EnCyb

TLP:GREEN

The Intel Bulletin

May 2026

A Monthly Threat Intelligence Overview

Prepared By
EnCyb TI Team

www.encyb.com | threatintelligence@encyb.com
Social: LinkedIn | X | Facebook |
PCI QSA | CERT-IN Empaneled | ISO 27001 & ISO 9001 Certified|
SWIFT - Cyber Security Partner
India| Middle East | USA | UK

CONTENTS

Executive Summary 3
Global Threat Overview 3
Top 5 Target Countries 3
Top 5 Target Sectors 3
Top 5 Risks Breakdown 4
Top 5 Active Malwares 4
Notable Events 5
Cyber Incidents Amid Iran–Israel Context 12
Vulnerability & Exploit Intelligence 19
MITRE ATT&CK / TTP Mapping 21
Recommendations 22
Appendix 23

Note:

- *The screenshot figures are being exposed by threat actors or victims.*
- *The report is strictly for intended audience only.*
- *Do not expose it outside the organization.*

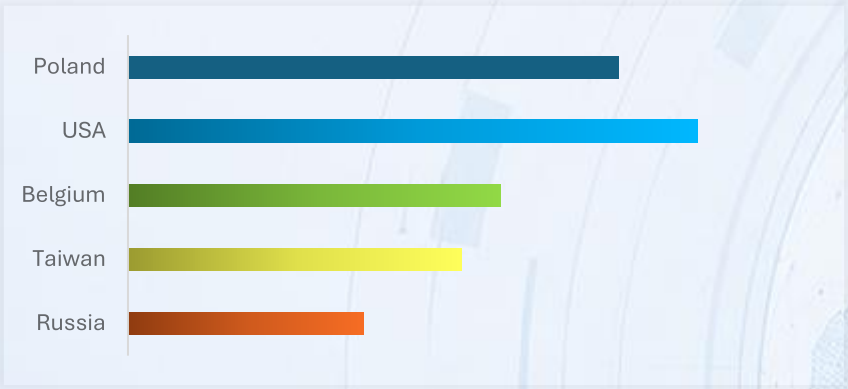
Executive Summary

May 2026 witnessed a significant escalation in global cyber threat activity, characterized by large-scale data breaches, ransomware operations, supply-chain compromises, state-sponsored espionage campaigns, and cyber activities linked to ongoing geopolitical tensions in the Middle East. Threat actors increasingly targeted educational institutions, telecommunications providers, software supply chains, critical infrastructure, cloud environments, and public-sector organizations.

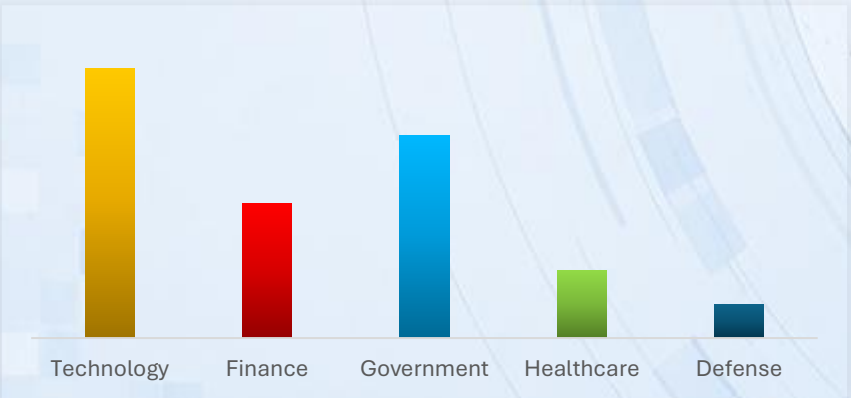
The reporting period was dominated by the activities of ShinyHunters, which claimed responsibility for multiple high-profile data breaches affecting educational institutions, 7-Eleven, Udemy, and several global brands. Advanced persistent threat (APT) groups linked to Iran and China demonstrated sophisticated cyber-espionage capabilities through campaigns involving Showboat (EvaRAT), Dindoor, Fakeset, MiniUpdate, and MiniJunk V2 malware families.

