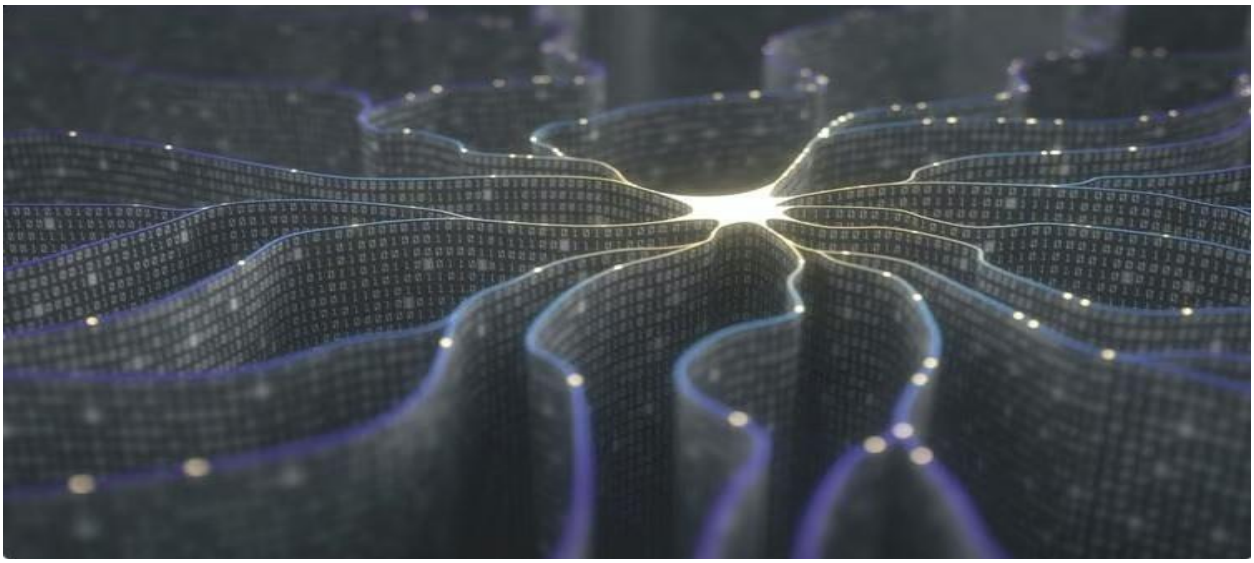
Serianu Cyber Threat Intelligence Bulletin, Quarter 1



Executive Summary

As the digital space continues to evolve, so do threats that aim to exploit existing and upcoming online infrastructure and entities. Intelligence gathered from Serianu indicates that cyber criminals are increasingly deploying both sophisticated and unsophisticated methods to gain access to sensitive information. In an attempt to evade detection from security controls, threat actors abuse common and valid processes and end up going undetected.

This quarterly report tries to offer an overview of the cyber trends in the region, analysis of top (Common Vulnerabilities & Exposures) CVEs, exploit tactics, phishing trends, vulnerability landscapes, dark web intelligence and geo-political cyber-criminal trends.

This should empower organizations to optimize their security posture and proactively detect and mitigate risks.

1. Common CVEs and Exploits identified in Q1

Common Vulnerabilities & Exposures (CVEs) enable Intrusion Detection Systems to prioritize events based on the severity and impact of known vulnerabilities and direct attention to critical threats.

By associating IPS events with CVEs, organizations can focus resources on addressing high priority vulnerabilities. This prioritization based on criticality of the CVEs helps mitigate the most significant risks and reduce the likelihood of a successful exploitation.

By prioritizing based on risk, organizations can effectively allocate resources and focus efforts on addressing the most critical security vulnerabilities to enhance the organization's overall security posture.

Threat analysis show a correlation between when a Critical Vulnerability is published, followed by a widespread weaponisation of the exploit and its use by adversaries to attack public facing assets. This increases the need for prioritized and urgent patching of devices, especially after a CVE is announced.

The most highly targeted vulnerabilities in the quarter include:

1. **CVE-2024-1708 and CVE-2024-1709 (ConnectWise ScreenConnect) – CVSS Score: 10:00 CRITICAL**

   These are incredibly easy to exploit vulnerabilities affecting ConnectWise ScreenConnect **23.9.7**. The vulnerabilities are actively exploited and have been observed to carry out malicious activities including **ransomware attempts** and deployment of remote access tools.

