# Weekly Intelligence Report – 12 December 2025 - CYFIRMA

Archived: 2026-04-05 15:33:51 UTC

Published On : 2025-12-12


## Ransomware of the week

CYFIRMA Research and Advisory Team would like to highlight ransomware trends and insights gathered while monitoring various forums. This covers a variety of topics that can be pertinent to your company, including technology, geography, and industries.

**Type:** Ransomware

**Target Technologies:** Windows

**Targeted Countries:** United States, India, Turkey, Peru, Mexico

**Targeted Industries:** Manufacturing, Technology, Financial Services, Public Sector, Business Services

**Introduction**

CYFIRMA Research and Advisory Team has found Black Shrantac Ransomware while monitoring various

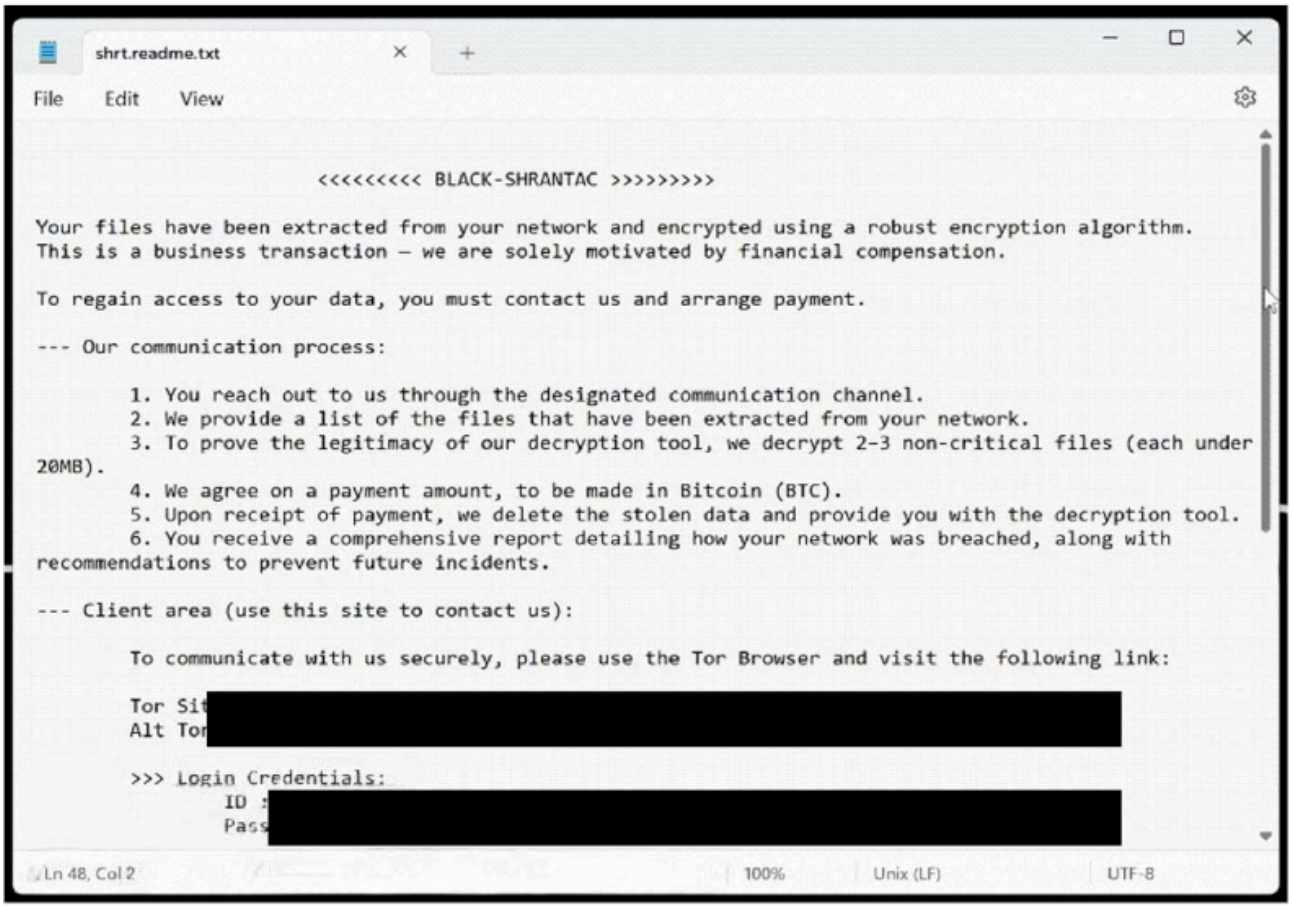
underground forums as part of our Threat Discovery Process.

**Black Shrantac Ransomware**

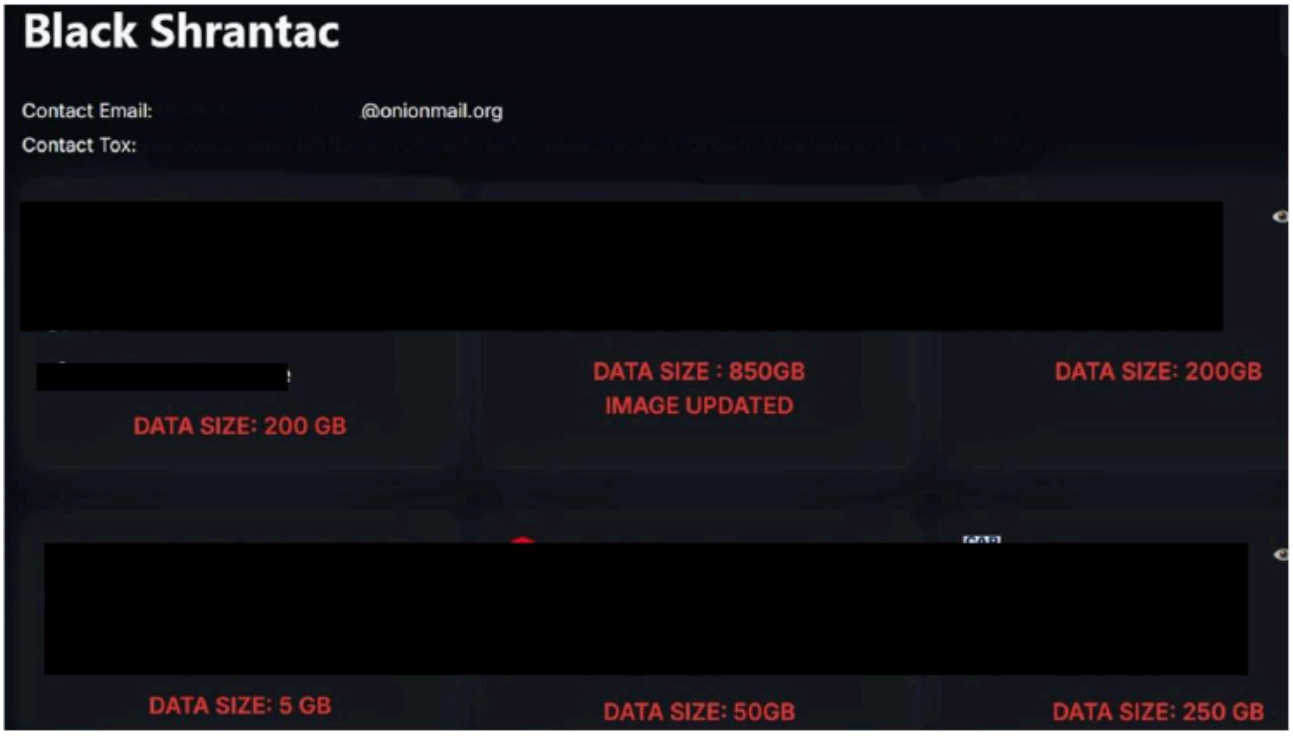
Researchers have identified Black Shrantac as a ransomware strain that encrypts files, alters their names, and leaves victims unable to access their data. In testing, it was observed that the malware replaces original filenames with random character strings and appends the ".shrt" extension, ex., converting "1.jpg" into something like "0WeRZQJSTkOAnYP4.shrt." After completing encryption, Black Shrantac changes the desktop wallpaper and generates a ransom message titled "shrt.readme.txt," signaling that the victim's data has been both encrypted and extracted from the system.


*Screenshot of files encrypted by ransomware (Source: Surface Web)*

The ransom note states that the attackers seek payment in Bitcoin and presents the extortion as a "business transaction." Victims are told they may submit a few small, non-critical files to verify the attackers' ability to decrypt. The message includes Tor- based communication portals, Tox contact information, and explicit warnings not to rename files or reboot systems, claiming such actions could cause irreversible damage. It also threatens to leak or sell stolen data if no contact is made, while emphasizing that access to negotiation credentials is required to proceed.




*The appearance of Black Shrantac ‘s ransom note (shrt.readme.txt) (Source: Surface Web)*




*The appearance of Black Shrantac’s data leak site (Source: Surface Web)*

**The following are the TTPs based on the MITRE Attack Framework**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| **Execution** | T1053 | Scheduled Task/Job |
| **Execution** | T1059 | Command and Scripting Interpreter |
| **Execution** | T1129 | Shared Modules |
| **Persistence** | T1053 | Scheduled Task/Job |
| **Persistence** | T1112 | Modify Registry |
| **Privilege Escalation** | T1053 | Scheduled Task/Job |
| **Privilege Escalation** | T1134 | Access Token Manipulation |
| **Defense Evasion** | T1027 | Obfuscated Files or Information |
| **Defense Evasion** | T1036 | Masquerading |
| **Defense Evasion** | T1070 | Indicator Removal |
| **Defense Evasion** | T1112 | Modify Registry |
| **Defense Evasion** | T1134 | Access Token Manipulation |
| **Defense Evasion** | T1202 | Indirect Command Execution |
| **Credential Access** | T1003 | OS Credential Dumping |
| **Credential Access** | T1552.001 | Unsecured Credentials: Credentials In Files |
| **Discovery** | T1057 | Process Discovery |
| **Discovery** | T1082 | System Information Discovery |
| **Discovery** | T1083 | File and Directory Discovery |
| **Discovery** | T1614 | System Location Discovery |
| **Collection** | T1005 | Data from Local System |
| **Collection** | T1114 | Email Collection |
| **Command and Control** | T1071 | Application Layer Protocol |
| **Command and Control** | T1090 | Proxy |
| **Impact** | T1486 | Data Encrypted for Impact |

**Relevancy and Insights:**

- The ransomware primarily affects the Windows operating system, which is commonly utilized in enterprise environments across multiple industries.
- The ransomware maintains a long-term presence on the system by creating and modifying Windows scheduled tasks, which allow it to automatically execute even after restarts or user logins. It sets tasks to run with SYSTEM-level privileges and uses recurring triggers such as hourly or logon events. By doing so, the malware ensures its payload is consistently launched, enabling it to finish encryption, re-establish control, or run additional malicious actions without relying on user interaction.
- Detect-debug-environment: The ransomware technique is used to determine if it is being monitored in environments such as sandboxes, virtual machines, or under debugging tools. To perform this check, the malware may look for specific processes, drivers, or artifacts linked to analysis tools, measure timing to spot inconsistencies, or scan for system traits uncommon in real user machines. When such conditions are identified, the malicious program can modify its behavior, such as pausing execution, shutting down, or withholding key payload actions to avoid detection and make detailed analysis more difficult.

**ETLM Assessment:**
CYFIRMA's assessment indicates that Black Shrantac is currently a capable and structured ransomware strain, featuring strong file-encryption behavior, randomized filename rewriting, data theft, scheduled-task persistence, and multi-channel communication through TOR and Tox. Its ransom delivery methods, wallpaper replacement, and extortion approach closely align with modern double-extortion families, showing that it already operates with a mature set of features designed for disruption and financial gain. Given this foundation, its evolution is likely to focus on strengthening its resilience, expanding its reach, and improving its ability to evade security controls.

As it evolves, Black Shrantac could adopt more effective anti-analysis strategies, incorporate automated lateral-movement techniques, and enhance its data- exfiltration processes to increase the pressure placed on victims. Future variants may introduce cloud-targeting capabilities, broader system-recovery destruction, and more robust encryption or obfuscation layers to hinder forensic investigation. By integrating modular components or adapting its infrastructure, the ransomware could become more scalable, harder to detect, and increasingly difficult for defenders to contain across enterprise environments.

**Sigma rule:**
title: Suspicious Schtasks Schedule Types tags:
– attack.privilege-escalation
– attack.persistence
– attack.execution
– attack.t1053.005 logsource:
product: windows category: process_creation
detection: selection_img:
– Image|endswith: '\schtasks.exe'
– OriginalFileName: 'schtasks.exe' selection_time:
CommandLine|contains:
– ' ONLOGON '
– ' ONSTART '
– ' ONCE '

– ‘ ONIDLE ‘
filter_privs: CommandLine|contains:
– ‘NT AUT’ # This covers the usual NT AUTHORITY\SYSTEM
– ‘ SYSTEM’ # SYSTEM is a valid value for schtasks hence it gets it’s own value with
space
– ‘HIGHEST’
condition: all of selection_* and not 1 of filter_* falsepositives:
– Legitimate processes that run at logon. Filter according to your environment level: high
(Source: Surface Web)

**IOCs:**
Kindly refer to the IOCs section to exercise control of your security systems.

**RECOMMENDATIONS**

**STRATEGIC RECOMMENDATIONS**

- Implement competent security protocols and encryption, authentication, or access credentials configurations to access critical systems in your cloud and local environments.
- Ensure that backups of critical systems are maintained, which can be used to restore data in case a need arises.