Global Threat Overview

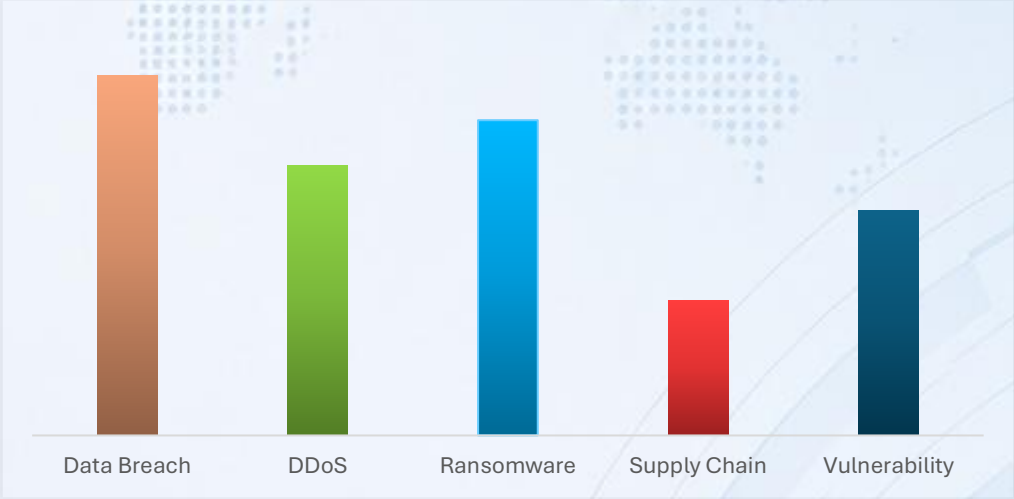
Top 5 Target Countries



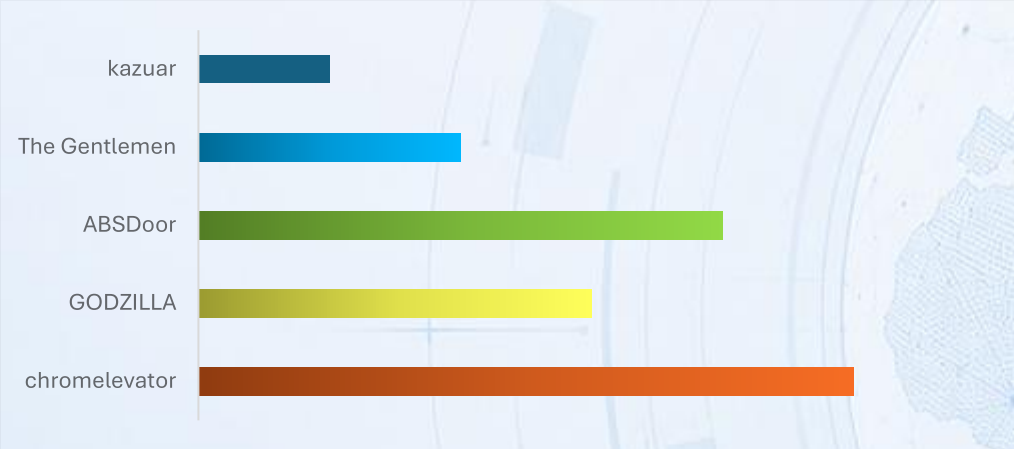
Top 5 Target Sectors



Top 5 Risks Breakdown



Top 5 Active Malwares



Notable Events

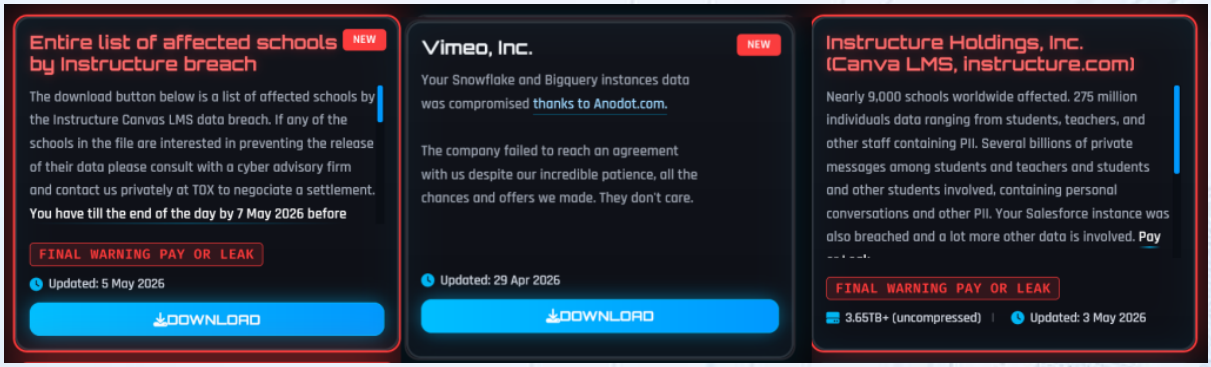
A summary of significant cyber incidents, threat actor activities, and major cybersecurity developments observed during the reporting period, with focus on events linked to ongoing geopolitical tensions and emerging cyber threats.

The Canvas Platform Mass Breach

A massive data breach impacted nearly **9,000 educational institutions worldwide**, including top-tier universities like Stanford, Harvard, UC Berkeley, and the National University of Singapore. The threat actors compromised **3.5 terabytes of data** belonging to roughly 275 million students and staff.

Threat Actor : ShinyHunters

ShinyHunters allege they have stolen data including names, email addresses, student IDs, and billions of private messages. They have given Instructure and affected schools until May 12 to negotiate payment or face public leaks. While Instructure disputes the scope, the group claims the breach could affect up to **275 million individuals**, making it one of the largest education-related data thefts if confirmed.



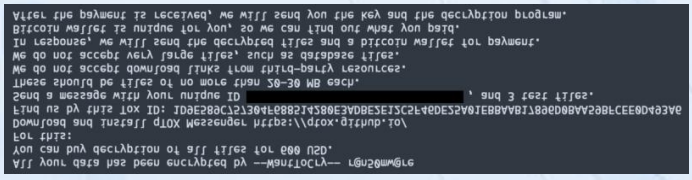
ShinyHunters' Data Leak Site Listing Data Stolen from Instructure and Vimeo.

WantToCry Remote Encryption Attacks

Malware : WantToCry Ransomware

Security researchers observed a surge in a new ransomware strain dubbed WantToCry (a nod to the infamous 2017 WannaCry). This variant aggressively targets exposed Server Message Block (SMB) services through brute-force attacks.

Evasion Tactic: It is highly evasive because it operates without local malware execution; instead, it exfiltrates data to attacker-controlled infrastructure and remotely encrypt/rewrites the files back onto the victim's disk, significantly minimizing the local Endpoint Detection and Response (EDR) footprint.



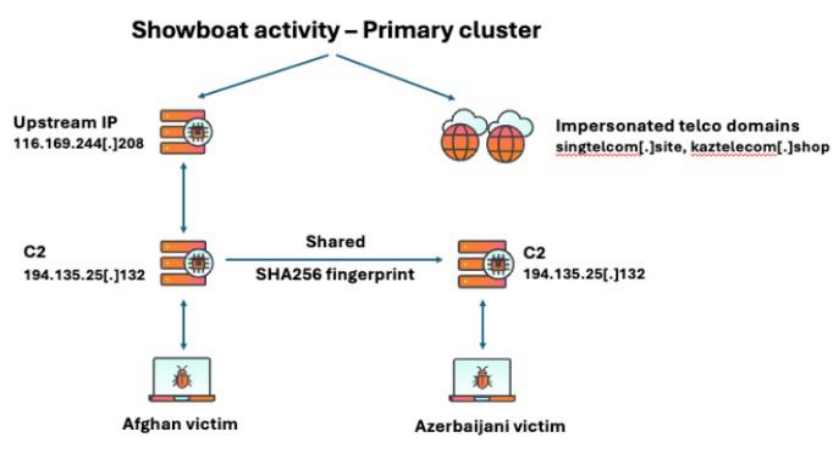
Ransom note observed in WantToCry attacks

"Showboat" Linux Telecom Espionage Framework

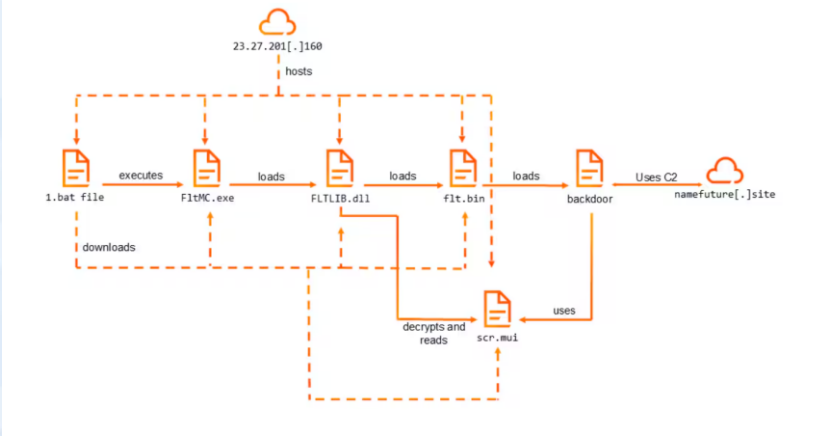
Security researchers observed a surge in a long-running, targeted cyber-espionage campaign deploying a newly uncovered Linux post-exploitation framework called Showboat (also tracked as EvaRAT). Attributed to Chinese state-aligned threat actors—specifically Calypso (also tracked as Red Lamassu or Bronze Medley)—this framework aggressively targets telecommunications providers and internet service providers (ISPs) across the Middle East and Central Asia. The backdoor functions by spawning remote interactive shells and dynamically establishing internal SOCKS5 proxies to systematically enumerate, compromise, and map out target local area networks (LAN).

Threat Actor : Calypso (Red Lamassu / Bronze Medley)
Target Verticals: Telecommunications, Internet Service Providers (ISPs), Critical Infrastructure (Middle East / Central Asia)

Evasion Tactic: It is highly evasive because it isolates malicious staging actions within internal network perimeters; instead of making frequent, suspicious outbound communication channels that would trigger boundary firewalls, it proxies its traffic through interior infrastructure. To hide its execution footprint on compromised Linux nodes, the malware creates local process wrappers masquerading as legitimate system threads (such as kworker) and utilizes external public clipboard utilities like Pastebin to dynamically fetch obfuscated configuration blocks, allowing the framework to maintain long-term persistence while minimizing the local security footprint.