   Connectwise has released a patch in version **23.9.8** and organizations are urged to upgrade immediately.

2. **Androxgh0st Malware Attack – CRITICAL**

   Androgh0st malware is a python-based malware, which primarily targets user environment (.env) files. These files may contain credentials for various high-profile applications like AWS, 0ffice 365, SendGrid and Twilio. The malware has

malicious functions to abuse SMTP, scan and exploit exposed credentials and deploy web shells to maintain persistent access to systems.

Androxgh0st malware targets vulnerabilities from the PHPUnit (CVE-2017-9841), Laravel Framework (CVE-2018-15133) and Apache Web Server (CVE-2021-41773) to spread and conduct information gathering attacks on the target networks.

3. **Microsoft SharePoint Server Elevation of Privilege Vulnerability (CVE-2023-29357) – CVSS Score: 9.8 CRITICAL**

This is an authentication bypass vulnerability that adversaries may use to escalate privileges (EoP) on affected installations of Microsoft SharePoint Server. Attackers can exploit the vulnerability by sending a spoofed JSON Web Token (JWT) authentication token to a vulnerable server giving them the privileges of an authenticated user on the target.

4. **PAN-OS Vulnerability (PALO ALTO) (CVE-2024-3400) – CVSS Score 10.0 CRITICAL**

This critical vulnerability is a case of command injection in the *GlobalProtect* feature of Palo Alto Networks PAN-OS software that an unauthenticated attacker could exploit to execute arbitrary code with root privileges on the firewall.

This vulnerability only affects PAN-OS 10.2, PAN-OS 11.0 and PAN-OS 11.1 firewalls configured with GlobalProtect gateway or GlobalProtect portal (or both).

5. **CVE-2024-0204 (Forta GoAnywhere MFT)– CVSS Score: 9.8 CRITICAL**

Authentication bypass in Fortra's GoAnywhere MFT prior to 7.4.1 allows an unauthorized user to create an admin user via the administration portal.

GoAnywhere MFT (Managed File Transfer) offers remote file transfer solutions with benefits like automation and improved data security.

6. **CVE-2024-21893 (Ivanti Connect Secure VPN gateway) – CVSS Score: 8.2 CRITICAL**

Ivanti Connect Secure flaw (CVE-2024-21893) is a Server Request Forgery (SSRF) vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA which allows an attacker to access certain restricted resources without authentication.

7. **CVE-2024-21887 (Ivanti Connect Secure) – CVSS Score: 9.1 CRITICAL**

A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.

8. **CVE-2024-22024 (Ivanti) – CVSS Score: 8.3 HIGH**

An XML external entity or XXE vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and ZTA gateways which allows an attacker to access certain restricted resources without authentication.

2. Threat Actor Targets

Threat actors were observed to target businesses of all sizes and nature. These include both SMEs and large corporate entities. Each of these entities had different motivations, exposures and vulnerabilities as described below.

Targeted Industries:

1. **Small & Medium Businesses:**

From statics collected it was observed threat actors preferred Small & Medium businesses due to the following reasons:

- **Resource Constraints:** Due to limited resources and a lack of expertise SMEs were more vulnerable to cyber-attacks, especially spear-phishing

for end users, customers and the C-suite. This led to more success as a majority of the victims lacked basic cybersecurity awareness or training.

- **Ransomware Vulnerability:** SMEs were more vulnerable to ransomware attacks due to limited security measures and processing of customer financial data. Most of them were customer facing meaning the impact would be directly significant as compared to B2B businesses.

2. **Enterprise Businesses:**

- **Sophisticated Attacks:** Large businesses faced more sophisticated attacks due to their size, value of data/assets and deployment of medium to optimum security measures. However, a majority of these solutions are from commonly known vendors which make them easily identifiable and vulnerable to similar attack Tactics, Techniques and Procedures.

  Associated vulnerabilities from vendor products are publicly announced, which launches vulnerability scans from attackers making publicly facing products more vulnerable and easily accessible/exploitable from the internet.

  Supply chain risks and multiple third party vendor products add on to the attack surface and increase complexities making it harder to detect “true-positive” threats.

  Due to security measures deployed by large organizations, threat actors result to more sophisticated methods to by-pass these measures or attack valid processes and procedures within a network to evade detection.

- **Insider Threats:** Insider threat activity was profound in the compromise of large enterprises. This was a result of both intentional and unintentional insider threat activities, where employees in organizations played a critical role in the compromise of the organization. Disgruntled employees, fear, greed and extortion were some of the motivations toward intentional insider threats whereas phishing, vishing, SIM Swaps, OTP manipulation and lack of general cybersecurity awareness were some of the techniques deployed to trick unsuspecting employees/customers.

