffic. By utilizing various DoS tools like ScaPy and Slowloris to emulate the CyberAv3ngers nation-state group, we flooded ICS, SCADA, and OT devices with traffic intending to overwhelm them. A denial of service can also lead to a loss of productivity and availability, leading to reduced revenue. The implemented detection tooling detected the flood of traffic using the Suricata IDS network analysis mechanism, and the connection was terminated using the Wazuh XDR function. Figure 8 below shows the DoS attacks detected and the response mechanisms.

T0829 - Loss of view

Loss of view intends to ensure that critical infrastructure is not visible on monitoring and control dashboards. This activity was emulated by disabling monitoring and control software on critical systems. Our SIEM solution detected this software and an active response was executed to enable it, thus defending against the CyberAv3ngers nation-state actor and reducing possible impact.

t _index	wazuh-alerts-4.x-2024.10.10
t agent.id	001
t agent.ip	192.168.33.6
t agent.name	emulation-windows-server-1
data.win.eventdata.creationUtcTime	2024-10-10 21:58:44.289
data.win.eventdata.image	C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe
data.win.eventdata.processGuid	{ffe40d62-4e0b-6708-ff04-000000000200}
data.win.eventdata.processId	6396
data.win.eventdata.ruleName	technique_id=T1059.001,technique_name=PowerShell
data.win.eventdata.targetFilename	C:\\Windows\\Temp__PSScriptPolicyTest_axfk3tgk.tyu.ps1
data.win.eventdata.user	NT AUTHORITY\\SYSTEM
data.win.eventdata.utcTime	2024-10-10 21:58:44.289
data.win.system.channel	Microsoft-Windows-Sysmon/Operational
data.win.system.computer	DESKTOP-5U43ENU
data.win.system.eventID	11
data.win.system.eventRecordID	98
data.win.system.keywords	0x8000000000000000
data.win.system.level	4
data.win.system.message	"File created: RuleName: technique_id=T1059.001,technique_name=PowerShell UtcTime: 2024-10-10 21:58:44.289 ProcessGuid: {ffe40d62-4e0b-6708-ff04-000000000200} ProcessId: 6396 Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Windows\Temp__PSScriptPolicyTest_axfk3tgk.tyu.ps1 CreationUtcTime: 2024-10-10 21:58:44.289 User: NT AUTHORITY\SYSTEM"