Primary cluster elements.



Infection chain overview.

Indicators of Compromise

IOC Type	IOC Value
File hash (SHA-256)	a05fbe8734a5a5a994a44dee9d21134ad7108d24ab0749499fe24fc4b36c4cbc
File hash (SHA-256)	047307aca3a94a6fc46c4af25580945defb15574fb236d13d2bb48037cc42208
File hash (SHA-256)	ac50887e2c513b50b2170d77441b9f7e8afcc774df6b54fdd8aac863095239f4
File hash (SHA-256)	a23d126f0446755859e4d81c0c9b50b65e0062c3de2a014c543f6b263321ad78
File hash (SHA-256)	ea57b5768c84164fcdb25bb8338d660c5586e17e37cee924c4e5a745510925f3
File hash (SHA-256)	cbef2064cf49b4b27dbf7d0c88c8f7bcdd6a7f25ee9c087beacb48cdd1b78731
File hash (SHA-256)	b77a233735ff237ab964d2bdb3f6d261a90efb2f86dcde458c419cee528686a9
IP	139.84.227[.]139
IP	194.135.25[.]132
IP	23.27.201[.]160
IP	101.36.105[.]222
IP	116.169.244[.]208:2096
IP	192.9.141[.]111
IP	64.176.43[.]209
Domains	telecom.webredirect[.]org
Domains	singtelcom[.]site
Domains	kaztelecom[.]shop
Certificate Indicators	27df475626aafce2ea1548a9f35efb9ad951298c8b11a6adb3ccdfcd5170c677
Certificate Indicators	A72427af3c046fd90999a6505b2372dc4ffde122227f30ed21621ecd4f2d3e8b.
Certificate Indicators	E28a96f983b8605decd2ac1db16ebad5fa741a6aa4e585a38ade0e5ad7d6cec0
Certificate Indicators	2229e7f3cabbce4d67cd79c89fd5a100b20e8a99f4a2bf9aac77a978f49eb520

The GitHub Internal Repositories Supply Chain Breach

Security researchers observed a high-profile breach of Microsoft-owned **GitHub**, where the platform confirmed unauthorized access and exfiltration of roughly **3,800 internal private repositories** containing platform source code, infrastructure configurations, and internal API schemas. Attributed to **TeamPCP** (formally tracked by Google Threat Intelligence as **UNC6780**), a financially motivated threat group specializing in open-source developer tooling and AI middleware, the massive compromise did not exploit a perimeter vulnerability but instead targeted developer identity through an interconnected web of upstream software supply chain infections.

Threat Actor : TeamPCP (UNC6780)
Target Verticals: Code Hosting Platforms, Open-Source Tooling, Developer Identity, and Enterprise CI/CD Ecosystems

Evasion Tactic: It is highly evasive because it weaponizes **trusted extension ecosystems and default auto-update behavior** to inject minified malicious code directly onto endpoints. The threat actor compromised a developer system belonging to Narwhal Technologies via a separate supply-chain attack on the *TanStack* library, scraping a GitHub personal access token. The actor then used this

stolen token to publish a poisoned release of **Nx Console** (version 18.95.0), a highly popular Visual Studio Code extension with over 2.2 million installs. Although the backdoored extension was live on the marketplace for only 18 minutes before being removed, it automatically pushed a minified 2,777-byte script to online developer endpoints—including a GitHub employee workstation. This payload operated entirely in memory, downloading a heavily obfuscated dropper from an orphaned commit on the official nrwl/nx repository to completely blind local EDR agents, silently harvesting developer credentials, cloud identities (AWS, Azure, GCP), and corporate tokens to pivot directly into GitHub's internal source code estate.



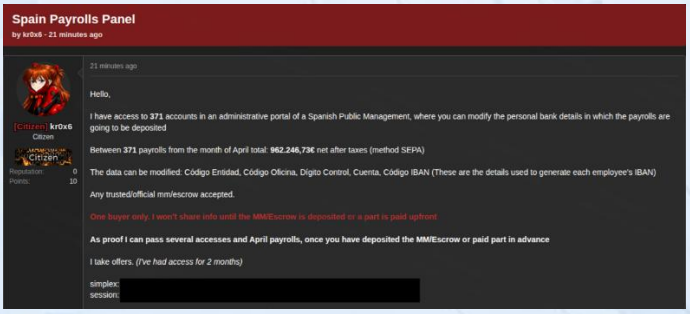
GitHub officially claiming the incident

Indicators of Compromise

IOC Type	IOC Value
File hash(SHA-256)	b0cefb66b953e5184b6adb3035e9e267335ac5eabfe1848e07834777b9397b74
File hash(SHA-256)	e7347d90653efc565f03733a95e9209d78f9cfa81e31ff2b2dd9d48d75a4b8b1
File hash(SHA-256)	b5c97557230a27460fdab01fafcfabeaa49590bafd5b6ef30501aa9e0a51142

Spanish Public-Sector Payroll Portal Access

A threat actor using the alias **kr0x6** claims to hold live access to an administrative portal of an unnamed Spanish public-management entity, **covering 371 accounts where employee bank details for payroll deposits can allegedly be modified.** The seller says the affected April payrolls total roughly **€962,246** and claims to have held access for around two months.



The Gentlemen ransomware, a Ransomware-as-a-Service (RaaS)

The Gentlemen" ransomware, a Ransomware-as-a-Service (RaaS) operation tracked as Storm-2697. The group has developed a Go-based ransomware encryptor designed not only to encrypt files using strong encryption methods, but also to rapidly propagate across compromised environments. The operation follows a double-extortion model, where victim data is exfiltrated prior to encryption and later used as leverage during ransom negotiations.

README-GENTLEMEN.txt - Notepad

File Edit Format View Help

```
<victim ID> = YOUR ID

Gentlemen, your network has been encrypted.

1. Any modification of encrypted files will make recovery impossible.
2. Only our unique decryption key and software can restore your files.
   Brute-force, RAM dumps, third-party recovery tools are useless.
   It's a fundamental mathematical reality. Only we can decrypt your data.
3. Law enforcement, authorities, and "data recovery" companies will NOT help you.
   They will only waste your time, take your money, and block you from recovering your files – your business will be lost.
4. Any attempt to restore systems, or refusal to negotiate, may lead to irreversible wipe of all data and your network.
5. We have exfiltrated all your confidential and business data (including NAS, clouds, etc).
   If you do not contact us, it will be published on our leak site and distributed to major hack forums and social networks.
   In addition, it will be reported to the relevant data protection authorities and regulators.
   This may result in official investigations, significant fines, and reputational damage for your company.
6. We guarantee 100% file recovery to their original state, bit by bit.
   To demonstrate the quality of our work, you can provide two sample files, and we will restore them free of charge.

TOX CONTACT - RECOVER YOUR FILES
Contact us (add via TOX ID): 15CE8D5DB0BAC3BCBB1FA69F2E672CC54EFBEC7684DA792F3CBF8B007A9FEA1D16374560DFA5
Download Tox messenger: https://tox.chat/download.html
Contact us (add via Session ID):
Download Session  https://getsession.org

CONTACT TO PREVENT DATA LEAK (7 DAYS BEFORE YOUR COMPANY DATA WILL BE PUBLISHED IN OUR BLOG, WITH 239 HOURS REVEAL TIMER)
Check our blog: http://tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad.onion/
Download Tor browser: https://www.torproject.org/download/
Follow us on X: https://x.com/TheGentlemen25

Any other means of communication are fake and may be set up by third parties.
Only use the methods listed in this note or on the specified website.
```