**MANAGEMENT RECOMMENDATIONS**

- A data breach prevention plan must be developed considering, (a) the type of data being managed by the company; (b) the remediation process; (c) where and how the data is stored; (d) if there is an obligation to notify the local authority.
- To reduce the risk of credentials being compromised, enable multifactor authentication (MFA) and zero-trust architecture.
- Foster a culture of cybersecurity, where you encourage and invest in employee training so that security is an integral part of your organization.

**TACTICAL RECOMMENDATIONS**

- Update all applications/software regularly with the latest versions and security patches alike.
- Incorporate the Sigma rule for threat detection and monitoring, which will assist in identifying and tracking suspicious activity as well as detecting anomalies in log events.
- Build and undertake safeguarding measures by monitoring/ blocking the IOCs and strengthening defence based on the tactical intelligence provided.

## Trending Malware of the Week

Type: Remote Access Trojan (RAT) | Objectives: Espionage & Credential Theft | Target Technology: Windows OS | Target Geography: Global

CYFIRMA collects data from various forums, based on which the trend is ascertained. We identified a few popular malwares that were found to be distributed in the wild to launch cyberattacks on organizations or individuals.

**Active Malware of the week**
**This week, “CastleRAT” is trending.**

**Overview of CastleRAT Malware**
CastleRAT is a newly observed remote access trojan that surfaced in early 2025 and has quickly gained attention for its flexible design and wide applicability across different attack campaigns. Distributed in both lightweight Python builds and more robust C- compiled versions, the malware is built to give attackers a discreet entry into Windows systems while avoiding common security controls. Its creators have designed CastleRAT to blend into normal system behavior, enabling it to operate quietly while establishing communication with remote servers controlled by the attacker.

Once active on a device, CastleRAT collects essential system details and maintains constant communication with its operator, allowing remote actions to be executed without the user’s awareness. It can capture on-screen information, monitor typed input, and access clipboard contents, activities that can reveal credentials, financial details, or other sensitive data. The malware also supports the delivery of additional tools from the attacker’s server and can open a hidden command interface, enabling further manipulation of the compromised system. Its ability to disguise itself as legitimate software components further strengthens its persistence.

The progression of CastleRAT demonstrates how contemporary adversaries are shifting toward highly flexible and low-visibility tooling to broaden their operational reach. Its preference for masked system activity, quietly re-launched browsers, and subtle data exchange methods reveal a clear focus on avoiding conventional security controls. For enterprise environments, this underscores the growing need to scrutinize irregular workstation behavior, enhance endpoint observability, and maintain well-rehearsed incident response procedures. In an era where intrusion techniques are becoming more seamless and unobtrusive, CastleRAT represents the kind of streamlined yet impactful threat that reinforces the critical role of early anomaly detection and behavior-driven defensive measures.

**Attack Method**
While the initial access method remains unclear, upon activation, CastleRAT performs an initial reconnaissance routine, collecting key host identifiers such as system metadata, user information, machine-specific GUIDs, and public IP details retrieved from an external lookup service. This data is transmitted to the command-and-control infrastructure as part of its periodic beaconing cycle. Subsequently, the malware launches multiple internal threads, each responsible for executing a distinct malicious function. Notably, early-stage tasks include the continuous monitoring of clipboard activity, enabling the silent acquisition of copied credentials, cryptocurrency information, and other sensitive artefacts that naturally pass through clipboard use.

As the intrusion progresses, CastleRAT shifts from passive surveillance to covert interactive manipulation. It intercepts clipboard operations and synthesizes paste actions to route harvested data through trusted user-facing applications, thereby embedding exfiltration within normal device behavior. In parallel, it employs RC4-based encryption to secure its communication with the C2 server, downloading DLL-based modular components and

executing them through legitimate Windows utilities, granting the operator a concealed remote shell environment. This shell is constructed through redirected inter-process communication pipes, allowing commands to be issued and responses retrieved without displaying any visible terminal window or generating conspicuous user-side activity.

CastleRAT further strengthens its presence by enabling a range of persistent surveillance and privilege-access features. It configures system-level hooks to capture keystrokes, stores intercepted input within temporary files prior to encryption and exfiltration, and periodically captures screenshots of the active desktop. Malware also manipulates browser behavior by terminating active sessions and silently spawning Chromium-based instances with audio-restrictive parameters, facilitating visual or auditory monitoring while minimizing user alerts. To ensure continued operation across system restarts, it registers a scheduled task that reinstates the malware at startup, thereby establishing durable persistence.

In its later operational phase, the malware expands its communication flexibility by leveraging legitimate web platforms as dead-drop locations for secondary configuration and tasking. Additionally, it employs an advanced privilege-escalation technique that abuses service-level behavior to identify privileged process handles, duplicate them, and integrate them into newly spawned malware instances. This handle-stealing approach enables elevated access and in-memory manipulation with limited on-disk evidence, complicating detection and forensic reconstruction. Collectively, these behaviors reflect a methodical attack methodology designed to maintain long-term, covert control through a combination of surveillance, stealthy system manipulation, and resilient communication mechanisms.

**The following are the TTPs based on the MITRE Attack Framework for Enterprise**

| Tactic (ID) | Technique ID | Technique Name |
|---|---|---|
| **Execution** | T1559 | Inter-Process Communication |
| **Persistence** | T1053.005 | Scheduled Task/Job: Scheduled Task |
| **Privilege Escalation** | T1548.002 | Abuse Elevation Control Mechanism: Bypass User Account Control |
| **Defense Evasion** | T1036 | Masquerading |
| **Defense Evasion** | T1218.011 | System Binary Proxy Execution: Rundll32 |
| **Credential Access** | T1056.001 | Input Capture: Keylogging |
| **Discovery** | T1082 | System Information Discovery |
| **Collection** | T1115 | Clipboard Data |
| **Collection** | T1185 | Browser Session Hijacking |
| **Collection** | T1125 | Video Capture |

| | | |
|---|---|---|
| **Collection** | T1113 | Screen Capture |
| **Command and control** | T1105 | Ingress Tool Transfer |
| **Command and control** | T1102.001 | Web Service: Dead Drop Resolver |

**INSIGHTS**

**Evolving Tradecraft in Covert Intrusions**

CastleRAT highlights how modern threat groups increasingly prioritize quiet, embedded operations over loud or disruptive attacks. Instead of relying on flashy techniques, the malware's workflow is designed to mimic the natural rhythm of a host system, allowing malicious activity to blend with routine behavior. This shift shows how attackers are refining their methods to maintain uninterrupted access by shaping their tools around subtlety, patience, and operational camouflage.

**Blending Surveillance with Everyday User Interactions**

One notable aspect of CastleRAT's behavior is the way it aligns its data-gathering and system-interaction capabilities with actions that users commonly perform. By structuring its monitoring functions to mirror ordinary digital tasks, it reduces the likelihood of drawing attention or triggering suspicion. This integration demonstrates a growing trend toward threats that study and replicate the flow of user activity, turning familiar interactions into windows for silent observation.

**Leveraging Legitimate System Pathways for Credibility**

CastleRAT's reliance on native components and standard system mechanisms reflects a broader pattern in threat operations: the use of trusted pathways to maintain legitimacy. Rather than introducing unfamiliar tools, the malware anchors itself to processes and utilities that already exist on the device, making its presence appear routine. This strategic piggybacking on built-in system behavior underscores how contemporary attackers increasingly depend on the credibility of the host environment itself to maintain persistence and avoid scrutiny.

**ETLM ASSESSMENT**

From an ETLM perspective, CYFIRMA assesses that the emergence of Castle RAT indicates a future in which traditional desktop environments will require markedly stronger scrutiny. As organizational workflows become more dependent on continuous workstation usage for communication, remote access, and integrated business applications, adversaries are likely to advance techniques that blend malicious activity into routine user behavior. This evolution will make it increasingly difficult for enterprises to determine whether system actions originate from legitimate employees or from an attacker operating unobtrusively within the same environment. Consequently, organizations may be compelled to adopt more rigorous validation mechanisms for ordinary workstation interactions and re-evaluate long-standing assumptions regarding endpoint trust. As professional ecosystems grow more interconnected, campaigns resembling Castle RAT may gradually reshape confidence in day-to-day desktop activity, prompting both users and security teams to approach familiar system behavior with heightened caution.

**IOCs:**

Kindly refer to the IOCs Section to exercise controls on your security systems.

**YARA Rules**

```
rule CastleRAT_IOC_Only
{
meta:
author = “CYFIRMA” date = “2025-12-08”
description = “IOC-only YARA rule for detecting CastleRAT samples”
sha256_1 = “963c012d56c62093d105ab5044517fdcce4ab826f7782b3e377932da1df6896d”
sha256_2 = “f2ff4cbcd6d015af20e4e858b0f216c077ec6d146d3b2e0cbe68b56b3db7a0be”
sha256_3 = “4ef63fa536134ad296e83e37f9d323beb45087f7d306debdc3e096fed8357395”
sha256_4 = “282fa3476294e2b57aa9a8ab4bc1cc00f334197298e4afb2aae812b77e755207”
strings:
// Dummy byte patterns to keep rule valid – modify as needed
$a = { 00 }
condition: any of them
}
```

**Recommendations:**

**STRATEGIC RECOMMENDATIONS**

- Strengthen Endpoint Visibility and Control: Establish an enterprise-wide strategy that prioritizes continuous monitoring of desktop endpoints, focusing on behavioral anomalies rather than signature-based detection. This includes integrating telemetry from EDR, SIEM, and identity systems to create a unified visibility layer.
- Adopt Zero-Trust for Workstation Interactions: Implement a long-term shift toward authentication models that verify each action, not just user identity. This includes device posture validation, contextual access decisions, and mandatory verification for sensitive transactions initiated from workstations.
- Prioritize Secure Remote Access Architecture: Reassess remote access pathways and privileged workstation operations, ensuring that attackers exploiting Castle RAT–like capabilities cannot pivot laterally. This may require segmentation of administrative workstations, hardened remote sessions, and isolation of critical functions.
- Invest in Threat Intelligence Integration: Incorporate structured threat intelligence feeds that track RAT evolution, affiliate behaviors, and distribution trends. This supports proactive risk modeling and informs strategic readiness for emerging variants.

**MANAGEMENT RECOMMENDATIONS**

- Enhance User Activity Validation Processes: Introduce verification workflows for high-risk or finance-related actions performed on desktops, reducing the likelihood of fraudulent transactions executed through covert remote-control modules.

- Implement Rigorous Workstation Hardening Policies: Enforce policies that restrict unnecessary executables, disable unused services, and limit installation privileges. Routine audits should be scheduled to validate compliance across departments.
- Strengthen Monitoring of Remote Interaction Indicators: Equip security teams with alerting mechanisms that flag suspicious screen-control activity, unauthorized command execution, or unusual process behavior that could indicate RAT-driven manipulation.
- Develop Workforce Awareness for Endpoint Deception Tactics: Provide management- driven training programs that help employees recognize subtle signs of system manipulation, unexpected interface behavior, or unexplained performance shifts that may accompany covert RAT activity.
- Regularly Test Incident Response Preparedness: Conduct periodic tabletop and technical exercises centered around RAT compromise scenarios. These exercises should validate escalation paths, containment procedures, and communication protocols across management layers.

**TACTICAL RECOMMENDATIONS**

- Deploy EDR Rules for Remote-Control Behavior: Configure detection logic for patterns such as unauthorized screen-capture calls, simulated input events, hidden window creation, and abnormal persistence mechanisms commonly linked to RAT activity.
- Harden PowerShell and Scripting Environments: Enforce constrained language mode, disable unapproved modules, and log all script block activity. Many RATs rely on script- based loaders, making this a critical layer of defense.
- Block Untrusted Binary Execution Paths: Apply application control policies (AppLocker/WDAC) to prevent execution from user directories, temp folders, and uncommon system paths often leveraged by droppers and loaders.
- Monitor for Suspicious Parent–Child Process Chains: Set alerts for anomalous process relationships, such as browsers launching unknown executables or system utilities spawning network-enabled processes.
- Enforce Network-Level Isolation for Compromised Hosts: Create automated playbooks in SOAR to quarantine endpoints that exhibit command-and-control–like traffic, unexpected beacons, or encrypted outbound connections to untrusted domains.
- Inspect Outbound Traffic for Behavioral IoCs: Implement rules for unusual DNS patterns, long-lived HTTP sessions, unidentified TLS certificates, and low-frequency beaconing intervals that may signal RAT communication.
- Regularly Validate Integrity of Critical System Files: Conduct automated hash- checking and file integrity monitoring on key directories to detect unauthorized modification or stealthy persistence methods.
- Implement Least-Privilege Local Access Controls: Remove local admin rights from standard employees, restrict the creation of scheduled tasks, and prevent unauthorized registry changes that RATs often exploit for persistence.
- Increase Logging Granularity for Input/Interaction Events: Enable enhanced logging for keyboard, mouse, and accessibility feature toggles to identify abnormal remote manipulation activity.
- Create SOC Playbooks for RAT Containment: Prepare rapid-action procedures that include isolating the host, collecting volatile memory, extracting network indicators, validating credential exposure, and initiating forensic triage to prevent lateral spread.