Common trend and processes abused by insider threat actors include database manipulation, money channels and mobile money transactions.

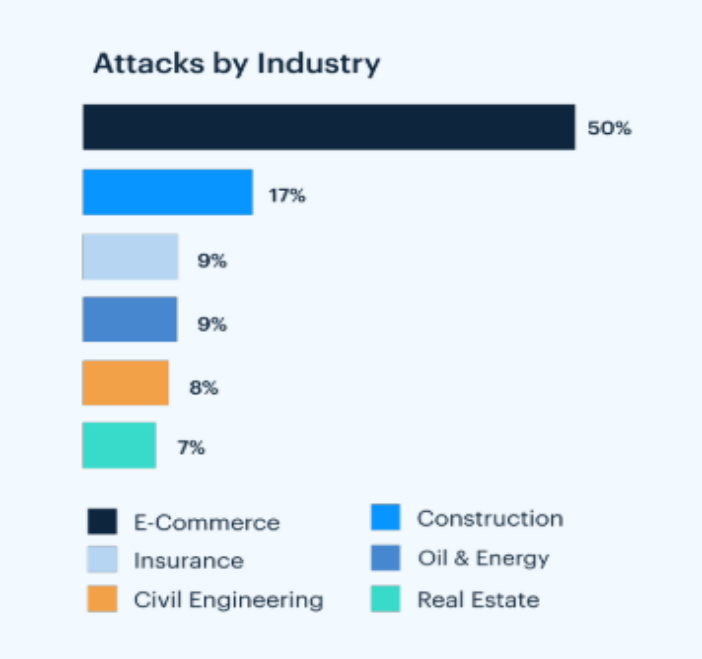
Organizations are advised to adopt a Zero-Trust approach model, apply vigilant monitoring of database activities, money channels and transactions and user awareness trainings to prevent some of these attacks.

- **High-profile targets:** The Executive suite are attractive targets for cybercriminals, especially those from large entities. Threat actors deployed spear-phishing methods and spoofing in an attempt to sway subordinate employees or gain unauthorized credentials to critical assets. More advanced method of attack detected this quarter was the use of deep fakes to impersonate executives into tricking unsuspecting users/employees.

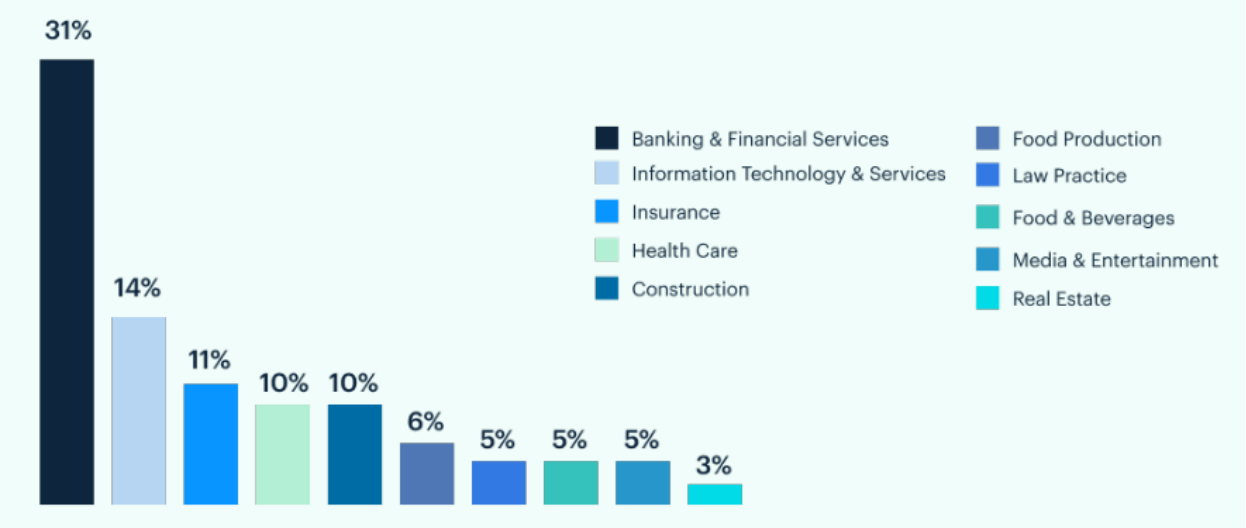
- **Increased Attack Surface:** Larger organizations have a broader attack surface which makes them more susceptible to a wider range of cyber threats that could potentially exploit existing vulnerabilities in their systems and networks. This include multiple vendors (increasing the complexity of processes), supply chain constraints and a high multitude of devices and employees.