Ransom note content



The Gentlemen ransomware's wallpaper on post-encryption

Key Activities Observed

- Utilized a self-propagating ransomware encryptor capable of spreading across networked systems after initial compromise.
- Leveraged multiple lateral movement techniques, including remote administration tools, WMI, scheduled tasks, PowerShell remoting, and service-based execution.
- Employed strong per-file encryption mechanisms, making unauthorized recovery of encrypted

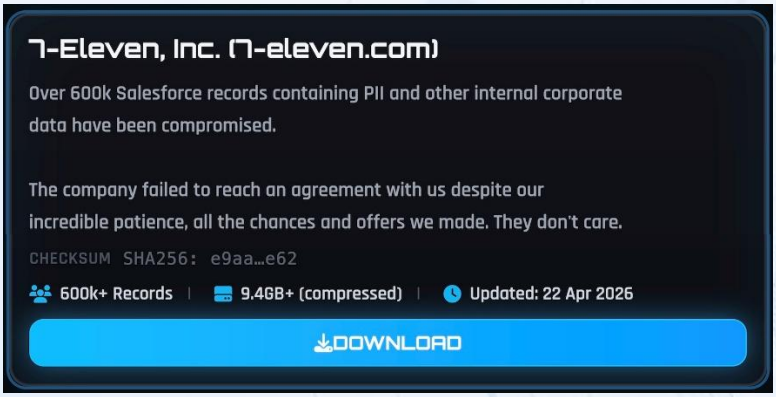
data highly difficult.

- Conducted data exfiltration activities prior to ransomware deployment to support double-extortion operations.
- Attempted to disable or evade endpoint security controls and antivirus protections.
- Deleted shadow copies and recovery artifacts to reduce the possibility of system restoration.
- Cleared Windows event logs and other forensic evidence to hinder incident investigation.
- Targeted Windows-based enterprise environments and network shares to maximize operational impact.
- Used affiliate-driven attack models, enabling multiple threat actors to conduct campaigns under the ransomware service.
- Demonstrated the ability to scale attacks rapidly across an organization once privileged access was obtained.

7-Eleven data breach claimed by ShinyHunters

7-Eleven disclosed a cyber incident involving unauthorized access to systems used for storing franchise-related documents. According to the company's notification, the compromise was identified in April 2026, and an investigation was launched to determine the scope of affected data. The threat actor group ShinyHunters claimed responsibility for the intrusion, alleging that they compromised the organization's Salesforce environment and exfiltrated a large volume of corporate and personal identifiable information (PII). Following unsuccessful ransom negotiations, the threat actors reportedly published a portion of the stolen data on their leak site.

Threat Actor : ShinyHunters



7-Eleven entry on ShinyHunters' leak site

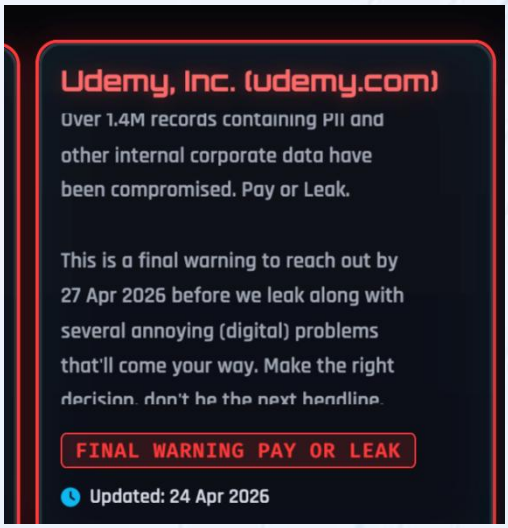
Key Activities Observed:

- Unauthorized access to 7-Eleven systems was reportedly obtained on 8 April 2026.
- Affected systems were associated with the storage of franchisee documentation.
- ShinyHunters claimed responsibility for the breach on 17 April 2026.
- Threat actors alleged the theft of more than **600,000 records containing corporate and personal information.**
- The group stated that the compromise involved a Salesforce environment.
- Following failed extortion negotiations, a **9.4 GB archive** of allegedly stolen data was leaked on a dark web platform.
- 7-Eleven issued breach notifications to affected individuals and initiated an internal investigation.

- The exact number of impacted individuals and the full categories of exposed data have not been publicly disclosed.
- The incident aligns with ongoing ShinyHunters activity targeting organizations through Salesforce-related compromises.

Udemy - Alleged Data Breach Claim by ShinyHunters

On 24 April 2026, the cybercrime and extortion group ShinyHunters claimed to have compromised Udemy, a global e-learning platform. The threat actor alleged that it had obtained more than **1.4 million records containing personally identifiable information (PII) and internal corporate data**. The claim was **published on the group's dark web leak site**, accompanied by an extortion demand and a deadline for Udemy to establish contact before the data is allegedly released. As of the reporting period, Udemy has not publicly confirmed the breach, and the claims remain unverified



Udemy entry on ShinyHunters' leak site

- ShinyHunters listed Udemy on its dark web leak portal as an alleged victim.
- The group claimed to have exfiltrated over 1.4 million records.
- The allegedly compromised data includes personally identifiable information (PII) and internal corporate information.
- The threat actor issued a public extortion demand, threatening to leak the data if communication was not established by 27 April 2026.
- The group also warned of potential additional disruptive digital activities if its demands were not met.
- No official confirmation of the breach had been released by Udemy at the time of reporting.



The gang also dumped Mytheresa, Zara, Carnival, and 7-Eleven data in a fresh leak wave

ShinyHunters is linked to major cybercrime campaigns, such as last year's Salesforce CRM data heist that targeted enterprise cloud services and customer databases.

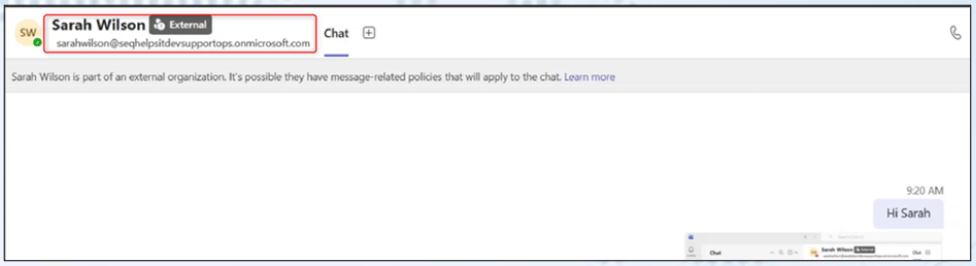
Cyber Incidents Amid Iran–Israel Context

Dindoor (DinDoor) & Fakeset Backdoor Frameworks

Observed a targeted cyber-espionage surge by the Iran-nexus advanced persistent threat (**APT**) group **Seedworm** (a specialized operational sub-cluster of **MuddyWater**, also tracked as Mango Sandstorm or Static Kitten). Acting as a key intelligence-gathering arm for Iran's Ministry of Intelligence and Security (MOIS), the group has executed highly focused corporate espionage campaigns designed to establish long-term persistence across banking, aviation, defense, and software supply chain infrastructures. The campaign is driven by a brand-new custom malware toolkit consisting of two distinct backdoors running in the wild: Dindoor, a specialized remote access trojan, and Fakeset, a python-based backdoor.