# Weekly Intelligence Trends/Advisory

## 1. Weekly Attack Types and Trends

Key Intelligence Signals:

- Attack Type: Ransomware Attacks, Spear-phishing, Vulnerabilities & Exploits, Data Leaks.
- Objective: Unauthorized Access, Data Theft, Data Encryption, Financial Gains, Espionage.
- Business Impact: Data Loss, Financial Loss, Reputational Damage, Loss of Intellectual Property, Operational Disruption.
- Ransomware – INC Ransomware, Lynx Ransomware| Malware – CastleRAT
- INC Ransomware – One of the ransomware groups.
- Lynx Ransomware – One of the ransomware groups.
  Please refer to the trending malware advisory for details on the following:
- Malware – CastleRAT
  Behavior – Most of these malwares use phishing and social engineering techniques as their initial attack vectors. Apart from these techniques, exploitation of vulnerabilities, defense evasion, and persistence tactics are being observed

## 2. Threat Actor in Focus

Iranian Threat Actor MuddyWater – Expanding Attack Surface

- Threat Actor: MuddyWater
- Attack Type: Connection Proxy, Credential Dumping, Exploitation of Vulnerabilities, Spear-phishing, Living off the Land (LOTL).
- Objective: Information theft, Espionage
- Suspected Target Technology: Office Suites Software, Operating System, Web Application, Huawei
- Suspected Target Geography: Austria, Azerbaijan, Bahrain, Belarus, Central Asia, Egypt, Georgia, India, Iran, Islamic Republic of Iraq, Islamic Republic of Israel, Jordan, Korea, Mali, Middle East, Pakistan, Republic of Russia, Saudi Arabia, Southwest Asia, Tajikistan, Turkey, Ukraine, United Arab Emirates, United States
- Suspected Target Industries: Aerospace & Defense, Agriculture, Capital Goods, Consumer Services, Energy Equipment & Services, Finance, Food, Gaming, High Tech, IT Service Providers, Individuals, Media & Entertainment, Military, NGO, Natural Resources, Oil & Gas, Politics, Telecommunication Services, Transportation, Construction, Cryptocurrency, Education, Engineering, Government, Healthcare, Metals.
- Business Impact: Data Theft, Operational Disruption, Reputational Damage

**About the Threat Actor**

MuddyWater is an APT group that primarily targets victims in the Middle East, employing in-memory attack techniques via PowerShell. Their operations fall under the “Living off the Land” category, as they avoid creating new binaries on the victim’s system, which helps maintain a low detection profile and minimal forensic footprint.

The threat actor continues to expand its attack surface by diversifying its tooling, initial access vectors, and regional targeting.

**Details on Exploited Vulnerabilities**

| CVE ID | Affected Products | CVSS Score | Exploit Links |
|---|---|---|---|
| **CVE-2017- 0199** | Microsoft Office | 7.8 | link1, link2, link3 |
| **CVE-2017- 8759** | Microsoft .NET Framework | 7.8 | link |
| **CVE-2017-11882** | Microsoft Office | 7.8 | link |
| **CVE-2017-17215** | Huawei HG532 | 8.8 | – |
| **CVE-2020- 0688** | Microsoft Exchange software | 8.8 | link1, link2 |

**TTPs based on MITRE ATT&CK Framework**

| Tactic | ID | Technique |
|---|---|---|
| **Resource Development** | T1588.002 | Obtain Capabilities: Tool |
| **Resource Development** | T1583.006 | Acquire Infrastructure: Web Services |
| **Initial Access** | T1566.001 | Phishing: Spear phishing Attachment |
| **Initial Access** | T1190 | Exploit Public-Facing Application |
| **Initial Access** | T1566.002 | Phishing: Spear phishing Link |
| **Execution** | T1059.001 | Command and Scripting Interpreter: PowerShell |
| **Execution** | T1059.003 | Command and Scripting Interpreter: Windows Command Shell |
| **Execution** | T1059.005 | Command and Scripting Interpreter: Visual Basic |
| **Execution** | T1059.006 | Command and Scripting Interpreter: Python |
| **Execution** | T1059.007 | Command and Scripting Interpreter: JavaScript |
| **Execution** | T1047 | Windows Management Instrumentation |
| **Execution** | T1204.001 | User Execution: Malicious Link |
| **Execution** | T1204.002 | User Execution: Malicious File |
| **Execution** | T1203 | Exploitation for Client Execution |

| | | |
|---|---|---|
| **Execution** | T1053.005 | Scheduled Task/Job: Scheduled Task |
| **Execution** | T1559.001 | Inter-Process Communication: Component Object Model |
| **Execution** | T1559.002 | Inter-Process Communication: Dynamic Data Exchange |
| **Persistence** | T1547.001 | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder |
| **Persistence** | **T1574.001** | **Hijack Execution Flow: DLL** |
| **Persistence** | T1137.001 | Office Application Startup: Office Template Macros |
| **Persistence** | T1053.005 | Scheduled Task/Job: Scheduled Task |
| **Privilege Escalation** | T1548.002 | Abuse Elevation Control Mechanism: Bypass User Account Control |
| **Privilege Escalation** | T1547.001 | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder |
| **Privilege Escalation** | T1574.001 | Hijack Execution Flow: DLL |
| **Privilege Escalation** | T1053.005 | Scheduled Task/Job: Scheduled Task |
| **Defense Evasion** | T1218.003 | System Binary Proxy Execution: CMSTP |
| **Defense Evasion** | T1218.005 | System Binary Proxy Execution: Mshta |
| **Defense Evasion** | T1548.002 | Abuse Elevation Control Mechanism: Bypass User Account Control |
| **Defense Evasion** | T1140 | Deobfuscate/Decode Files or Information |
| **Defense Evasion** | T1574.001 | Hijack Execution Flow: DLL |
| **Defense Evasion** | **T1562.001** | **Impair Defenses: Disable or Modify Tools** |
| **Defense Evasion** | T1036.005 | Masquerading: Match Legitimate Resource Name or Location |
| **Defense Evasion** | T1027.010 | Obfuscated Files or Information: Command Obfuscation |
| **Defense Evasion** | T1027.003 | Obfuscated Files or Information: Steganography |
| **Defense Evasion** | T1027.004 | Obfuscated Files or Information: Compile After Delivery |
| **Defense Evasion** | T1218.011 | System Binary Proxy Execution: Rundll32 |
| **Credential Access** | T1555 | Credentials from Password Stores |
| **Credential Access** | T1555.003 | Credentials from Password Stores: Credentials from Web Browsers |
| **Credential Access** | T1003.001 | OS Credential Dumping: LSASS Memory |

| | | |
|---|---|---|
| **Credential Access** | T1003.004 | OS Credential Dumping: LSA Secrets |
| **Credential Access** | T1003.005 | OS Credential Dumping: Cached Domain Credentials |
| **Credential Access** | T1552.001 | Unsecured Credentials: Credentials In Files |
| **Discovery** | **T1083** | **File and Directory Discovery** |
| **Discovery** | T1057 | Process Discovery |
| **Discovery** | T1033 | System Owner/User Discovery |
| **Discovery** | T1049 | System Network Connections Discovery |
| **Discovery** | T1016 | System Network Configuration Discovery |
| **Discovery** | T1087.002 | Account Discovery: Domain Account |
| **Discovery** | T1082 | System Information Discovery |
| **Discovery** | T1518 | Software Discovery |
| **Discovery** | T1518.001 | Software Discovery: Security Software Discovery |
| **Lateral Movement** | T1210 | Exploitation of Remote Services |
| **Collection** | T1113 | Screen Capture |
| **Collection** | T1560.001 | Archive Collected Data: Archive via Utility |
| **Collection** | **T1074.001** | **Data Staged: Local Data Staging** |
| **Command and Control** | T1071.001 | Application Layer Protocol: Web Protocols |
| **Command and Control** | T1132.001 | Data Encoding: Standard Encoding |
| **Command and Control** | T1573.001 | Encrypted Channel: Symmetric Cryptography |
| **Command and Control** | T1105 | Ingress Tool Transfer |
| **Command and Control** | T1104 | Multi-Stage Channels |
| **Command and Control** | T1090.002 | Proxy: External Proxy |

| | | |
|---|---|---|
| **Command and Control** | T1219 | Remote Access Tools |
| **Command and Control** | T1102.002 | Web Service: Bidirectional Communication |
| **Exfiltration** | T1041 | Exfiltration Over C2 Channel |

**Latest Developments Observed**

The threat actor is suspected of targeting organizations in Israel and Egypt, leveraging a custom Fooder loader designed to deploy the MuddyViper backdoor. The campaign appears to focus on enhancing defense evasion and maintaining long-term persistence within compromised environments. Once deployed, the MuddyViper backdoor enables extensive post-compromise activity, including system information collection, execution of files and shell commands, file transfer operations, and the exfiltration of Windows login credentials and browser-stored data.

**ETLM Insights**

MuddyWater, a well-established Iranian threat actor, continues to demonstrate increasing operational maturity, with recent insights showing expanded regional targeting, greater use of custom loaders, and a growing reliance on compromised credentials and exposed services for initial access. Their campaigns frequently combine living-off-the-land techniques with modular backdoors to maintain persistence, evade detection, and enable long-term espionage activities. Overall, the threat actor represents a persistent, adaptive, and geopolitically motivated cyber-espionage threat.

The actor’s primary objectives center on information theft and strategic intelligence collection, including:

- Sustaining long-term access to government and critical infrastructure networks.
- Gathering political, military, and strategic intelligence.
- Monitoring and surveillance of energy, telecommunications, and high- technology ecosystems.

**IOCs:**

Kindly refer to the IOCs section to exercise control of your security systems.

**YARA Rules**

rule APT_MuddyWater_Generic
{
meta:
description = “Generic detection for MuddyWater malware families (PowGoop, MuddyViper, loaders)”
author = “CYFIRMA”
threat_actor = “MuddyWater (Iran)” date = “2025-01-01”
strings:
// Common MuddyWater PowerShell patterns
$ps1 = “IEX (New-Object Net.WebClient).DownloadString” nocase
$ps2 = “FromBase64String” nocase
$ps3 = “Invoke-Expression” nocase
$ps4 = “System.Net.WebRequest” nocase

```
// MuddyViper / Fooder loader artifacts (publicly documented)
$mv1 = “MuddyViper” wide ascii
$mv2 = “FooderLoader” wide ascii
$mv3 = “viper_execute” ascii
// Known C2-related patterns (genericized)
$c2_1 = “/gate.php” ascii
$c2_2 = “/index.php?id=” ascii
// MuddyWater obfuscation markers
$obf1 = “PowerShell -ExecutionPolicy Bypass” nocase
$obf2 = “Add-Type -TypeDefinition” nocase
// DLL loader characteristics
$dll1 = “ExportedFunction” ascii
$dll2 = “LoadLibraryA” ascii condition:
(uint16(0) == 0x5A4D) and 3 of ($ps*) and
1 of ($mv* or $dll* or $obf* or $c2_*)
}
```

**Recommendations Strategic**

- Incorporate Digital Risk Protection (DRP) as part of the overall security posture to proactively defend against impersonations and phishing attacks.
- Assess and deploy alternatives for an advanced endpoint protection solution that provides detection/prevention for malware and malicious activities that do not rely on signature-based detection methods.

**Management**

- Look for email security solutions that use ML- and AI-based anti-phishing technology for BEC protection to analyze conversation history to detect anomalies, as well as computer vision to analyze suspect links within emails.
- Regularly reinforce awareness of unauthorized attempts with end-users across the environment and emphasize the human weakness in mandatory information security training sessions.

**Tactical**

- Build and undertake safeguarding measures by monitoring/ blocking the IOCs and strengthening defence based on the tactical intelligence provided.
- For better protection coverage against email attacks (like spear phishing, business email compromise, or credential phishing attacks), organizations should augment built-in email security with layers that take a materially different approach to threat detection.
- Protect accounts with multi-factor authentication. Exert caution when opening email attachments or clicking on embedded links supplied via email communications, SMS, or messaging.
- Patch software/applications as soon as updates are available. Where feasible, automated remediation should be deployed since vulnerabilities are one of the top attack vectors.

- Add the YARA rule for threat detection and monitoring, which will help to detect anomalies in log events, identify and monitor suspicious activities.