Fig. 5: Detection of execution scripts

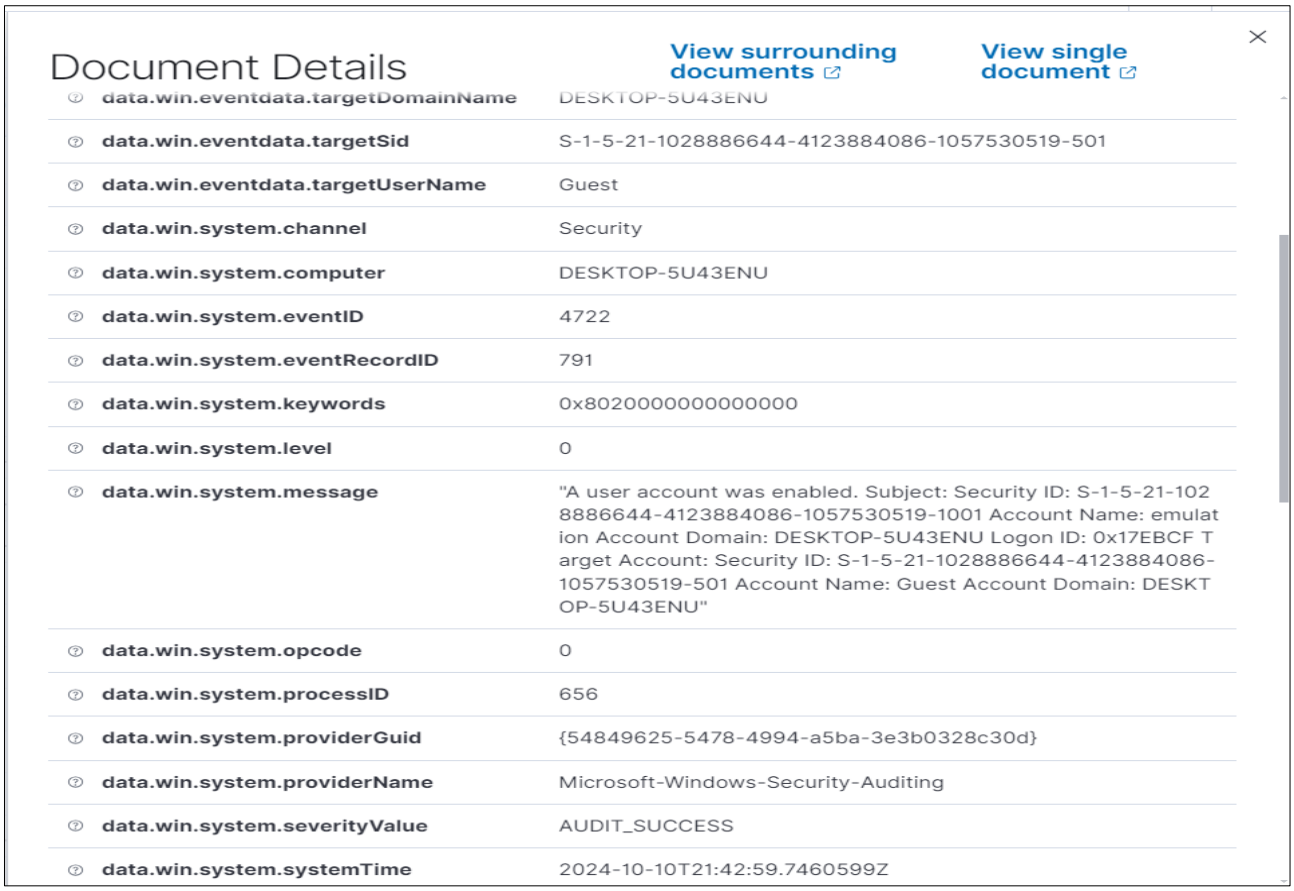

Fig. 6: Security alert identifying account creation used for persistence by nation-state actors