Threat Actor : Seedworm (MuddyWater / MOIS Sub-Cluster)
Target Verticals : Aviation/Airports, Financial Services, Defense & Aerospace, and Technology Operations (US / Middle East / Israel)

Evasion Tactic: It is highly evasive because it shifts from noisy, host-based data manipulation to abusing specialized runtimes and signed dual-use utilities to bypass standard Endpoint Detection and Response (EDR) blind spots. The Dindoor variant utilizes the Deno JavaScript/TypeScript runtime environment, running highly obfuscated, Base64-encoded scripts directly in memory to completely hide its execution logic from traditional file-based signature scanners. Concurrently, the Fakeset backdoor is dropped via malicious installer packages hosted on legitimate commercial Backblaze storage buckets, leveraging stolen and valid individual code-signing certificates to masquerade as trusted applications.



Attacker reaching the user through Microsoft Teams

Through this interaction, the user was convinced to execute a malicious installer named update_ms.msi, masquerading as a Windows update package. This MSI served as the initial dropper for a custom backdoor referred to as Dindoor.

Cloud Evasion & Data Exfiltration: To defeat automated Data Loss Prevention (DLP) and network visibility filters, the threat actor completely bypasses custom host-based exfiltration scripts. Instead, they leverage Rclone a legitimate, command-line cloud management utility—to compress, sync, and pump stolen corporate file arrays, databases, and configuration directories directly into secure, commercial Wasabi S3 and Backblaze buckets. Because this data movement blends completely with routine enterprise administrative cloud syncs, it renders perimeter anomaly detection blind.

Indicators of Compromise

Malware:

FAMILY	SHA-256 HASH
Dindoor	0f9cf1cf8d641562053ce533aaa413754db88e60404cab6bbaa11f2b2491d542
Dindoor	1d984d4b2b508b56a77c9a567fb7a50c858e672d56e8cf7677a1fca5c98c95d1
Dindoor	2a00705cfd3c15cf8913e9eb4e23968efd06f1feceaef9987d26c5518887d043
Dindoor	2a09bbb3d1ddb729ea7591f197b5955453aa3769c6fb98a5ef60c6e4b7df23a5
Dindoor	42a5db2a020155b2adb77c00cbe6c6ad27c2285d8c6114679d9d34137e870b3f
Dindoor	7467f326677a4a2c8576e71a832e297e794ea00e9b67c4fcbe78b5aec697cec4
Dindoor	7c30c16e7a311dc0cdb1cdfd9ea6e502f44c027328dbe7d960b9bcd85ccf5eef
Dindoor	b0af82de672d81f3c2f153977923b3884a8a9e7045b182c2379b19a1996931a0
Dindoor	bd8203ab88983bc081545ff325f39e9c5cd5eb6a99d04ae2a6cf862535c9829a
Dindoor	c7cf1575336e78946f4fe4b0e7416b6ebe6813a1a040c54fb6ad82e72673478e
Fakeset	077ab28d66abdafad9f5411e18d26e87fe43da1410ee8fe846bd721ab0cb52de
Fakeset	15061036c702ad92b56b35e42cf5dc334597e7311e98d2fdd3815a69ac3b1d84
Fakeset	2b7d8a519f44d3105e9fde2770c75efb933994c658855dca7d48c8b4897f81e6
Fakeset	4aef998e3b3f6ca21c78ed71732c9d2bdcc8a4e0284f51d7462c79d446fbc7be
Fakeset	64263640a6fdeb2388bca2e9094a17065308cf8dcb0032454c0a71d9b78327eb
Fakeset	64cf334716f15da1db7981fad6c81a640d94aa1d65391ef879f4b7b6edf6e7f1

Fakeset	74db1f653da6de134bdc526412a517a30b6856de9c3e5d0c742cb5fe9959ad0d
Fakeset	94f05495eb1b2ebe592481e01d3900615040aa02bd1807b705a50e45d7c53444
Fakeset	a4bd1371fe644d7e6898045cc8e7b5e1562bdfd0e4871d46034e29a22dec6377
Fakeset	a5d4d6be3bfe0cba23fe6b44984b5fc9c7c7e10030be96120bb30da0f2545d4c
Fakeset	ddceade244c636435f2444cd4c4d3dc161981f3af1f622c03442747ecef50888
Stagecomp	24857fe82f454719cd18bcbe19b0cfa5387bee1022008b7f5f3a8be9f05e4d14
Stagecomp	a92d28f1d32e3a9ab7c3691f8bfca8f7586bb0666adbba47eab3e1a8faf7ecc0
Darkcomp	3df9dcc45d2a3b1f639e40d47eceeafb229f6d9e7f0adcd8f1731af1563ffb90
Darkcomp	1319d474d19eb386841732c728acf0c5fe64aa135101c6ceee1bd0369ecf97b6

Network Indicators:

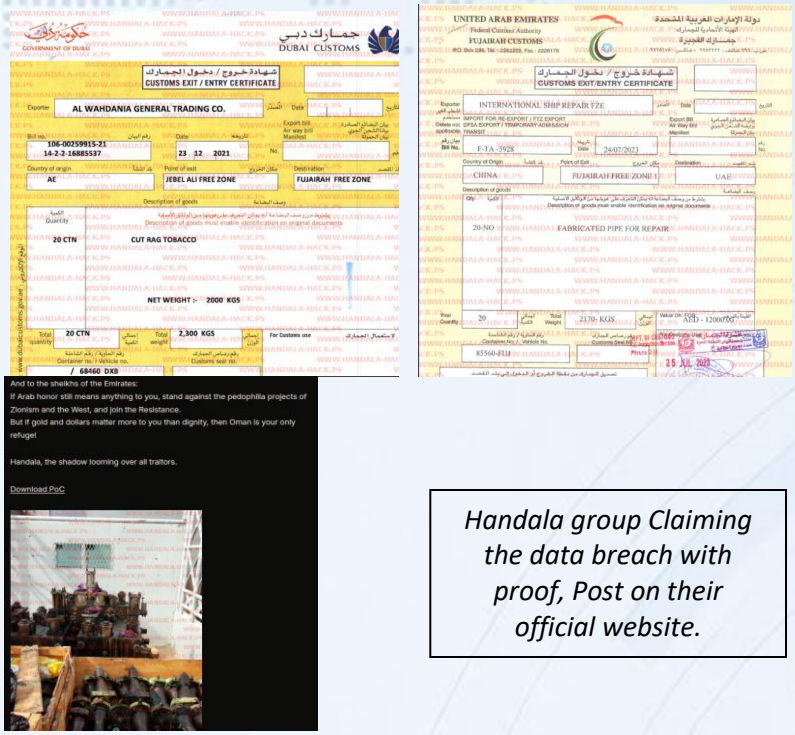
TYPE	INDICATOR
S3 Bucket	gitempire.s3.us-east-005.backblazeb2[.]com
S3 Bucket	elvenforest.s3.us-east-005.backblazeb2[.]com
Domain	uppdatefile[.]com
Domain	serialmenot[.]com
Domain	moonzonet[.]com

Handala and IRGC Target Fujairah

Handala Hack Team claimed responsibility for a cyberattack targeting the Port of Fujairah in the UAE. The group alleged that it compromised the port's infrastructure and exfiltrated more than 430,000 confidential documents, including shipping data, financial records, operational contracts, and maps related to oil pipeline infrastructure.