## 3. Major Geopolitical Developments in Cybersecurity

**US and Canadian intelligence agencies outline a Chinese hacking campaign**
The U.S. Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Canadian Centre for Cyber Security have jointly released a report on a Chinese state-sponsored malware campaign dubbed BRICKSTORM. BRICKSTORM is a sophisticated backdoor that targets both VMware vSphere environments (primarily vCenter servers and ESXi hosts) and Windows systems. Once attackers gain access to a compromised vCenter management console, they can steal cloned virtual machine snapshots to extract credentials offline and deploy hidden, rogue virtual machines for persistent access and further operations.

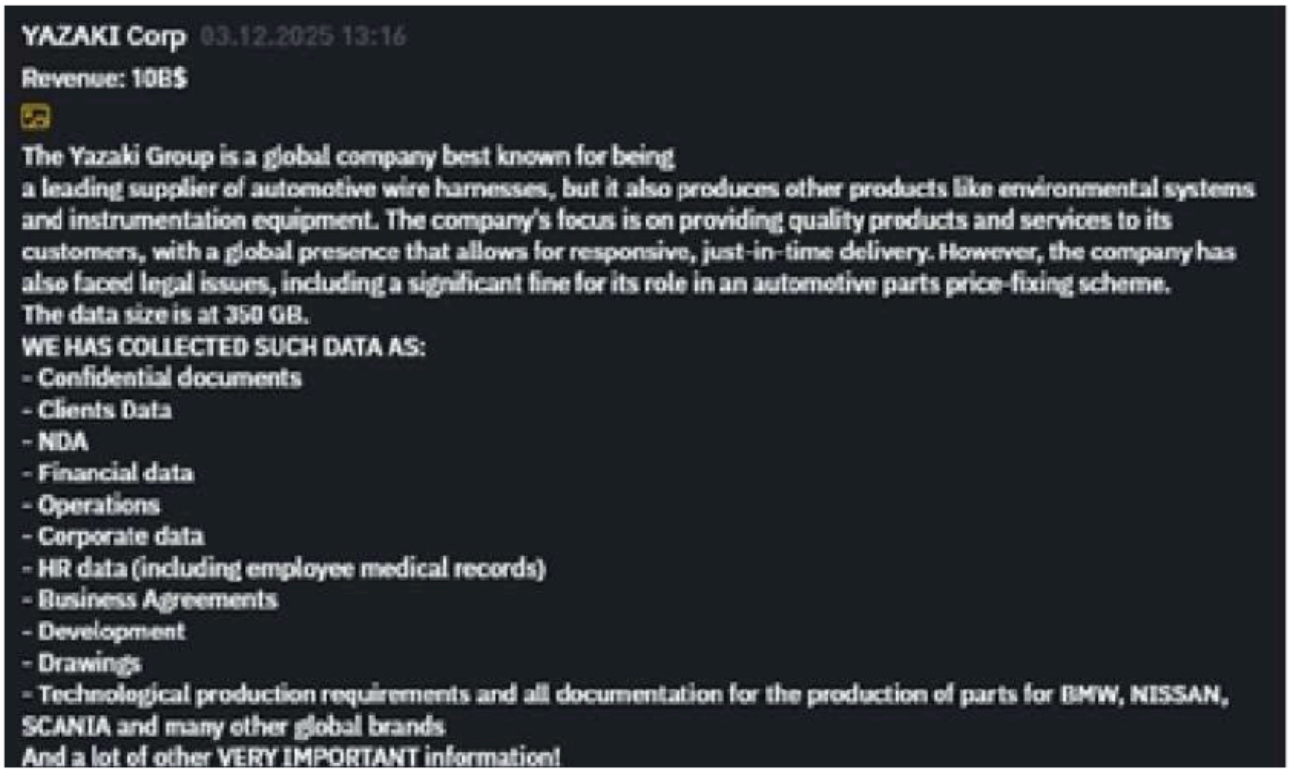
**ETLM Assessment:**
No specific APT designation (e.g., Volt Typhoon) has been publicly tied to the campaign yet, but it aligns with broader Chinese campaigns against critical infrastructure and especially accessing government entities and their classified data. The campaign highlights ongoing Chinese efforts to compromise virtualization infrastructure for espionage and long-term network persistence.

## 4. Rise in Malware/Ransomware and Phishing

INC Ransomware Impacts YAZAKI Corp

- Attack Type: Ransomware
- Target Industry: Manufacturing
- Target Geography: Japan
- Ransomware: INC Ransomware
- Objective: Data Theft, Data Encryption, Financial Gains
- Business Impact: Financial Loss, Data Loss, Reputational Damage

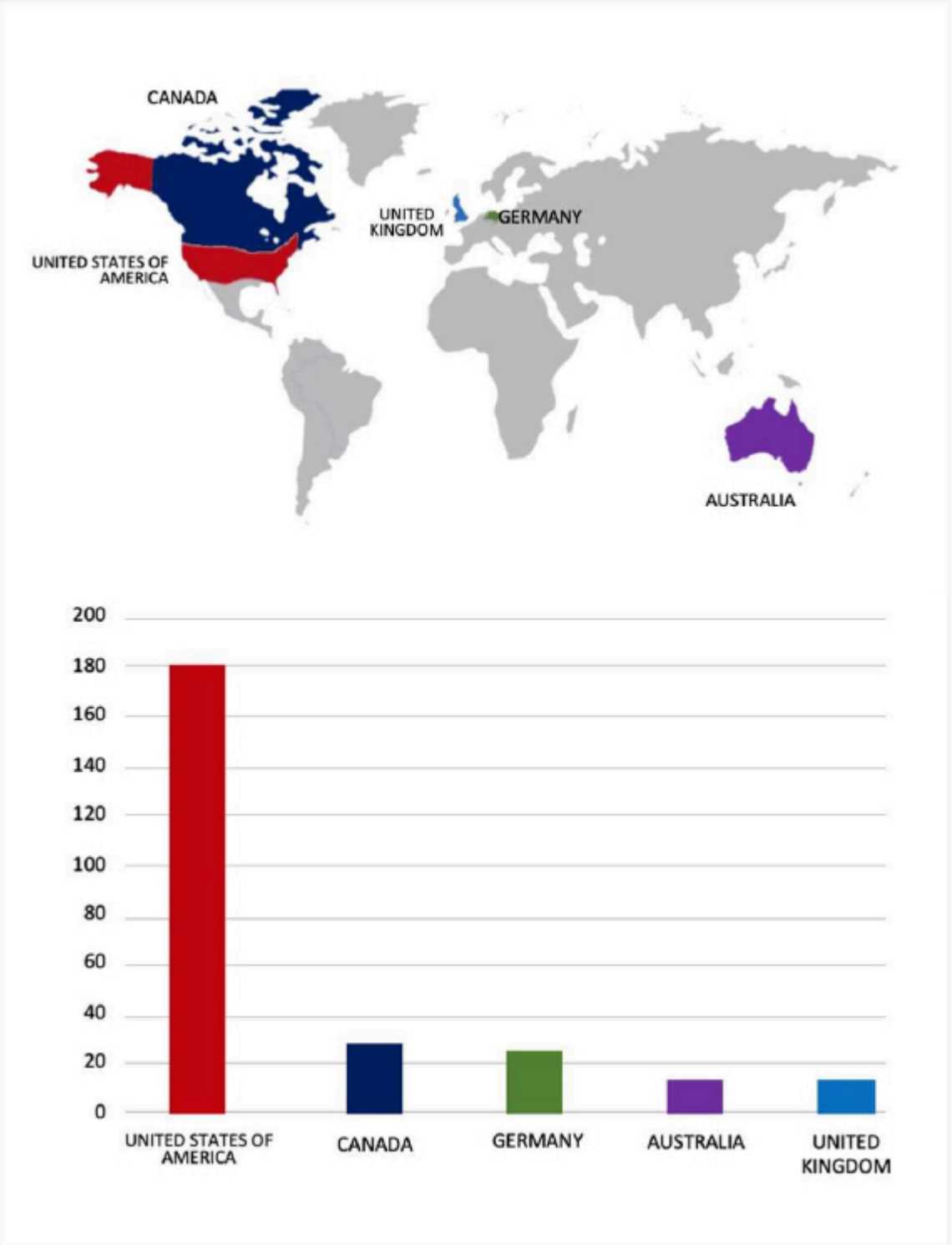
**Summary:**
CYFIRMA observed in an underground forum that a company from Japan, YAZAKI Corp (https[:]//www[.]yazaki-group[.]com/), was compromised by INC Ransomware. The Yazaki Group is a global company best known for being a leading supplier of automotive wire harnesses, but it also produces other products like environmental systems and instrumentation equipment. The compromised dataset includes a wide range of sensitive information, such as confidential documents, client data, non-disclosure agreements (NDAs), financial and operational records, corporate and HR data (including employee medical records), business agreements, development materials, technical drawings, technological production requirements, and complete documentation related to the manufacturing of parts for various clients. The total volume of exposed data is estimated to be approximately 350 GB.



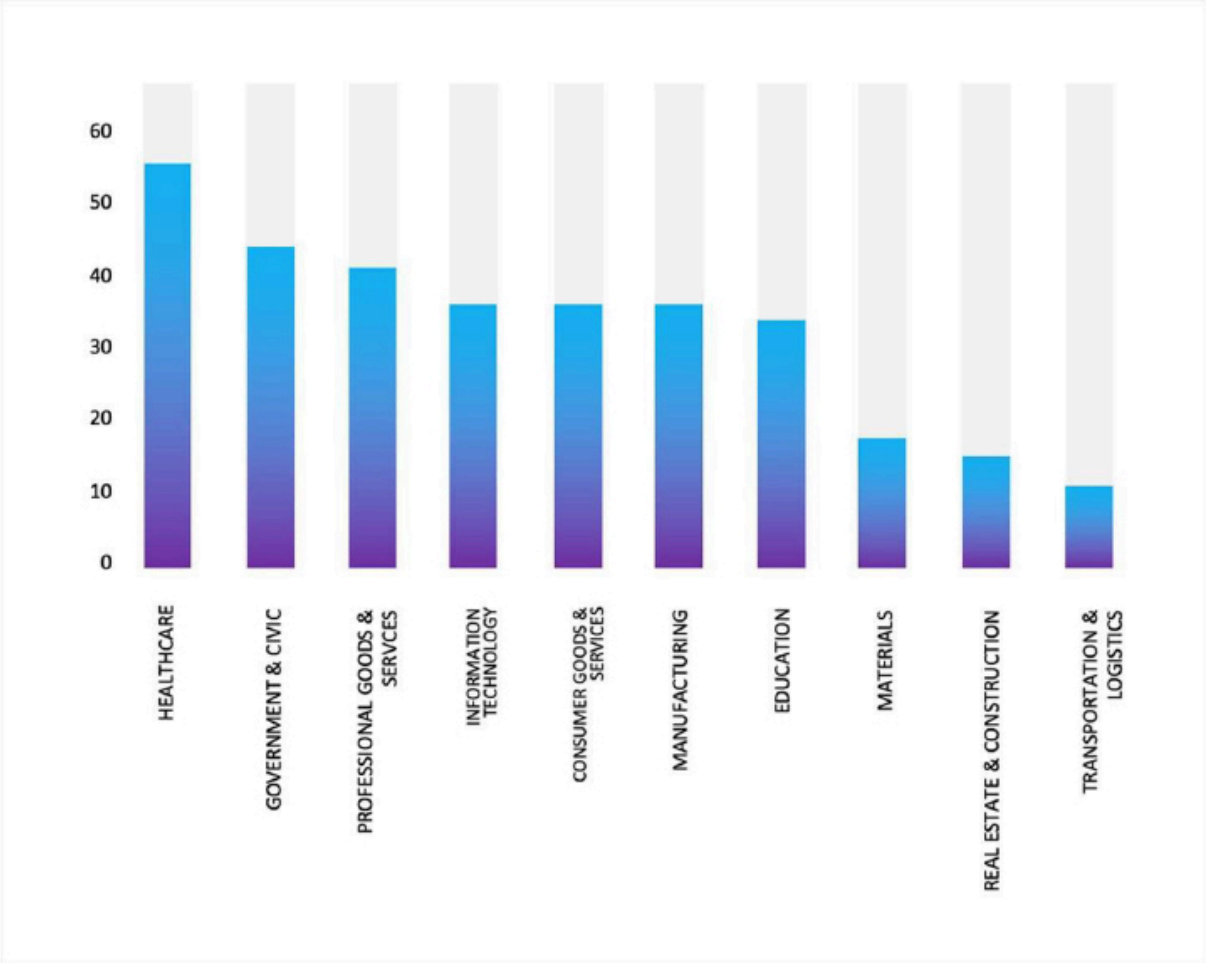

*Source: Dark Web*

**Relevancy & Insights:**

- INC Ransomware, also known as Incransom, is a cyber threat that emerged in mid-2023. Incransom uses strong encryption algorithms to lock files, making recovery without the decryption key virtually impossible. The ransomware typically appends specific file extensions to encrypted files, signalling that they have been compromised.
- Incransom is commonly distributed through:
- Phishing emails: Containing malicious attachments or links that, when opened, deploy the ransomware.
- Malicious downloads: From compromised websites or software packages.
- The INC Ransomware group primarily targets countries such as the United States of America, Canada, Germany, Australia, and the United Kingdom.
- The INC Ransomware group primarily targets industries, such as Healthcare, Government & Civic, Professional Goods & Services, Information Technology, and Consumer Goods & Services.
- Based on the INC Ransomware victims list from 1st Jan 2025 to 09th December 2025, the top 5 Target Countries are as follows:




- The Top 10 Industries most affected by the INC Ransomware victims list from 1st Jan 2025 to 09th December 2025 are as follows:




**ETLM Assessment:**

Based on recent assessments by CYFIRMA, INC Ransomware represents a significant threat within the evolving landscape of ransomware attacks. Its use of strong encryption methods and double extortion tactics highlights the increasing sophistication of cybercriminal operations. Organizations are advised to enhance their cybersecurity measures by implementing robust defenses against phishing attacks, maintaining updated security protocols, and monitoring for unusual network activity to mitigate risks associated with this and other ransomware variants.

