Date of Publication
April 28, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

20 to 26 APRIL 2026

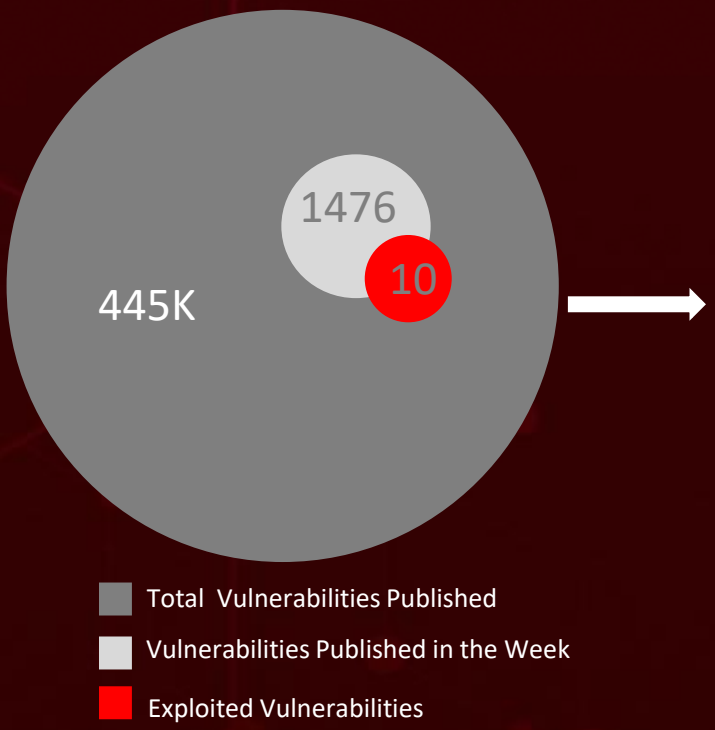
Table Of Contents

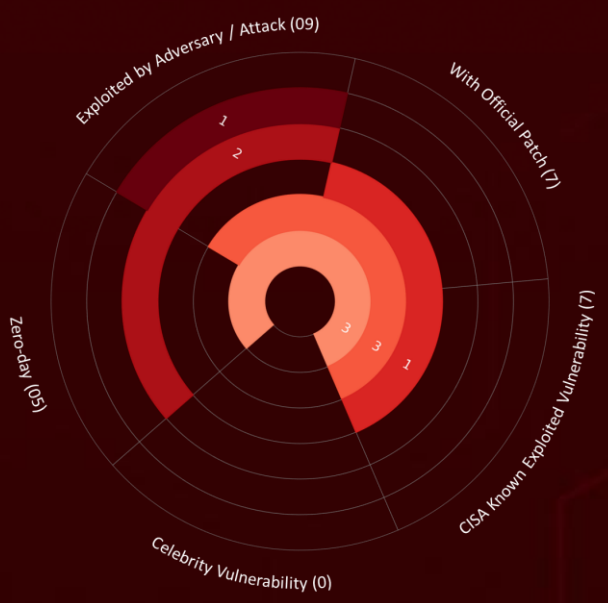
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **seventeen** major attacks were detected, **ten** vulnerabilities were exploited, and **six** active threat actor groups were monitored, signaling a concerning escalation in malicious activity.

Among the most pressing issues, a long-overlooked flaw in Apache ActiveMQ (**CVE-2026-34197**) reveals how a seemingly harmless security adjustment can introduce serious risk. Changes made to maintain Jolokia functionality unintentionally exposed sensitive management operations, allowing attackers to abuse them remotely. By chaining this weakness with ActiveMQ's VM transport and Spring XML handling, threat actors can load malicious configurations and execute arbitrary commands, effectively gaining control over the system. At the same time, groups like **Scattered LAPSUS$ Hunters (SLH)** are scaling cloud-focused data theft and extortion by exploiting trusted SaaS integrations, moving laterally across platforms, and pressuring victims through data leaks, DDoS attacks, and targeted harassment, often blurring attribution as impersonators mimic well-known cybercrime brands.