Key Activities Observed:

- Claimed unauthorized access to systems associated with the Port of Fujairah.
- Alleged theft of over 430,000 confidential documents from port infrastructure.
- Claimed exposure of sensitive operational data, including:
  Ship movement and traffic information
  Financial transaction records
  Contractual documentation
  Oil pipeline and critical infrastructure maps
- Claimed coordination between cyber operations and missile strike activities targeting the port.
- Issued public threats warning of continued cyber and intelligence operations against UAE entities.
- Used the incident for propaganda and psychological messaging targeting regional political relationships.



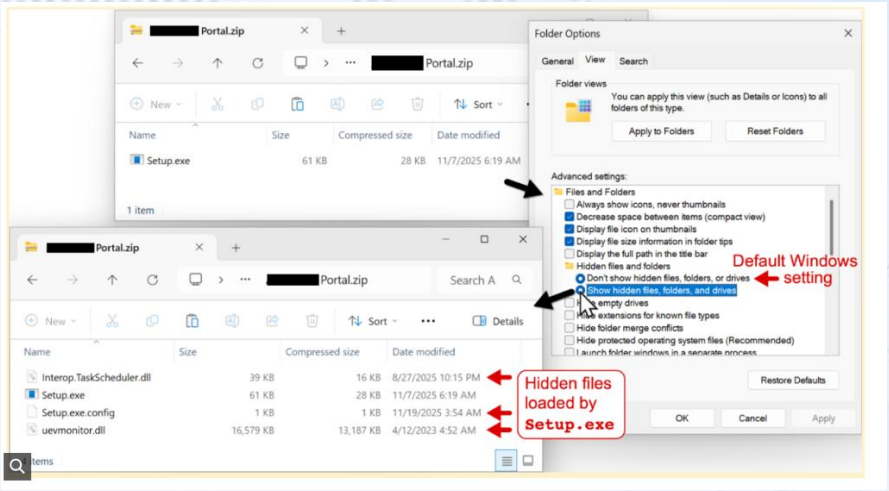
Handala group Claiming the data breach with proof, Post on their official website.

Operation Persistent Serpens

Security researchers observed a surge in a new cyber-espionage campaign deploying the **MiniUpdate and MiniJunk V2 RAT families** by the Iran-nexus advanced persistent threat (APT) group **Screening Serpens** (**UNC1549**, **Smoke Sandstorm**, or **Nimbus Manticore**). This variant aggressively targets high-value aerospace, defense manufacturing, and telecommunications sectors across the United States, Israel, and the United Arab Emirates through highly tailored social engineering. Both malware families build directly upon the actor's established playbook, utilizing targeted spear-phishing lures and fake software updates that leverage DLL sideloading for execution. To maximize operational resiliency and prevent cross-contamination, the threat actor routes command and control (C2) traffic through a dedicated set of three to five unique subdomains hosted on legitimate Azure infrastructure for each specific target and variant.

Threat Actor: Screening Serpens
Target Verticals: Aerospace, Defense, Telecom, Technology Providers (Middle East / US)

Evasion Tactic: It is highly evasive because it operates via **AppDomainManager Hijacking** during its infection chain; instead of relying on traditional executable files that flag security software, it utilizes legitimate configuration files to manipulate the initialization phase of trusted .NET applications. This technique instructs the system runtime to proactively disable the application's own security mechanisms—such as Event Tracing for Windows (ETW) and strong-name signature validation—allowing the embedded remote access trojans (RATs) to execute silently in memory and significantly minimize the local Endpoint Detection and Response (EDR) footprint.



Contents of the Portal.zip archive containing hidden files, with uevmonitor.dll used as the payload for the attack (MiniJunk V2).



The ZIP contains a nested payload archive (Hiring Portal.zip) packaged alongside six PDF documents (MiniUpdate).

Indicators of Compromise

Domains:

- licencemanagers.azurewebsites[.]net
- LicenceSupporting.azurewebsites[.]net
- PeerDistSvcManagers.azurewebsites[.]net
- ThemesManagers.azurewebsites[.]net
- ThemesProviderManagers.azurewebsites[.]net
- docspace-y4cumb.onlyoffice[.]com
- NanoMatrix.azurewebsites[.]net
- QuantumWeave.azurewebsites[.]net
- ElementShift.azurewebsites[.]net
- business-startup[.]org
- business-startup.azurewebsites[.]net
- Businessstartup.azurewebsites[.]net
- app[redacted][.]live
- buisness-centeral.azurewebsites[.]net
- buisness-centeral-transportation.azurewebsites[.]net
- Buisness-centeral-transportation[.]com
- docspace-twpf0e.onlyoffice[.]com
- PremierHealthAdvisory[.]com
- PremierHealthAdvisory.azurewebsites[.]net
- Premier-HealthAdvisory.azurewebsites[.]net
- Ramiltonsfinance[.]com

- Ramiltonsfinance.azurewebsites[.]neti
- Ramiltons-finance.azurewebsites[.]net

URLs:

- hxxps[:]//docspace-y4cumb.onlyoffice[.]com/storage/files/root/folder_3602000/file_3601577/v1/content.zip
- hxxps[:]//app[redacted][.]live/meeting/edcdba624ddb43c2a1dcf334aa493068
- hxxps[:]//docspace-twpf0e.onlyoffice[.]com/storage/files/root/folder_3765000/file_3764519/v1/content.zip?filename=remote.[REDACTED].zip
- hxxps[:]//2117.filemail[.]com/api/file/get?filekey=T0EnWQ6NugHkW_kLfDxPBEw_um6NSkg9ZwNRQ_5lrKrLLUo35pV8m3TKv1LqF3zZzdUm

SHA256 Hashes:

MiniUpdate: US Campaign

- 44f4f7aca7f1d9bfdaf7b3736934cbe19f851a707662f8f0b0c49b383e054250 - Initial archive file
- 332ba2f0297dfb1599adecc3e9067893e7cf243aa23aedce4906a4c480574c17 - Hiring Portal.zip
- 0db36a04d304ad96f9e6f97b531934594cd95a5cea9ff2c9af249201089dc864 - UpdateChecker.dll

MiniUpdate: Israel Campaign

- 38bd137c672bd58d08c4f0502f993a6561e2c3411773d1ae57ee0151a0a9d11d - Initial archive file
- d4a7e9f107fe40c1a5d0139c6c6e25bf6bf57f61feff090bee28f476bb3cc3c2 - UpdateChecker.dll

MiniUpdate: UAE Campaign

- bc3b44154518c5794ce639108e7b9c5fecb0c189607a26de1aaed518d890c7ad - UpdateChecker.dll