Continuous vigilance is essential to protect against the threats posed by emerging ransomware groups like INC Ransomware.

**Lynx Ransomware Impacts TOC Co., Ltd**

- Attack Type: Ransomware
- Target Industry: Real Estate, Transportation and Logistics
- Target Geography: Japan
- Ransomware: Lynx Ransomware
- Objective: Data Theft, Data Encryption, Financial Gains
- Business Impact: Financial Loss, Data Loss, Reputational Damage

**Summary:**

CYFIRMA observed in an underground forum that a company from Japan, TOC Co., Ltd (www[.]toc[.]co[.]jp),

was compromised by Lynx Ransomware. The TOC Building is a commercial facility that provides a comprehensive floor guide, event information, and tenant details for visitors. The building hosts a variety of shops and services, including clothing stores, kitchenware, and cafes. It aims to attract a diverse clientele, including families and individuals looking for shopping and entertainment options. The compromised data contains confidential and sensitive information belonging to the organization.

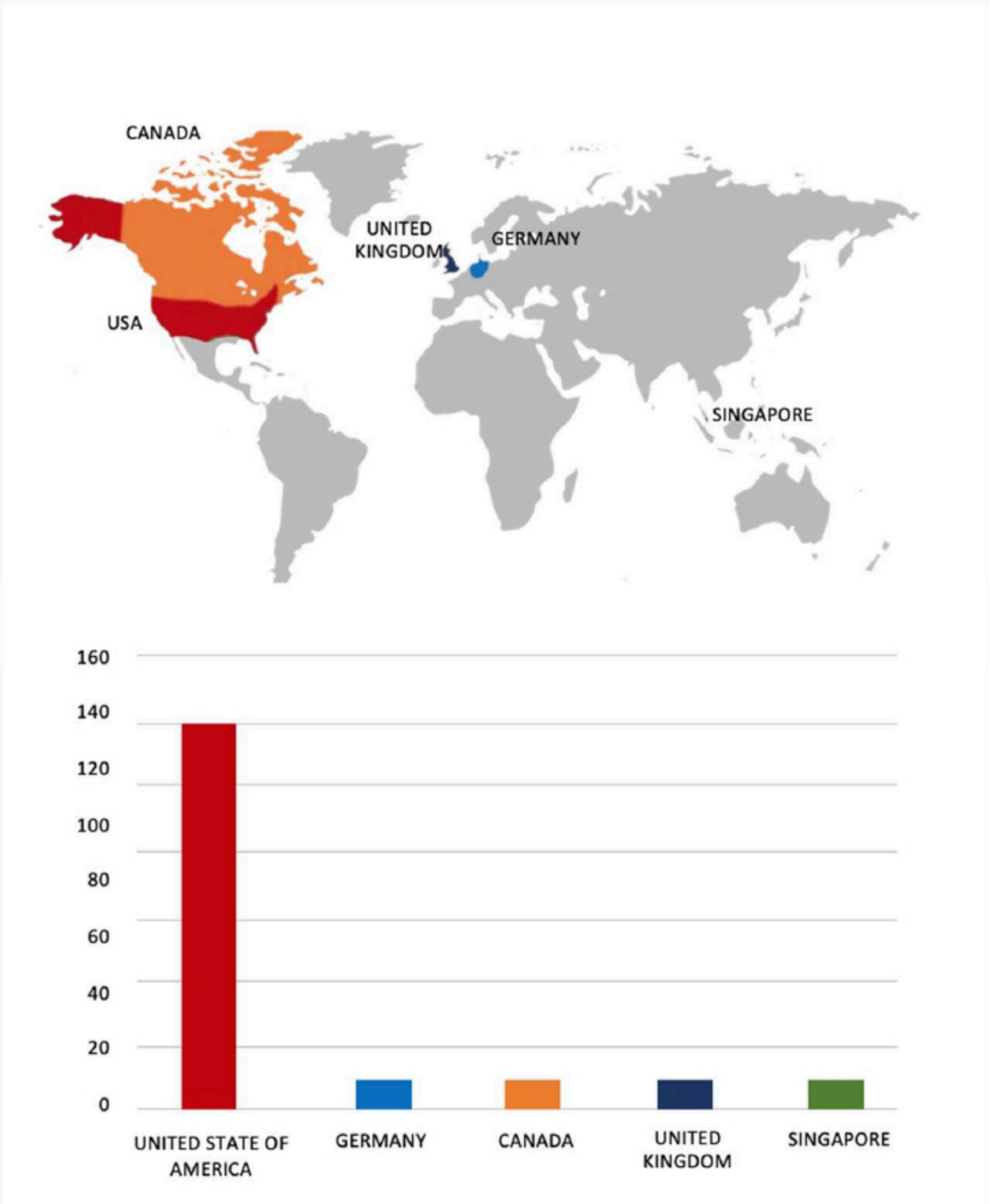


*Source: Dark Web*

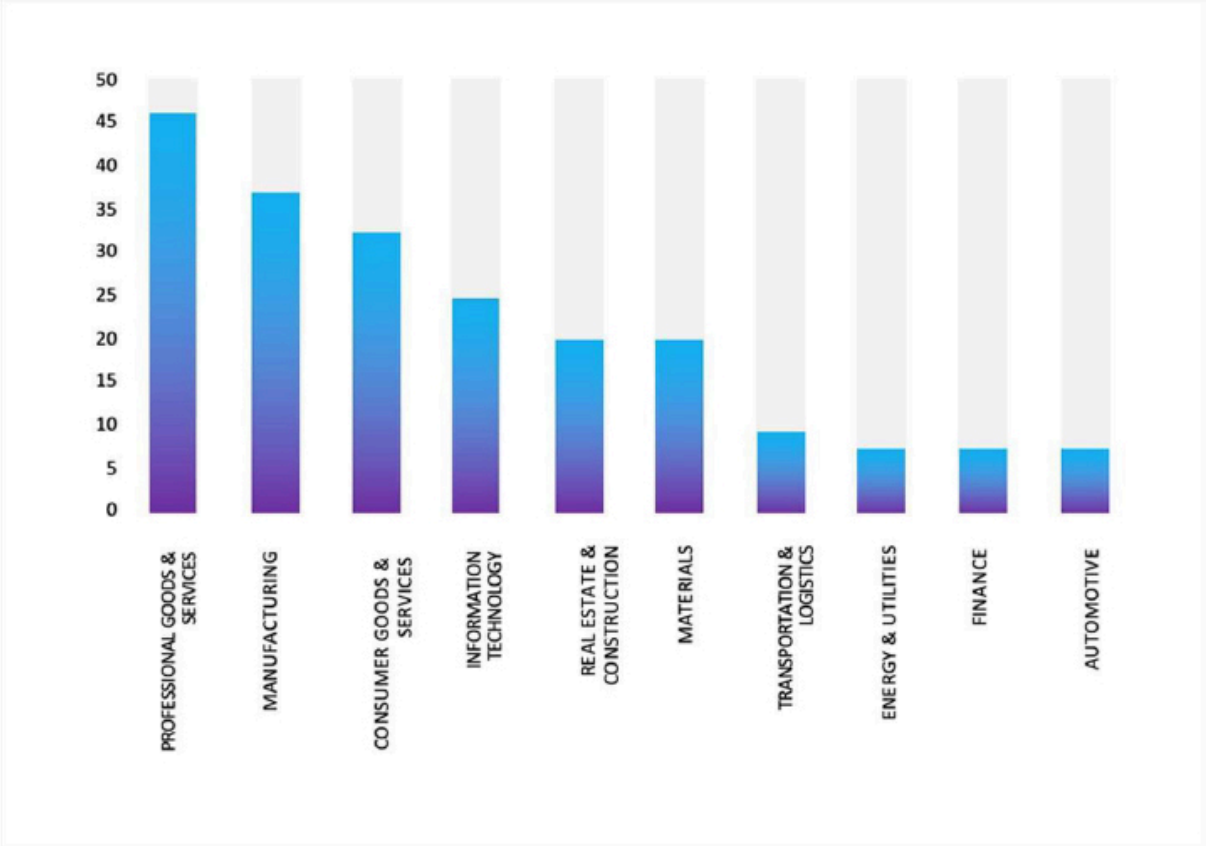
**Relevancy & Insights:**

- The Lynx Ransomware is confirmed to use a hybrid encryption approach, with AES-128 in CTR mode for fast file encryption and Curve25519 Donna for robust asymmetric key exchange, ensuring files are only recoverable with the attacker's private key.
- Lynx provides a comprehensive platform for affiliates, including tools for managing victims, negotiating ransoms, and sharing access with sub-affiliates.

- The Lynx Ransomware group primarily targets countries such as the United States of America, Germany, Canada, the United Kingdom, and Singapore.
- The Lynx Ransomware group primarily targets industries, including Professional Goods & Services, Manufacturing, Consumer Goods & Services, Information Technology, and Real Estate & Construction.
- Based on the Lynx Ransomware victims list from 1st Jan 2025 to 09th December 2025, the top 5 Target Countries are as follows:




- The Top 10 Industries most affected by the Lynx Ransomware victims list from 1st Jan 2025 to 09th December 2025 are as follows:




**ETLM Assessment:**

According to CYFIRMA's assessment, Lynx ransomware has emerged as a significant threat in the cybersecurity landscape, leveraging advanced encryption and double extortion tactics to target small and medium-sized businesses. Its structured affiliate program and versatile ransomware toolkit make it a formidable force in the RaaS ecosystem.

## 5. Vulnerabilities and Exploits

Vulnerability in PgBouncer

- Attack Type: Vulnerabilities & Exploits
- Target Technology: Server application
- Vulnerability: CVE-2025-12819
- CVSS Base Score: 7.5 Source
- Vulnerability Type: Untrusted Search Path
- Summary: The vulnerability allows a remote attacker to execute arbitrary SQL commands.

**Relevancy & Insights:**

The vulnerability exists due to the usage of an untrusted search path passed via the search_path parameter in the StartupMessage.

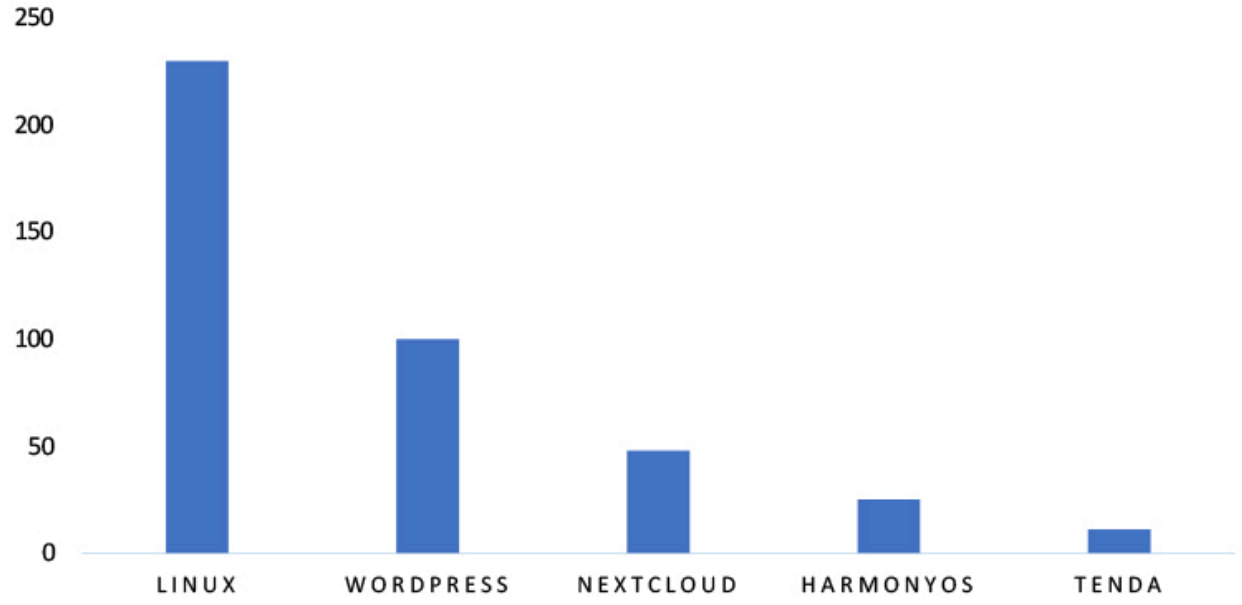
**Impact:**

A remote non-authenticated attacker can send a specially crafted request during authentication and execute arbitrary SQL commands in the database.