Meanwhile, evolving intrusion campaigns continue to rely on stealth and social engineering to stay effective. The latest **LOTUSLITE** wave uses banking-themed lures and CHM files to trigger multi-stage infections that abuse legitimate Windows components for covert execution. Similarly, **UNC6692** combines email bombing with Microsoft Teams impersonation to deploy a modular malware toolkit, enabling credential theft, lateral movement, and large-scale data exfiltration. In parallel, **Tropic Trooper** is targeting users across Asia with weaponized documents and trojanized software, leveraging loaders, GitHub-based command-and-control channels, and even VS Code tunnels for persistent remote access. Together, these incidents highlight how modern attackers blend technical exploitation with deception, reinforcing the need for rapid patching, continuous monitoring, and layered defenses to stay ahead.





High Level Statistics

17
Attacks Executed

10
Vulnerabilities Exploited

6
Adversaries in Action

- LummaC2
- StealC
- Vidar
- RedLine
- Meduza
- Rhadamanthys
- Nexcorium
- Lotus Wiper
- LOTUSLITE
- SNOWBELT
- SNOWGLAZE
- SNOWBASIN
- EntryShell
- AdaptixC2 Beacon agent
- TOSHIS loader
- The Gentlemen
- SystemBC

- CVE-2026-34197
- CVE-2025-31324
- CVE-2025-61882
- CVE-2021-35587
- CVE-2024-3721
- CVE-2017-17215
- CVE-2024-55591
- CVE-2023-27532
- CVE-2024-37085
- CVE-2025-7771

- Scattered Spider
- ShinyHunters
- LAPSUS$
- Mustang Panda
- UNC6692
- Tropic Trooper

Insights

Nexcorium weaponizes **CVE-2024-3721** to turn vulnerable DVRs into a self-propagating IoT botnet, spreading via default creds and unleashing large-scale DDoS on command.

A fix meant to secure Apache ActiveMQ quietly backfired, **CVE-2026-34197** turned tighter Jolokia controls into a doorway for remote abuse.

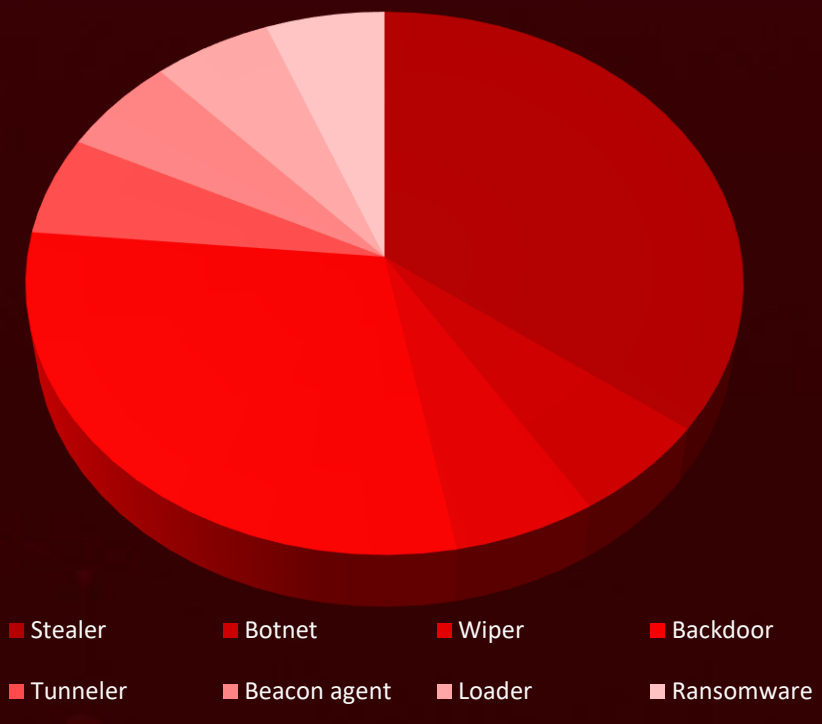
UNC6692 turns trust into a weapon, pairing email bombing with fake IT helpdesk lures to deploy a stealthy SNOW-malware stack and drive deep, cloud-backed compromise.

The Gentlemen RaaS surges ahead, blending multi-OS encryption with stealthy tunneling and domain-wide deployment to execute fast, synchronized double-extortion at scale.