3. Attacks by Industry

Below were industry-wise cyber-attacks as observed over the first quarter.

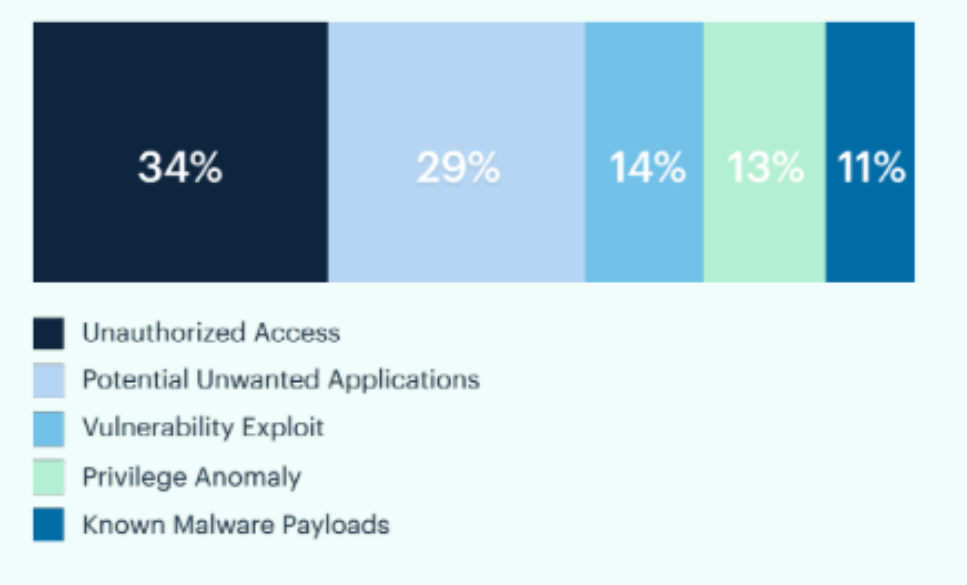


Top 10 Industry-wise Incidents Raised include:



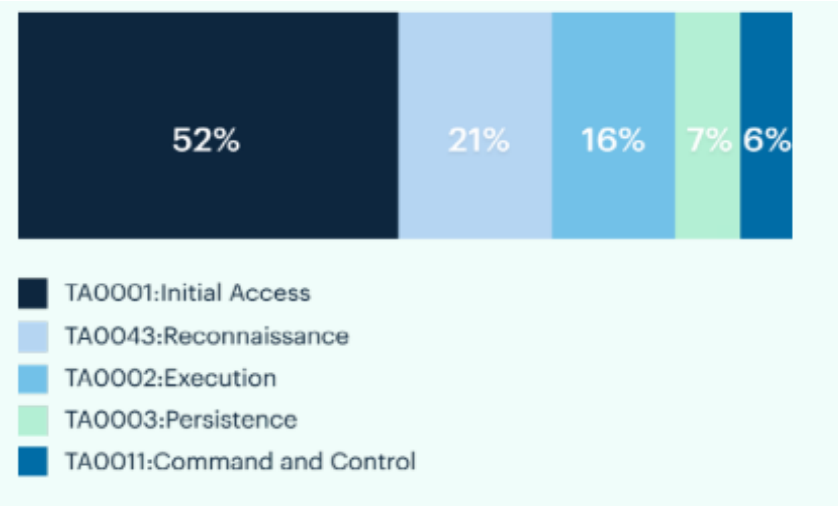
Top 5 Incident Areas include:

These are areas that showcase a range of security that pose significant challenges to industries worldwide.