**Affected Products:**
https[:]//www[.]pgbouncer[.]org/changelog.html#pgbouncer- 125x

**Recommendations:**
Monitoring and Detection: Implement monitoring and detection mechanisms to identify unusual system behavior that might indicate an attempted exploitation of this vulnerability.

**TOP 5 AFFECTED TECHNOLOGIES OF THE WEEK**
This week, CYFIRMA researchers have observed significant impacts on various technologies due to a range of vulnerabilities. The following are the top 5 most affected technologies.




**ETLM Assessment**
Vulnerability in PgBouncer can pose significant threats to user privacy and database security. This can impact various industries globally, including technology, finance, healthcare, and enterprise IT. Ensuring the security of PgBouncer is crucial for maintaining the integrity and protection of PostgreSQL database connections worldwide. Therefore, addressing these vulnerabilities is essential to safeguarding connection pooling, authentication mechanisms, and database performance management across different geographic regions and sectors.

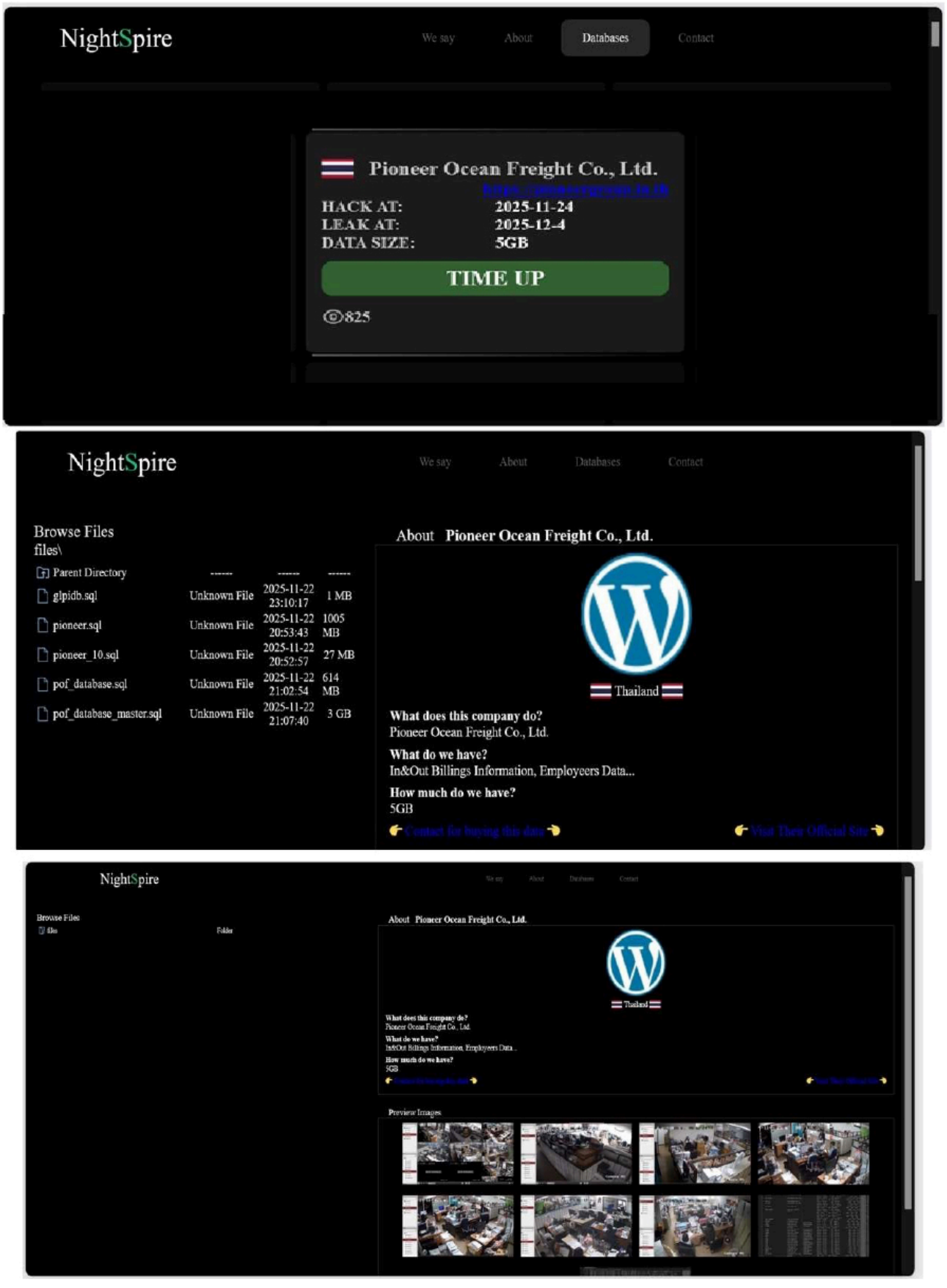
## 6. Latest Cyber-Attacks, Incidents, and Breaches

NightSpire Ransomware attacked and published the data of Pioneer Ocean Freight Co., Ltd.

- Threat Actor: NightSpire Ransomware
- Attack Type: Ransomware
- Objective: Data Leak, Financial Gains
- Target Technology: Web Applications
- Target Industry: Transportation and Logistics
- Target Geography: Thailand
- Business Impact: Operational Disruption, Data Loss, Financial Loss, Potential Reputational Damage

**Summary:**

Recently, we observed that NightSpire Ransomware attacked and published the data of Pioneer Ocean Freight Co., Ltd (https[:]//pioneergroup[.]in[.]th/) on its dark web website. Pioneer Group is a freight-forwarding and logistics company based in Thailand, providing sea-air freight forwarding, customs brokerage, inland & heavy- cargo transport, warehousing, packaging, and project-cargo services. The data leak resulting from the ransomware attack includes billing information (both incoming and outgoing), employee data, financial records, and other sensitive and confidential information. The total size of the compromised data is approximately 5 GB.




*Source: Dark Web*

**Relevancy & Insights:**

- NightSpire employs a double extortion strategy, encrypting data and threatening to leak stolen information unless a ransom is paid. This approach is typical of modern ransomware groups and adds pressure on victims to comply with demands.
- NightSpire's operations show strong influences from existing Ransomware-as-a- Service (RaaS) models, suggesting they might be an emerging group or a rebrand of an existing actor.

**ETLM Assessment:**
According to CYFIRMA's assessment, NightSpire is a new ransomware group that emerged in early 2025, marking itself as a formidable player in the rapidly evolving ransomware landscape. Despite its recent appearance, NightSpire has already gained attention for its aggressive tactics and well-structured operations.

## 7. Data Leaks

Bank Mandiri Data Advertised on a Leak Site

- Attack Type: Data leak
- Target Industry: Financial Services
- Target Geography: Indonesia
- Objective: Financial Gains
- Business Impact: Data Loss, Reputational Damage

Summary: The CYFIRMA research team has identified claims from a threat actor operating under the name "BreachLaboratory," who alleges responsibility for compromising Bank Mandiri.

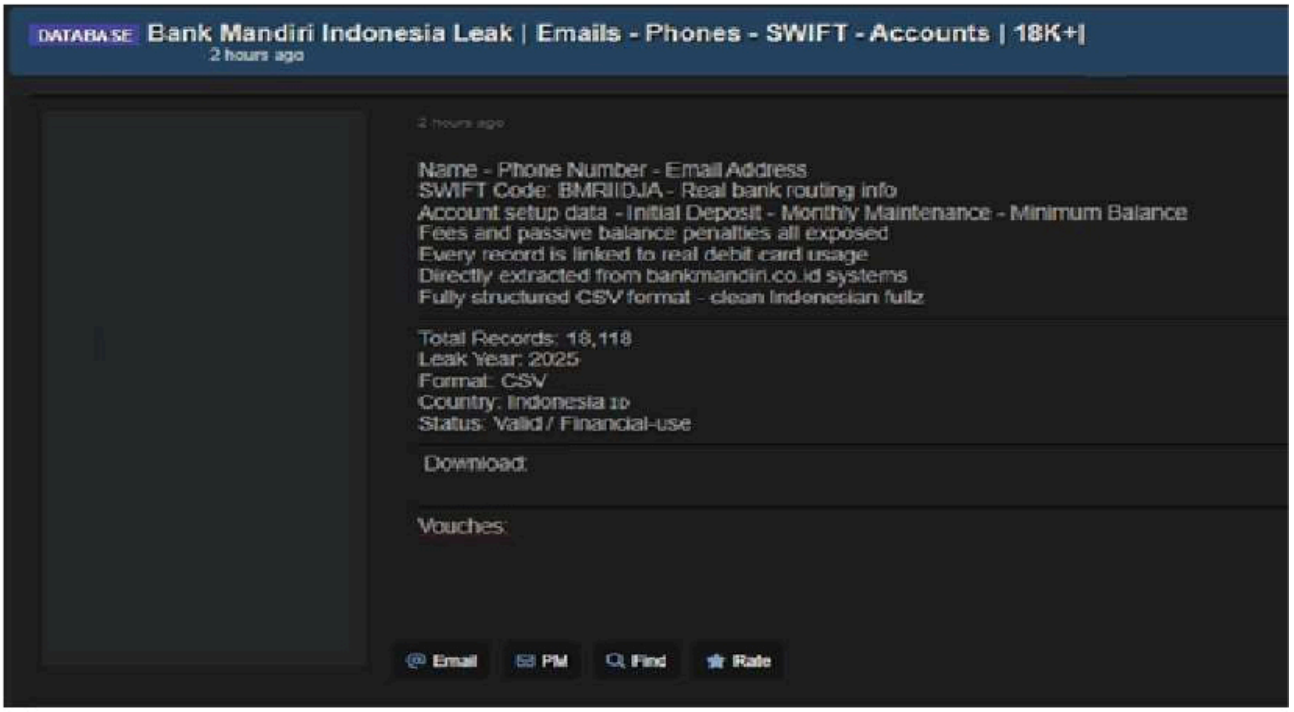
Bank Mandiri is Indonesia's largest bank by assets, providing a broad range of banking and financial services to both corporate clients and individual customers across the country.

According to the threat actor's claims, more than 18,000 financial records were leaked. The exposed data reportedly includes:

- Personal customer information
- SWIFT code: BMRIIDJA
- Account setup and configuration details
- Account balance information
- Fee-related data
- Debit card usage records

These allegations suggest a significant exposure of sensitive financial and customer- related information.Top of FormBottom of Form

The authenticity of this breach remains unverified at the time of reporting, as the claim originates solely from the threat actor.



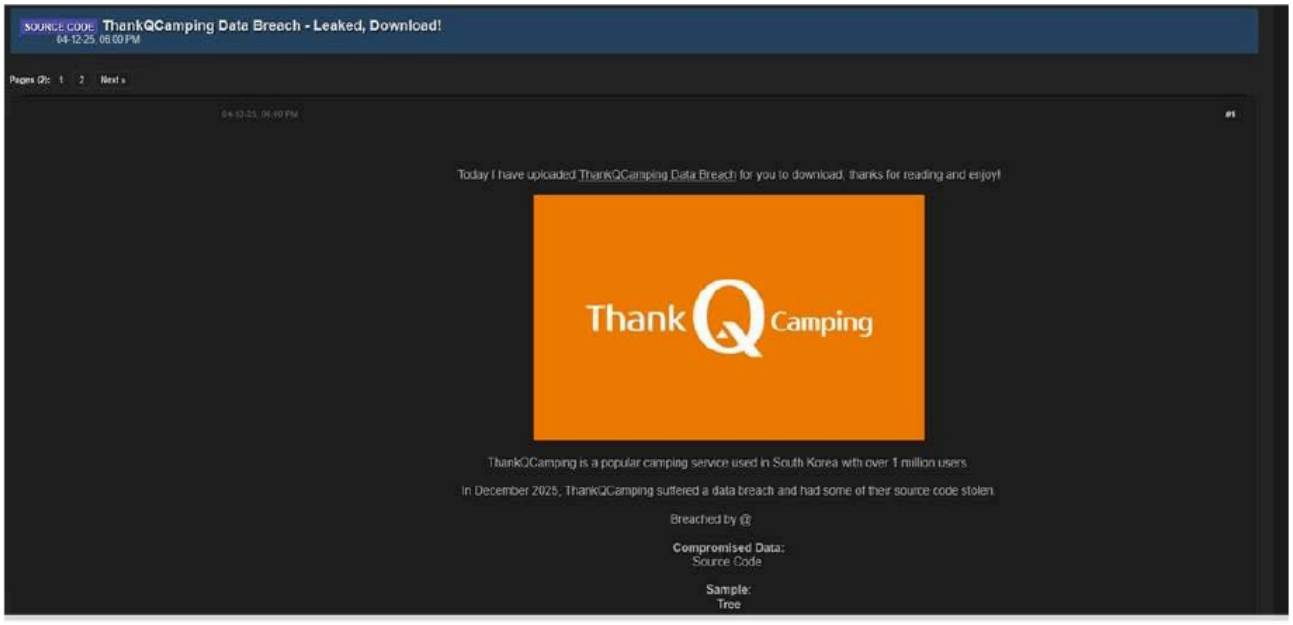

*Source: Underground Forums*

ThankQCamping Data Advertised on a Leak Site

- Attack Type: Data leak
- Target Industry: Outdoor Recreation and Travel
- Target Geography: South Korea
- Objective: Data Theft, Financial Gains
- Business Impact: Data Loss, Reputational Damage

**Summary:**
The CYFIRMA Research team has observed claims made by a threat actor identified as “888,” who alleges responsibility for a cybersecurity breach involving ThankQCamping. ThankQCamping is a well-known camping service platform in South Korea, reportedly serving over one million users nationwide. According to the threat actor, the incident took place in December 2025.