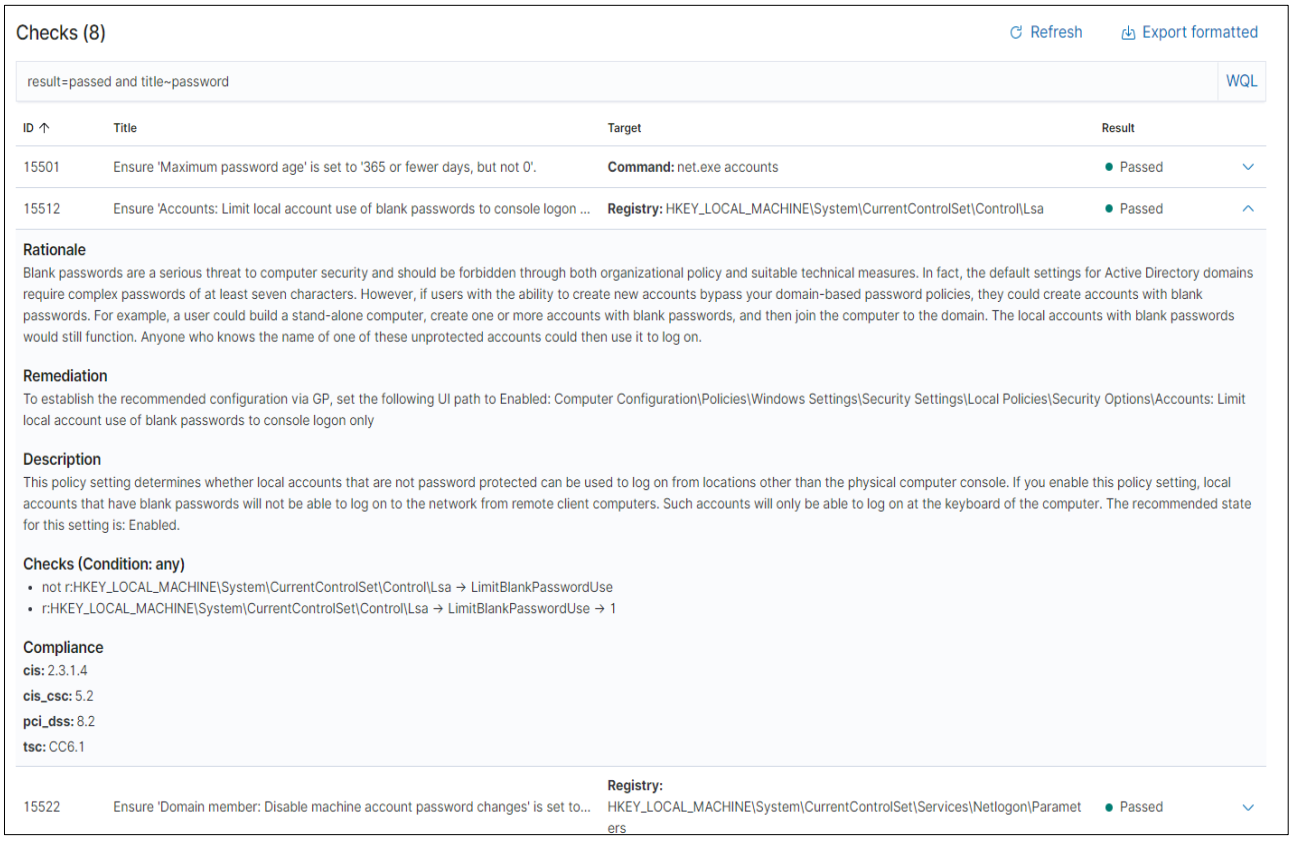

Fig. 7: SCA checks to detect blank credentials being used for console login

Fig. 8: **Denial of service attacks detected and the response**

4. CONCLUSION

This paper successfully identified nation-state groups that attack critical infrastructure and their tooling, techniques, tactics, and procedures. Analyzing the techniques used by nation-state actors showed significant overlap among these threat actors, leading to the hypothesis that multiple hostile nation-states may collaborate. This is a path for future research.

The attack path for these nation-state actors was identified, and a virtual organization implementing critical infrastructure and enterprise infrastructure domains was built. Subsequently, security was embedded in the virtual organization's critical and enterprise infrastructure domains using a multilayered approach with a shell, core, and root security layer, each protecting different aspects of the organization. Access to the critical infrastructure domain was tightly controlled using ACLs, firewalls, and jump servers.

Following the implementation of the multilayered defense in all aspects of the organization, we proceeded to execute adversary emulation using the techniques of nation-state groups, with a focus on breaching the CI domain. All techniques were detected, and appropriate mitigations were applied. This work forms a benchmark for implementing standard defense mechanisms to protect critical infrastructure from state-sponsored attacks.

Conflict of Interest: There are no conflicts of interest.

REFERENCES

- Viganò, E., Loi, M., & Yaghmaei, E. (2020). Cybersecurity of critical infrastructure. *The International library of ethics, law and technology, 21*, (pp. 157–177). Springer, Cham. https://doi.org/10.1007/978-3-030-29053-5_8
- Pollard, M. (2024). A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States. *Pepperdine Policy Review, 16(1)*. https://digitalcommons.pepperdine.edu/ppr/vol16/iss1/1
- Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *WIRED*. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. Accessed 12 Oct. 2024.
- Knake, R. (2017.) A Cyberattack on the U.S. Power Grid. *Center for Preventive Action.* https://cdn.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf
- MITRE.org (2024a). *Sandworm Team, ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM, Seashell Blizzard, FROZENBARENTS, Group G0034 | MITRE ATT&CK®*. https://attack.mitre.org/groups/G0034/
- Baezner, M. (2018). Synthesis 2017: Cyber-conflicts in Perspective. *CSS Cyberdefense Hotspot Analyses, 12*. https://doi.org/10.3929/ethz-b-000314603

- Mims, N. (2016). Cyber-Attack Process. *Computer and Information Security Handbook (Third Edition)*, (pp. 1105-1116). https://doi.org/10.1016/B978-0-12-803843-7.00084-3
- Malatji, M., Marnewick, A. L., & Von Solms, S. (2021). Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security*, *30*(2), 255–279. https://doi.org/10.1108/ics-06-2021-0091
- Knapp, E. (2024). Industrial Network Security. *Syngress*. Elseiver, Boston, MA, United States.
- Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., & Schwarzenbach, A. (2020). National Cyber Power Index 2020: Methodology and Analytical Considerations. *The Belfer Center for Science and International Affairs*. https://www.belfercenter.org/publication/national-cyber-power-index-2020
- Pandey, S., Singh, R.K., Gunasekaran, A., and Kaushik, A. (2020), Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13(1)*. (pp. 103-128). https://doi.org/10.1108/JGOSS-05-2019-0042
- Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Revista Academiei Forţelor Terestre*, *26*(1), (pp. 69–75). https://doi.org/10.2478/raft-2021-0011
- Lehto, M. (2022). Cyber-Attacks against critical infrastructure. *Computational methods in applied sciences, 56.* (pp. 3-42). https://doi.org/10.1007/978-3-030-91293-2_1
- MITRE.org (2024b). *Groups | MITRE ATT&CK®*. https://attack.mitre.org/groups/
- MITRE.org (2024c). *Techniques - ICS | MITRE ATT&CK®*. https://attack.mitre.org/techniques/ics/