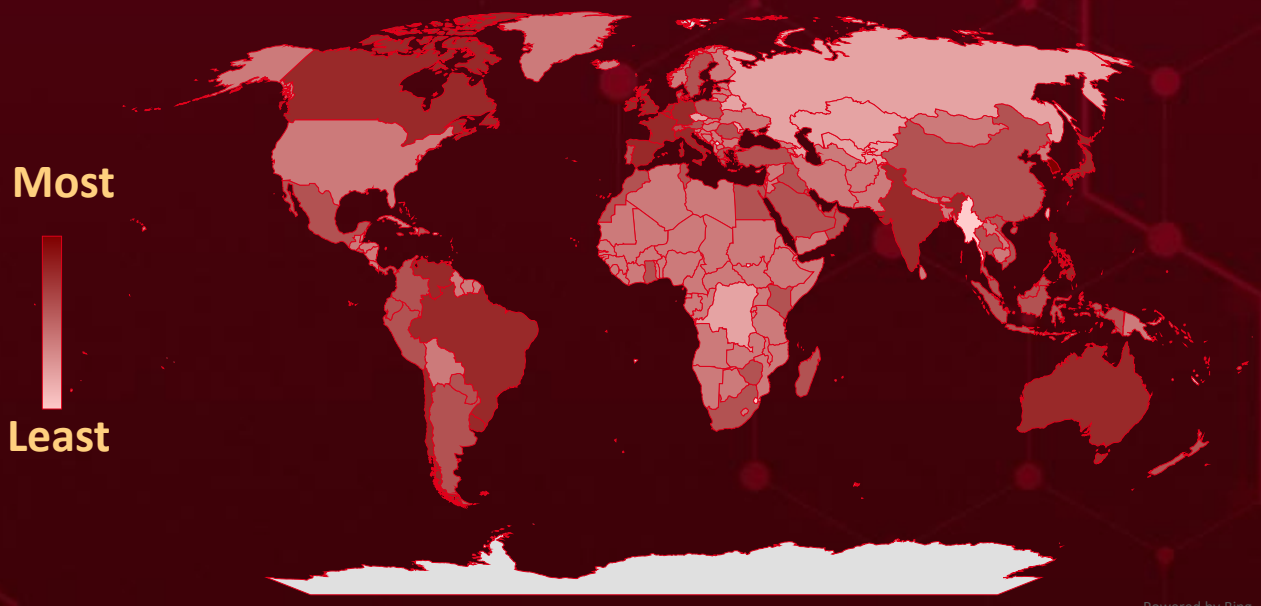
Scattered LAPSUS$ Hunters blurs the lines between legacy notoriety and modern extortion, mixing real threat actors with impostors to weaponize reputation and obscure attribution.

Tropic Trooper blends lures with living-off-the-platform tradecraft, hiding C2 in GitHub and abusing VS Code tunnels to turn trusted tools into covert access channels.