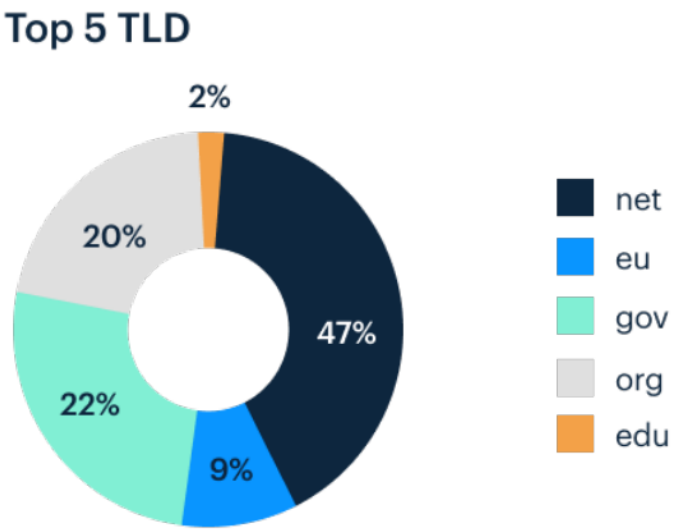
Top 5 MITRE Tactics

This is a categorization of threats based on tactics used by attackers.



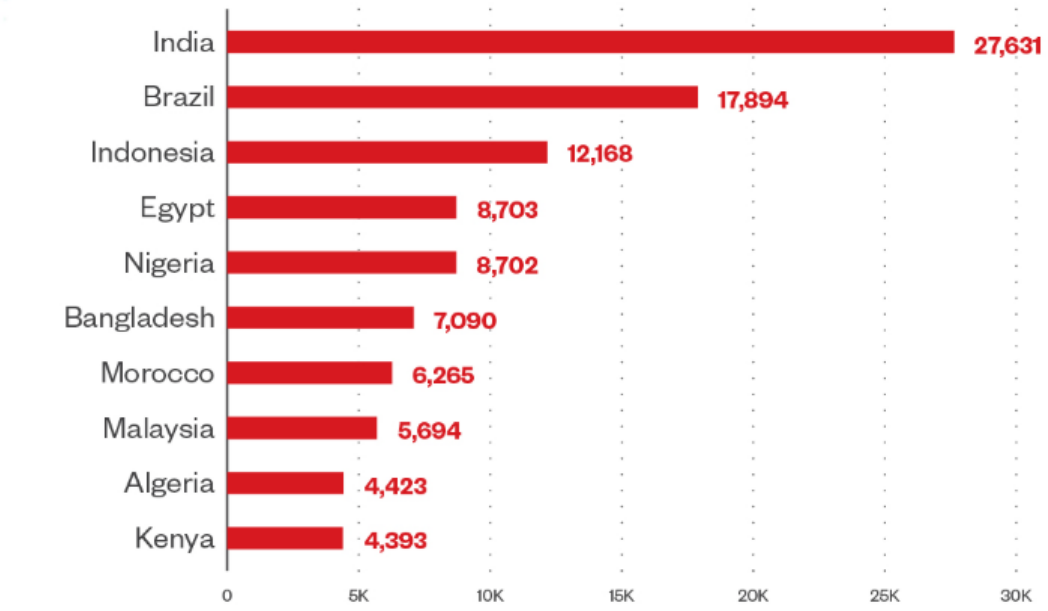
Top Level Domains used in Phishing

Phishing remains the most prevalent method used by cybercriminals as an initial access tool. It is recommended that organizations should invest in security best practices to combat phishing through practices such as user awareness training, email filtering, email security gateways and multi-factor authentication to reduce these risks.



Top Countries associated in Data Heists and Stolen Information

This list highlights top countries in regard to stolen information and data heists.



4. Emerging Technologies, Trends and Future Outlook

As AI and Machine Learning algorithms grow more sophisticated and widespread, so do the dangers that these technologies pose.

According to World Economic Forum, all industries and the general public will be directly or indirectly be affected by high adoption of specialized language models that will provide more tailored content and actionable insights.

The landscape of cyber threats will include more sophisticated artificial intelligence techniques, such as advanced phishing campaigns and deep fakes, for which organizations must prepare for in advance.

New regulations will galvanize more cybersecurity expertise in the boardroom plus strategic risk management and third-party assessment to enhance cyber resilience.

As a leading company in cybersecurity we try to share some key cybersecurity predictions for 2024 and what to look out for based on trends observed over the first quarter and the past years.

- **Rise of specialized language models**

Large language models have transformed organizational outputs, with the power to sift large amounts of data into actionable insights through simple queries. These sophisticated models have demonstrated remarkable capabilities in understanding and generating human-like text enhancing advancements across various domains.