The actor claims that unauthorized access to ThankQCamping’s systems resulted in the theft of proprietary information, specifically the company’s source code. At the time of this report, there is no independent confirmation of the incident. The details shared are based solely on the threat actor’s statements, and the authenticity of the breach has not yet been verified.




*Source: Underground Forums*

**Relevancy & Insights:**
Financially motivated cybercriminals are continuously looking for exposed and vulnerable systems and applications to exploit. A significant number of these malicious actors congregate within underground forums, where they discuss cybercrime and trade stolen digital assets. Operating discreetly, these opportunistic attackers target unpatched systems or vulnerabilities in applications to gain access and steal valuable data. Subsequently, the stolen data is advertised for sale within underground markets, where it can be acquired, repurposed, and utilized by other malicious actors in further illicit activities.

**ETLM Assessment:**
The threat actor known as “888” is a highly active and sophisticated group specializing in data-leak operations. Multiple credible reports link the group to a series of security breaches involving unauthorized system access and the sale of stolen data across dark web marketplaces. Their activities reflect the persistent and rapidly evolving cyber threats emerging from underground communities. These incidents reinforce the need for organizations to strengthen their cybersecurity posture through continuous monitoring, advanced threat-intelligence capabilities, and proactive defense measures to safeguard sensitive data and critical infrastructure.

**Recommendations: Enhance the cybersecurity posture by:**

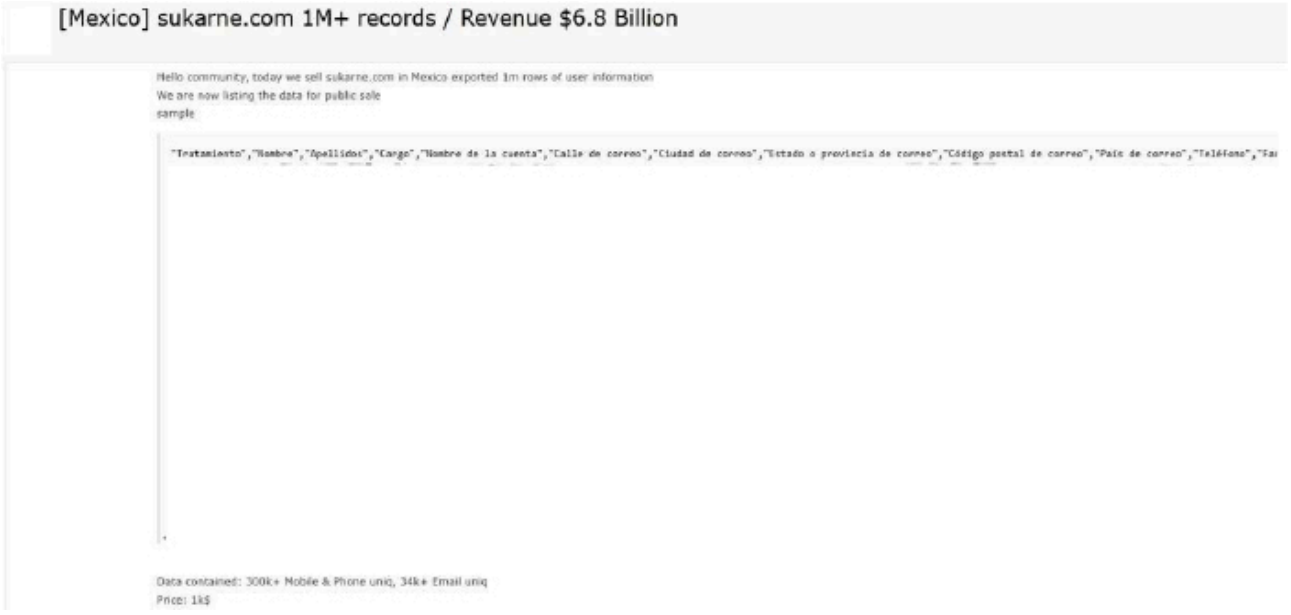
1. Updating all software products to their latest versions is essential to mitigate the risk of vulnerabilities being exploited.
2. Ensure proper database configuration to mitigate the risk of database-related attacks.
3. Establish robust password management policies, incorporating multi-factor authentication and role-based access to fortify credential security and prevent unauthorized access.

## 8. Other Observations

The CYFIRMA Research team observed that SuKarne, a Mexican multinational corporation and a major player in the global meat processing industry with reported revenues of $6.8 billion, has allegedly been compromised. A threat actor attempting to sell data on a dark web forum claims to have exported a database containing over 1 million rows of user and business information. The dataset is currently listed for sale for $1,000.
According to the actor, the compromised data includes 300,000+ unique mobile numbers and 34,000+ unique email addresses. Based on the sample logs provided, the exposed fields appear to cover:

- Full names (Nombre, Apellidos)
- Physical addresses (Street, City, State, Zip Code)
- Email addresses (Personal and corporate)
- Phone and mobile numbers
- Dates of birth
- Tax IDs (RFC) and National Identity Codes (CURP)
- Bank account numbers and financial keys (No. Cuenta Bancaria, Clave de Banco)
- Job titles and department details
- Annual revenue figures and credit limits

The authenticity of this breach remains unverified at the time of reporting, as the claim originates solely from the threat actor.




*Source: Underground Forums*

The CYFIRMA Research team has identified claims from a threat actor alleging a data breach involving Volkswagen Mandi, which the actor describes as the target of a cyber incident in December 2025. The claim was posted on a cybercrime forum, where the threat actor asserts that a large database was exfiltrated from the affected entity. Although the actor explicitly references “Volkswagen Mandi”— potentially pointing to a dealership located in Mandi, Himachal Pradesh, or an internally labeled database—the breadth of the sample data raises concerns of a much wider impact. Data samples reportedly contain addresses from multiple Indian states, including

Maharashtra, Tamil Nadu, Madhya Pradesh, and Kerala, indicating that the breach may involve a centralized CRM or lead management system connected to Volkswagen operations across India.

According to the threat actor, the allegedly compromised dataset consists of more than 2.5 million records, encompassing approximately 1.7 million unique phone numbers and 2.1 million unique email addresses. The structure and identifiers present in the data suggest it may originate from a Customer Relationship Management (CRM) platform, with references to systems such as Salesforce and Zoho. If accurate, the exposure could have significant implications due to the volume and sensitivity of the information involved.

The data allegedly exposed in the breach includes the following categories:

**Identity Information:**
Salutations, first and last names, titles, and other personal identifiers.

**Contact Details:**
Mobile numbers, landline phone numbers, fax numbers, and both business and personal email addresses.

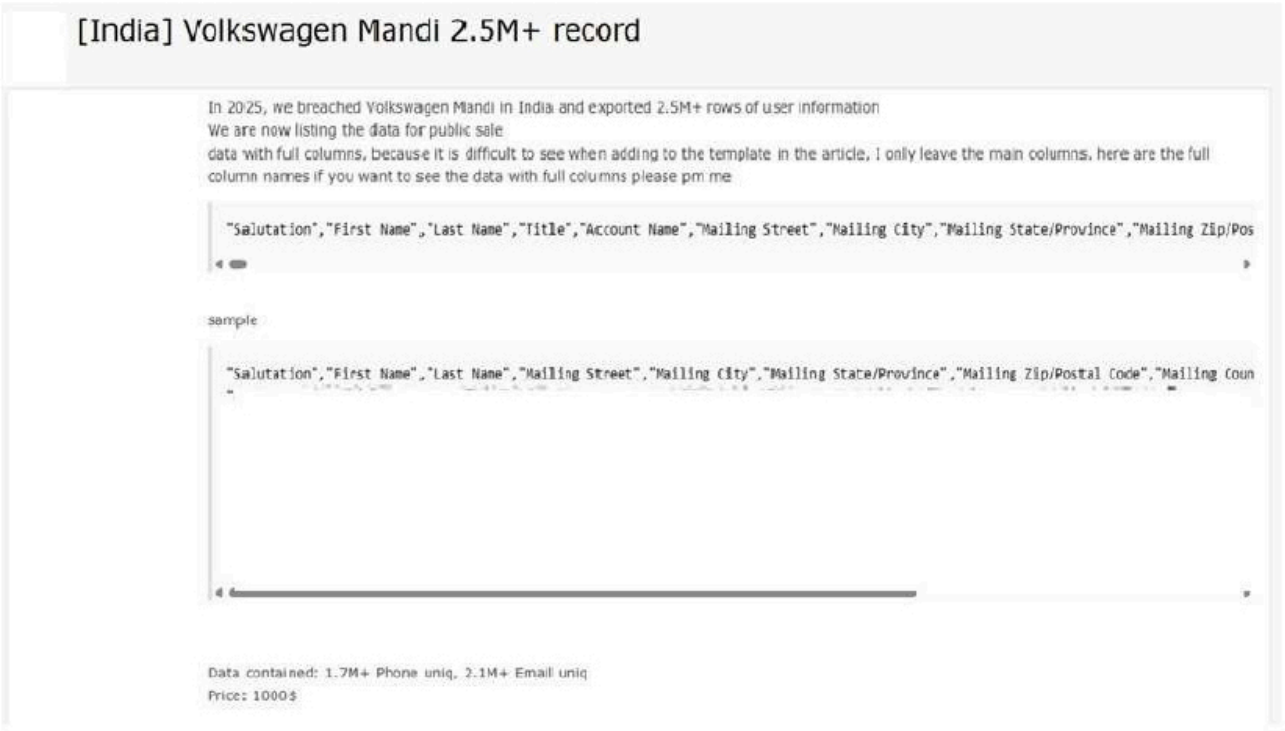
**Physical Address Information:**
Complete mailing, billing, and shipping addresses, including street details, cities, states/provinces, postal/ZIP codes, and countries.

**Vehicle-Related Information:**
Vehicle Identification Numbers (VINs), vehicle details, registration numbers, and test drive history.

**Account and Dealer Data:**
Account IDs, account owners, dealer codes, dealer city information, and system identifiers such as Zoho IDs and Data.com keys.

**Internal and Operational Records:**
Lead source information, purchase agreements, warranty details, service manager names, customer feedback, and service-related logs.

At the time of reporting, these claims remain unverified and are based solely on assertions made by the threat actor. Further validation is required to confirm the authenticity, scope, and impact of the alleged breach.




*Source: Underground Forums*

**STRATEGIC RECOMMENDATIONS**

- Attack Surface Management should be adopted by organisations, ensuring that a continuous closed-loop process is created between attack surface monitoring and security testing.
- Delay a unified threat management strategy – including malware detection, deep learning neural networks, and anti-exploit technology – combined with vulnerability and risk mitigation processes.
- Incorporate Digital Risk Protection (DRP) in the overall security posture that acts as a proactive defence against external threats targeting unsuspecting customers.
- Implement a holistic security strategy that includes controls for attack surface reduction, effective patch management, and active network monitoring, through next-generation security solutions and a ready-to-go incident response plan.
- Create risk-based vulnerability management with deep knowledge about each asset. Assign a triaged risk score based on the type of vulnerability and criticality of the asset to help ensure that the most severe and dangerous vulnerabilities are dealt with first.

**MANAGEMENT RECOMMENDATIONS**

- Take advantage of global Cyber Intelligence, providing valuable insights on threat actor activity, detection, and mitigation techniques.
- Proactively monitor the effectiveness of risk-based information security strategy, the security controls applied, and the proper implementation of security technologies, followed by corrective actions, remediations, and lessons learned.
- Consider implementing Network Traffic Analysis (NTA) and Network Detection and Response (NDR) security systems to compensate for the shortcomings of EDR and SIEM solutions.