MiniUpdate: Middle Eastern Campaign

- 74882085db2088356ed7f72f01e0404a0a98cda88ef56fb15ce74c1f36b26d27
- bc3b44154518c5794ce639108e7b9c5fecb0c189607a26de1aaed518d890c7ad - UpdateChecker.dll

MiniJunk V2: Middle Eastern Campaign

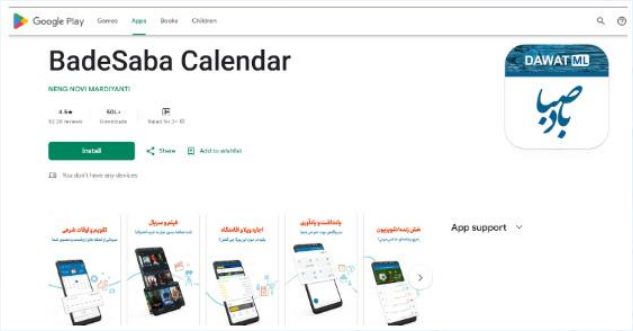
- 9cf029daca89523d917dafed0568d11d00e45ec96b5b90b4a1f7fd4018c7da84 - uevmonitor.dll
- B19e06da580cf91691eda066ac9ee4b09c6e5dc26c367af12660fe1f9306eec4 - unbcl.dll

MiniJunk V2: U.S. Campaign

- 8808c794c24367438f183e4be941876f1d3ecd0c8d2eb43b10d2380841d2283b - Portable Platform.zip
- 43dc62cef52ebdd69e79f10015b3e13890f26c058325c0ff139c70f8d8eadcfa - Connection.dll
- 9e4a658e6d831c9e9bdfe11884a75b7c64812ed0a80e8495ddf6b316505acac1 - unbcl.dll

BadeSaba Calendar application compromise

An information operation was reportedly conducted through the **BadeSaba** Calendar application, one of **Iran's most widely used prayer and calendar apps**. According to multiple media reports, the application's push notification service was allegedly compromised and used to deliver messages encouraging Iranian security personnel to distance themselves from the government. The activity occurred shortly after military strikes targeting Iranian leadership and strategic assets, indicating a possible effort to influence public perception and security force morale through a trusted digital platform.



BadeSaba App in Google Play Store

- Alleged unauthorized access to the **BadeSaba application's push notification infrastructure.**
- Distribution of politically themed messages to millions of users through the application's notification channel.
- Messages reportedly encouraged security forces to abandon support for the regime and emphasized support for those who chose to protect the nation.
- The operation leveraged a highly trusted religious application with a large user base and regular daily engagement.
- Multiple media outlets attributed the activity to Israel or an Israel-aligned entity, although no public technical evidence or official attribution has been released.
- Users shared screenshots of the notifications across social media and messaging platforms, increasing the visibility of the operation.



Notifications from the app

Iranian authorities reportedly responded by restricting or throttling internet connectivity in affected regions and framing the incident as a foreign psychological warfare campaign. The incident demonstrates the use of legitimate digital platforms as channels for influence operations during periods of geopolitical tension. The reported compromise highlights how trusted consumer applications can be leveraged to deliver influence and psychological operations at scale, extending the impact of geopolitical conflicts into the digital domain.

Vulnerability & Exploit Intelligence

Enterprise Edge Infrastructure & Networking

CVE-2026-20182 | Cisco Catalyst SD-WAN Controller

- **Severity & Metrics:** 10.0 (Critical) | Added to CISA's Known Exploited Vulnerabilities (KEV) Catalog on May 14, 2026.
- **The Vulnerability:** A flaw in the "vdaemon" DTLS peering authentication mechanism allows remote, unauthenticated attackers to connect using any self-signed client certificate by claiming to be a "vHub" device type.
- **Operational Impact:** By bypassing checking logic entirely, adversaries become authenticated peers on the target appliance. This lets them inject public keys into the administrative account's authorized SSH keys file, execute arbitrary NETCONF commands, and completely manipulate network routing configuration across the entire SD-WAN fabric.
- **Regional Threat Context:** Actively exploited in the wild by threat cluster UAT-8616. It poses an extreme risk to Middle Eastern telecommunications architectures and distributed enterprise WAN networks.

CVE-2024-5910 | Palo Alto Networks Expedition

- **Severity & Metrics:** 9.3 (Critical) | Actively targeted exploitation vector.
- **The Vulnerability:** A critical missing authentication vulnerability within the migration tool component.
- **Operational Impact:** Allows external network actors to gain unauthorized administrative access to the platform configuration utilities without prompting for valid credentials.
- **Regional Threat Context:** Leveraged heavily by regional APT groups to silently extract firewall configurations, decrypt sensitive connection keys, and build maps of internal protected zones for downstream lateral movement.

Directory Services & Identity Platforms

CVE-2026-41089 | Windows Netlogon Directory Core

- **Severity & Metrics:** 9.8 (Critical) | Disclosed via Microsoft Patch Tuesday on May 12, 2026.
- **The Vulnerability:** A classic stack-based buffer overflow flaw embedded within the Windows Netlogon parsing engine.
- **Operational Impact:** External, unauthorized attackers can transmit crafted network traffic to execute arbitrary code with highest privileges over an open network share without needing valid initial access credentials.
- **Regional Threat Context:** Weaponized by opportunistic operators immediately following disclosure to target central Domain Controllers, looking to transition an initial perimeter

beachhead into an immediate domain-wide compromise.

Core Operating System Components

CVE-2026-41096 | Windows DNS Client Resolver

- **Severity & Metrics:** 9.8 (Critical) | Released in the May 2026 cumulative patch bundle.
- **The Vulnerability:** A severe heap-based buffer overflow bug hidden inside the DNS response parsing logic of dnsapi.dll.
- **Operational Impact:** Triggers when an application forces the workstation to look up a domain and receives a malicious, oversized DNS response packet. This allows an attacker to execute arbitrary code silently under the NETWORK SERVICE context without any user interaction.
- **Regional Threat Context:** Highly dangerous for remote workstations connected to rogue public Wi-Fi networks, or networks prone to local ARP spoofing and DNS resolver hijacking.

CVE-2026-43284 | Linux Kernel ("Dirty Frag")

- **Severity & Metrics:** 8.8 (High) | Disclosed publicly on May 7, 2026.
- **The Vulnerability:** A kernel bug within the IPsec Encapsulating Security Payload (ESP) handling logic (esp4 / esp6), where the system performs in-place decryption directly over un-copied, externally backed page fragments.
- **Operational Impact:** Local unprivileged attackers can run specialized tools to corrupt sensitive page-cache memory zones (such as /etc/passwd), immediately yielding absolute root privileges on the target node.
- **Regional Threat Context:** Actively exploited to compromise Linux-based data servers, cloud instances, and edge enterprise Network-Attached Storage (NAS) platforms running unpatched kernels.

SaaS & Shared Hosting Web Assets

CVE-2026-48172 | LiteSpeed Web Server cPanel Plugin

- **Severity & Metrics:** 10.0 (Critical) | Active wide-scale scanner target.
- **The Vulnerability:** A flaw located inside the lsws.redisAble function of the management extension.
- **Operational Impact:** Allows any low-privilege, authenticated cPanel tenant on a shared hosting box to elevate permissions and execute arbitrary scripts with full root shell capabilities.
- **Regional Threat Context:** Leveraged heavily in automated internet scanning sweeps by hacktivist syndicates to hijack corporate public-facing web servers and execute widespread portal defacements.