- **Threat actors will use AI to get ahead**

The emergence of generative AI has been widely adopted by both security enablers and threat actors. Organizations must work quickly to harness generative AI before threat actors can exploit it to their advantage. Dangers already observed being harnessed by threat actors include but not limited to;

  - Deep fakes
  - Sophisticated and automatic phishing campaigns

- Privacy violations
- Algorithmic bias, caused by “bad data”
- Weapons automation
- Uncontrollable self-aware AI
- Social Manipulation through AI Algorithms

Hackers are also able to gain access to detailed information about their targets while also getting around endpoint security defenses.

Threat intelligence also indicates a substantial correlation between generative AI, dark web intelligence and data leakage through leaked data/credentials, phishing, exposure of sensitive information, exploit attempts and targeted attack vectors such as online brand domain impersonation. These insights can empower organizations to reduce their attack surface by adopting the perspective of potential attackers.

It is advised for security leaders to prepare for the coming wave of AI-generated threats.

- **Spike in third-party data breaches**

A majority of the breaches observed over the quarter targeted major tech vendors supporting a multitude of clients/customers. This targeting is due to a number of factors, including API proliferation, data digitization and undetected zero-day vulnerabilities. It is also important to note that these vendors pose a central point of failure having significant impact when attacked.

Organizations should enable and enforce key performance indicators to detect, measure and manage these risks effectively.

- **Cyber expertise coming to the boardroom**

In an effort to cultivate a culture of cybersecurity the executive board needs to approach and address cybersecurity risks like any other material business risk. It is important to foster a culture of cybersecurity resilience and incorporate accommodating language in the board room in addressing cybersecurity concepts and its ties to financial concepts.

This new governance is an opportunity for both the CISO and board members to refine their communication skills in order to bring cyber-literacy to the boardroom and increase the organization's cyber resilience.

- **Managing third-party risk to stay resilient**

Threat actors will continue evolving their tactics, techniques and procedures and organizations must pivot accordingly. Over the past year, we witnessed several massive supply chain disruptions whose effects were quite significant. As a result, organizations must re-examine not only their own cybersecurity practices and posture but also those of their vendors and third-party suppliers.

It is exceedingly important to stay proactive and ahead in the ever-evolving technological advancements. As we look into 2024, it is important to leverage advanced technologies, foster collaboration and prioritize cybersecurity education and awareness to mitigate risks and ensure a secure digital future.

5. Geo-political Threat Activity

According to 2024 Annual Threat Assessment, the following are state of the hacks deployed by threat actors and factors affecting the geo-political landscape:

- Exploitation of Network Edge Devices
- Targeting the Cloud
- Ransomware Groups – Automation of Ransomware activities, increase in Ransomware-as-a-service (*RaaS*) operations.
- APT (Advanced Persistent Threat) for hire
- Stolen Information as a commodity
- Russia / Ukraine cyber warfare
- Hacktivism and Nation state cyber warfare
- Targeting of Critical Infrastructure
- Use of Artificial Intelligence

Chinese threat actor group ***Volt Typhoon*** was the most active and persistent cyber threat to the private-sector and critical infrastructure, having existed within some critical infrastructure since 2021 through "*Living off the Land*" technique (this is a cybersecurity strategy used by threat actors to carry out attacks while

minimizing detection by leveraging tools and resources already present on a targeted system. Instead of relying on custom malware that might trigger security alerts, attackers utilize legitimate system administration tools and built-in functionalities to conduct malicious activities).

This allowed the threat actor to evade detection by blending with normal Windows system and network activities, avoiding endpoint detection and response (EDR) products that would rise an alert on the introduction of third-party applications. Some of the built-in tools used were: *wmic, ntdsutil, netsh* and *Powershell.*

In general, the group compromised environments of multiple critical infrastructure organizations – primarily in Communications, Energy, Transportation Systems and Water and wastewater systems.

Best Practices for Detecting Living off the Land Activities

- Implement detailed logging, and aggregate logs in a write-once, read-many location to avoid the risk of attackers modifying logs.
- Apply and maintain security baselines of network, user, admin and application activity and least privilege restrictions.
- Build or acquire automation to continually review all logs.
- Apply and consult vendor-recommended guidance for security hardening
- Enhance IT and OT network segmentation and monitoring
- Implement authentication and authorization control for all human-to-software and software-to-software interactions

Applying what we have Learnt

- Hardening the Attack Surface;
    - Implementing Zero-Trust
    - Adopting AI in defense measures
- Stay alert and Informed;
    - Information, advisories and technical guidance
- Partnership and collaboration is Key;
    - Government, industry players, academia, select foreign partners