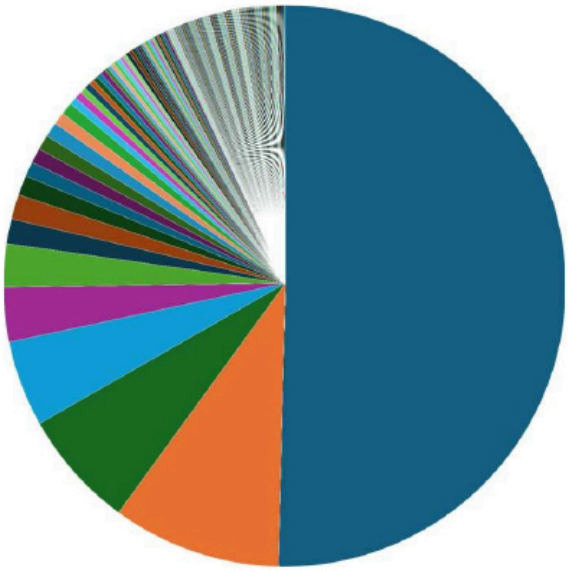
- Detection processes are tested to ensure awareness of anomalous events. Timely communication of anomalies and continuously evolved to keep up with refined ransomware threats.

**TACTICAL RECOMMENDATIONS**

- Patch software/applications as soon as updates are available. Where feasible, automated remediation should be deployed since vulnerabilities are one of the top attack vectors.
- Consider using security automation to speed up threat detection, improved incident response, increased the visibility of security metrics, and rapid execution of security checklists.
- Build and undertake safeguarding measures by monitoring/ blocking the IOCs and strengthening defences based on the tactical intelligence provided.
- Deploy detection technologies that are behavioral anomaly-based to detect ransomware attacks and help to take appropriate measures.
- Implement a combination of security control such as reCAPTCHA (completely Automated Public Turing test to tell Computers and Humans Apart), Device fingerprinting, IP backlisting, Rate-limiting, and Account lockout to thwart automated brute-force attacks.
- Ensure email and web content filtering uses real-time blocklists, reputation services, and other similar mechanisms to avoid accepting content from known and potentially malicious sources.

## Situational Awareness – Cyber News

Please find the Geography-Wise and Industry-Wise breakup of cyber news for the last 5 days as part of the situational awareness pillar.

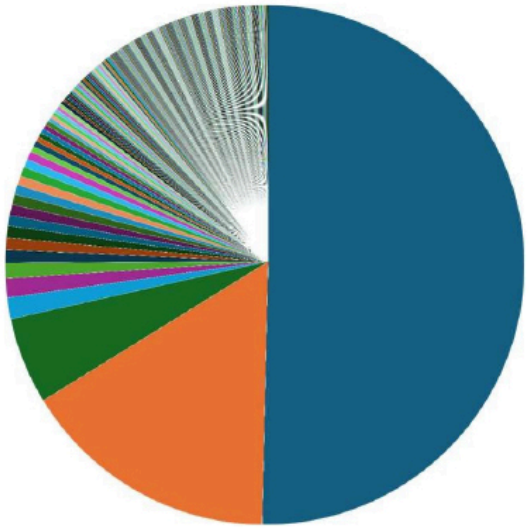


## Geography-Wise Graph

- Worldwide
- India
- United States
- United Kingdom
- China
- Global
- Morocco
- Hong Kong
- Japan
- Russia
- Falkland Islands
- Thailand
- Europe
- Peru
- Indonesia
- Asia
- Brazil
- United Arab Emirates
- Myanmar, India
- Canada
- Australia
- China, Taiwan
- Spain
- Georgia, United States
- Cambodia
- Venezuela, United States
- Hong Kong, Worldwide, North Korea
- Singapore
- Pakistan
- United States, Georgia
- United States, China
- Pakistan, India
- Iran
- Norway
- United States, Ukraine, Russia
- Bangladesh
- Falkland Islands, United States
- Italy
- Morocco, France
- Europe, Global
- Global, China
- Philippines
- Africa, Ethiopia
- Belgium
- Morocco, Belgium
- Vietnam
- Hong Kong, Russia, North Korea
- South Korea
- United States, United Kingdom
- Hong Kong, North Korea
- Global, Russia, Hong Kong, North Korea
- Taiwan
- Vietnam, United States, United Kingdom
- Jamaica
- Mexico
- Thailand, Spain
- Hong Kong, Tanzania, Aruba, Jersey, Global, India
- United States, China, Russia
- China, Japan, Taiwan
- Global, Europe, India, United States
- China, Russia
- United Arab Emirates, Germany
- India, Myanmar
- United States, Thailand, Russia
- India, Pakistan
- Saudi Arabia, Morocco
- India, United States
- Taiwan, Russia
- Belize
- Ukraine
- China, Ukraine, Russia, India
- United Kingdom, Kyrgyzstan, Russia
- Iran, Asia
- United States, India
- Israel
- United States, United Kingdom, Australia, Nepal, Global, India
- Israel, Iran, Sri Lanka
- Hong Kong, United States, North Korea
- Denmark
- Singapore, Vietnam
- Ecuador, Colombia, China, Yemen
- Sweden
- Egypt
- Global, Spain
- Japan, Hong Kong
- Turkey
- Japan, Laos
- Greece, Europe, France, Bulgaria, Germany, Albania
- Japan, United Kingdom
- United Kingdom, Australia, Russia
- Jersey
- Greece, United States
- Kenya
- Belgium, France
- Lebanon, Kuwait, Turkey, Iran, Global, Saudi Arabia
- United States, Nigeria
- Lebanon, Morocco, United States, Egypt, Jordan
- Hong Kong, Global, Russia, North Korea
- Mauritania, Morocco
- Venezuela
- Bangladesh, Vietnam, China, Thailand, India
- Vietnam, Singapore
- Mexico, Malaysia, Global
- Hong Kong, Worldwide, Global, Russia, North Korea
- Europe, France
- Global, China, Europe, Iran, Australia, Russia, United States, United Kingdom

- Somalia, Sudan
- Morocco, Brazil
- Global, India
- Europe, Slovakia
- Canada, United States, Europe, United Kingdom, Australia
- Morocco, Iran
- Tanzania
- Morocco, Macao
- Thailand, Myanmar
- Morocco, Macao, Egypt
- Thailand, Taiwan, Russia, Global, United States
- Morocco, United States
- Turkey, United States
- Myanmar
- Ukraine, Russia
- Myanmar, Cambodia, India
- United Arab Emirates, Europe, Russia, United States
- Australia, United States, United Kingdom
- Greece, Russia, Ukraine
- Myanmar, Thailand, India
- United Kingdom, Global
- Myanmar, United States
- United Kingdom, Russia
- Namibia
- Guernsey, Hong Kong, United Kingdom, Montenegro
- Netherlands, Morocco, United Kingdom
- United States, Denmark, Malaysia, Australia
- New Zealand, Australia
- United States, Global
- Niger, Africa
- United States, Mexico
- Nigeria, Global
- United States, Russia
- Falkland Islands, United Kingdom
- United States, Ukraine
- Belgium, Europe, India

- China, Global
- Canada, India
- Uzbekistan
- Panama
- China, Indonesia
- Canada, Singapore, Japan, United Kingdom, France
- Vietnam, Asia
- Global, Australia, Canada, Netherlands, Russia, United States, United Kingdom, New Zealand
- Hong Kong, United States, North America
- RÃ©union
- Worldwide, Russia
- Romania
- Canada, United States

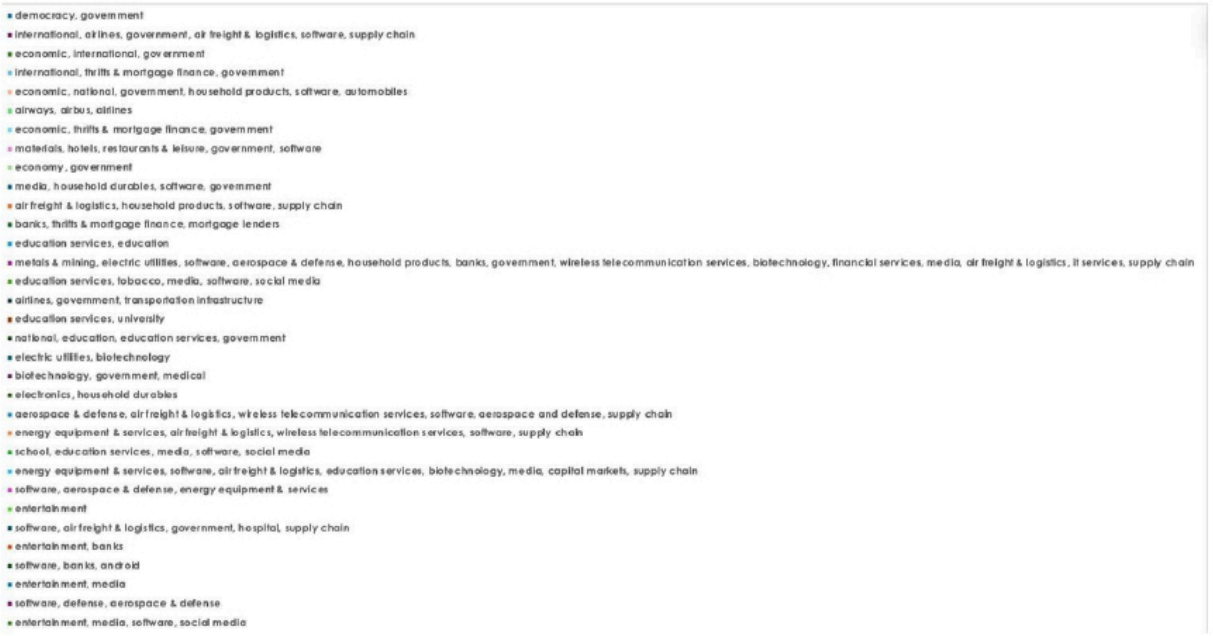


## Industry-Wise Graph

- No Specific Industry
- software
- government
- air freight & logistics, supply chain
- banks
- household durables
- media
- banks, software, internet banking
- university, education services
- software, banks
- capital markets
- airlines
- household products
- education services
- international, government
- national, government
- software, air freight & logistics, supply chain
- world, government
- air freight & logistics, software, supply chain
- computer, household products
- aerospace & defense
- media, software, social media
- defense, aerospace & defense
- college, education services
- software, government
- automobiles
- nissan, automobiles
- antivirus, software
- banks, savings bank
- equity real estate investment trusts (reits), real estate
- air freight & logistics
- it services
- banks, thrifts & mortgage finance, equity real estate investment trusts (reits), real estate

- metals & mining
- biotechnology
- software, air freight & logistics
- biotechnology, medical
- household durables, software
- national, materials, government
- airlines, software
- financial services, equity real estate investment trusts (reits), real estate
- government, software
- banks, equity real estate investment trusts (reits), real estate
- software, education services
- salt, metals & mining
- software, cloud computing
- government, airlines
- banking, banks
- medical, biotechnology
- household products, government
- ministry, government
- insurance
- exploits, software
- airlines, air freight & logistics, supply chain
- school, education services
- it services, office 365
- software, biotechnology
- materials
- media, government
- household durables, wireless telecommunication services
- thrifts & mortgage finance
- hospital
- air freight & logistics, supply chain, banks
- banks, thrifts & mortgage finance, equity real estate investment trusts (reits), real estate, banking
- capital markets, software
- capital markets, software, media

- national, at&t, transportation, government, metals & mining, wireless telecommunication services, transportation infrastructure, software
- cars, vehicles, automobiles
- capital markets, financial services
- chemicals
- banks, software
- clinic, biotechnology
- medical, biotechnology, household durables
- clothing, media, software, household products, social media
- national, publishing, media, government
- at&t, wireless telecommunication services
- software, banking, banks
- comments, banks
- software, media, entertainment
- comments, government
- international, government, media
- computer, air freight & logistics, household products, software, supply chain
- logistics, software, air freight & logistics, mobile app
- air freight & logistics, banks, software, supply chain
- media, software, air freight & logistics, supply chain
- computer, household products, airlines
- military, aerospace & defense
- computer, software, household products, government, aerospace & defense
- national, government, wireless telecommunication services, software, mobile services
- database, software
- biotechnology, software
- database, software, equity real estate investment trusts (reits), real, estate, real estate
- software, air freight & logistics, antivirus
- airlines, government, transportation infrastructure, air travel
- software, browsers
- defense, android, aircraft, software, materials, media, airlines, aerospace & defense, it services, banks, capital markets, government, infrastructure services, microsoft azure, operating system
- software, government, banks
- defense, telecommunications, wireless telecommunication services, aerospace & defense, metals & mining
- software, vulnerabilities





For situational awareness intelligence and specific insights mapped to your organisation’s geography, industry, and technology, please access DeCYFIR.

---

Source: https://www.cyfirma.com/news/weekly-intelligence-report-12-december-2025/#:~:text=well%2Dstructured%20operations.-,7.%20Data%20Leaks,-Bank%20Mandiri%20Data