Adversary-in-the-Middle (AiTM) | Cloud Identity Environments

- **Severity & Metrics:** High Priority | Tactic-based threat variant.
- **The Vulnerability:** Architectural manipulation of standard web-session cookies and security assertion markup language (SAML) tokens.
- **Operational Impact:** Uses proxy-phishing engines to intercept valid authentication tokens, enabling threat actors to copy an active session state directly to their own machine.
- **Regional Threat Context:** Bypasses traditional Multi-Factor Authentication (MFA) parameters, allowing malicious entities to log straight into Microsoft 365 or Entra ID cloud infrastructure, compromise corporate directories, and run automated corporate BEC actions.

MITRE ATT&CK / TTP Mapping

TACTIC	TECHNIQUES (MITRE ATT&CK)		OBSERVED IN (Threat Actors / Campaigns)
INITIAL ACCESS	T1566.001	Spearphishing Attachment	• WantToCry • GitHub Supply Chain Breach • Dindoor/Fakeset • MiniUpdate/MiniJunk V2
	T1566.002	Spearphishing Link	
	T1195	Supply Chain Compromise	
	T1190	Exploit Public-Facing Application	
	T1133	External Remote Services	
	T1110	Brute Force	
EXECUTION	T1059.001	PowerShell	• Dindoor • Fakeset • Persistent Serpens • GitHub Supply Chain Attack
	T1059.007	JavaScript	
	T1059.006	Python	
	T1204	User Execution	
	T1218	Signed Binary Proxy Execution	
	T1574.014	DLL Search Order Hijacking	
PERSISTENCE	T1547	Boot or Logon Autostart Execution	• MiniJunk V2 • Showboat • The Gentlemen RaaS
	T1136	Create Account	
	T1546.014	AppDomainManager Hijacking	
	T1053	Scheduled Tasks	
DEFENSE EVASION	T1027	Obfuscated Files or Information	• Dindoor • Fakeset • Showboat • GitHub Supply Chain Breach • The Gentlemen RaaS
	T1218	Signed Binary Proxy Execution	
	T1562.001	Disable Security Tools	
	T1070.001	Clear Windows Event Logs	
	T1036	Masquerading	
CREDENTIAL ACCESS	T1552	Unsecured Credentials	• GitHub Supply Chain Breach • WantToCry • ShinyHunters Operations
	T1555	Credentials from Password Stores	
	T1528	Steal Application Access Token	
	T1110	Password Brute Force	
DISCOVERY	T1087	Account Discovery	• Showboat • Dindoor • MiniUpdate
	T1018	Remote System Discovery	
	T1046	Network Service Scanning	
	T1082	System Information Discovery	
LATERAL MOVEMENT	T1021.002	SMB/Windows Admin Shares	• WantToCry • The Gentlemen RaaS • Showboat
	T1021.006	WinRM	
	T1570	Lateral Tool Transfer	
	T1563	Remote Service Session Hijacking	
COMMAND & CONTROL	T1071.001	Web Protocols	• Showboat • Dindoor • Persistent Serpens • GitHub Supply Chain Breach
	T1090	Proxy	
	T1105	Ingress Tool Transfer	
	T1573	Encrypted Channel	
EXFILTRATION	T1567.002	Exfiltration to Cloud Storage	• Dindoor/Fakeset • ShinyHunters • GitHub Supply Chain Breach • The Gentlemen RaaS
	T1041	Exfiltration Over C2 Channel	
	T1020	Automated Exfiltration	
IMPACT	T1486	Data Encrypted for Impact	• WantToCry • The Gentlemen RaaS
	T1490	Inhibit System Recovery	
	T1489	Service Stop	
	T1531	Account Access Removal	

LEGEND – MITRE ATT&CK TACTICS

Initial Access | Execution | Persistence | Defense Evasion | Credential Access | Discovery | Lateral Movement | Command & Control | Exfiltration | Impact

This matrix maps MITRE ATT&CK techniques to observed usage across multiple threat actors and campaigns.

Source: MITRE ATT&CK® (v15.1)

Recommendations

Cloud & Identity Security

- Enforce phishing-resistant MFA across critical systems.
- Monitor and rotate privileged credentials periodically.
- Restrict personal access token (PAT) usage within development environments.
- Perform vulnerability assessments and validation scans to identify exposed services and misconfigurations.
- Review cloud storage activity for unusual uploads, synchronization activity, or bulk data transfers.

Ransomware Readiness

- Maintain backups.
- Test recovery procedures periodically.
- Segment critical assets from user networks.

Email & Social Engineering Protection

- Strengthen email security controls to identify and block phishing, spear-phishing, and malicious attachments.
- Conduct user awareness exercises focused on:
  - Fake software updates.
  - Microsoft Teams impersonation attacks.
  - Credential harvesting campaigns.
  - Business Email Compromise (BEC) attempts.

Vulnerability Management

- Prioritize remediation of latest vulnerabilities.
- Verify that internet-facing assets are fully patched and periodically validated.

Appendix

Threat Actors Observed

Threat Actor	Motivation	Primary Activity
ShinyHunters	Financial	Data Theft & Extortion
TeamPCP (UNC6780)	Financial	Supply Chain Compromise
Calypso (Red Lamassu)	Espionage	Telecom Espionage
Seedworm (MuddyWater)	State-Sponsored Espionage	Corporate Intelligence Collection
Screening Serpens	State-Sponsored Espionage	Aerospace & Defense Targeting
Handala	Hacktivism / Geopolitical	Critical Infrastructure Targeting
Storm-2697 (The Gentlemen)	Financial	Ransomware Operations

Malware Families Observed

Malware	Category
Showboat / EvaRAT	Linux Backdoor
Dindoor	Remote Access Trojan
Fakeset	Python Backdoor
MiniUpdate	RAT Loader
MiniJunk V2	RAT
WantToCry	Ransomware
The Gentlemen	Ransomware
GoGra	Infostealer
Remcos	RAT
Vidar	Information Stealer
PsExec	Administrative Tool Abuse

Acronyms

Acronym	Meaning
APT	Advanced Persistent Threat
IOC	Indicator of Compromise
TTP	Tactics, Techniques and Procedures
RAT	Remote Access Trojan
RaaS	Ransomware-as-a-Service
C2	Command & Control
EDR	Endpoint Detection and Response
SIEM	Security Information and Event Management
DLP	Data Loss Prevention
CSPM	Cloud Security Posture Management

SMB	Server Message Block
ISP	Internet Service Provider
MOIS	Ministry of Intelligence and Security(Iran)
PAT	Personal Access Token
SAML	Security Assertion Markup Language
ETW	Event Tracing for Windows
DLL	Dynamic Link Library
WMI	Windows Management Instrumentation
NETCONF	Network Configuration Protocol
SSH	Secure Shell
DTLS	Datagram Transport Layer Security
VPN	Virtual Private Network
CI/CD	Continuous Integration / Continuous Deployment
PII	Personally Identifiable Information
KEV	Known Exploited Vulnerabilities
NAS	Network Attached Storage
BEC	Business Email Compromise
TLS	Transport Layer Security