Threat Distribution



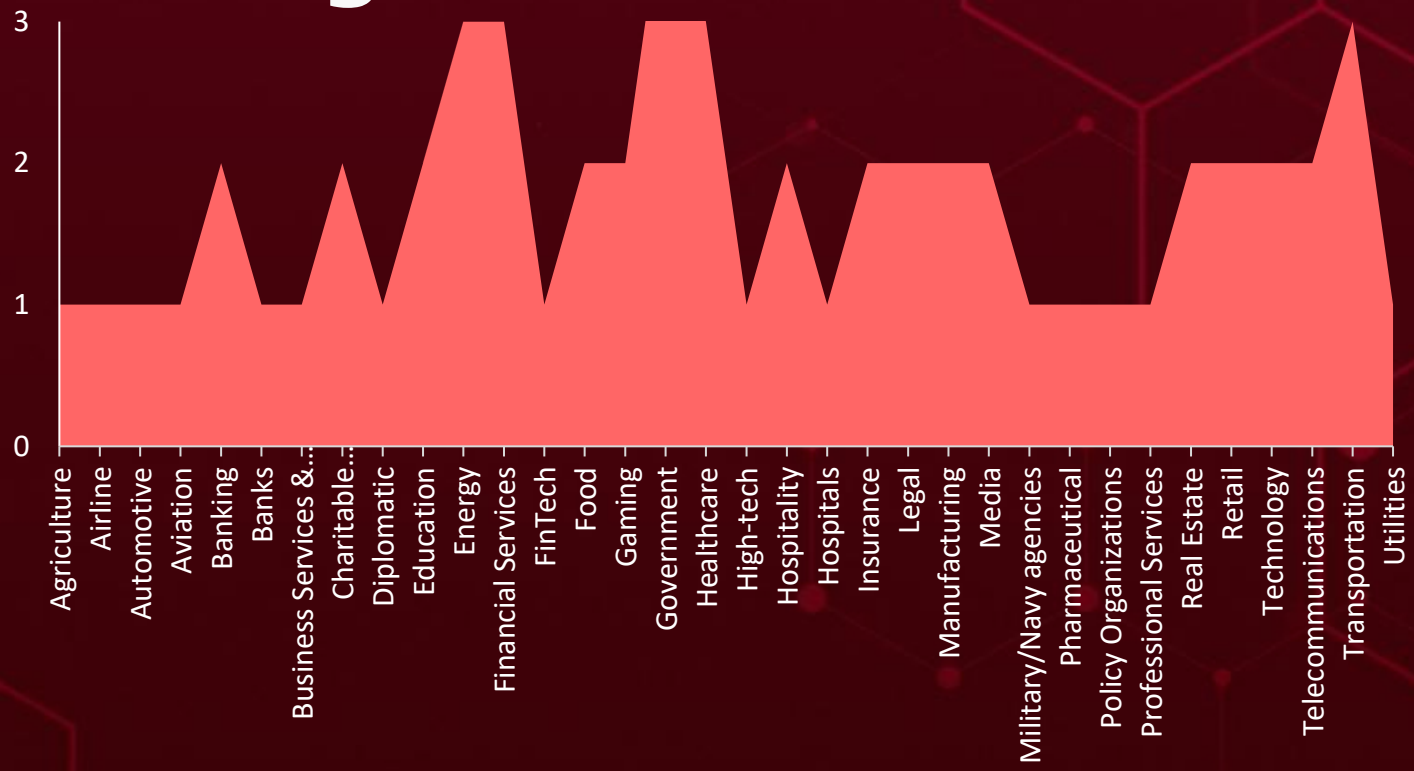
Targeted Countries



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Countries	Countries	Countries	Countries
South Korea	Thailand	Mauritius	Haiti
Spain	Iraq	Switzerland	Dominica
Uruguay	Panama	Mexico	Holy See
Italy	Colombia	Tunisia	Samoa
Belgium	Poland	Morocco	Honduras
Philippines	Israel	United Arab Emirates	Slovakia
Brazil	Fiji	Egypt	Hungary
Ireland	Denmark	Greece	Sri Lanka
Canada	Sweden	New Zealand	Iceland
Japan	Jamaica	Kuwait	Timor-Leste
Chile	Turkey	Lebanon	Botswana
Netherlands	Dominican Republic	Zimbabwe	Uganda
France	Oman	Cyprus	Antigua and Barbuda
Australia	Kenya	Finland	Bosnia and Herzegovina
Singapore	Paraguay	Serbia	Iran
Germany	Ecuador	Grenada	Pakistan
United Kingdom	El Salvador	United States	Brunei
India	Vietnam	Guatemala	Bahamas
Venezuela	Portugal	Republic of Congo	Bulgaria
Argentina	Luxembourg	Guinea	Bangladesh
Peru	Saudi Arabia	Eritrea	Burkina Faso
Ghana	Madagascar	Guinea-Bissau	Rwanda
China	South Africa	French Guiana	Burundi
Romania	Malaysia	Guyana	Angola
Indonesia	Austria	Norway	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1053** Scheduled Task/Job	**T1036** Masquerading
T1204 User Execution	**T1041** Exfiltration Over C2 Channel	**T1078** Valid Accounts	**T1036.005** Match Legitimate Resource Name or Location	**T1547** Boot or Logon Autostart Execution
T1105 Ingress Tool Transfer	**T1059.003** Windows Command Shell	**T1053.005** Scheduled Task	**T1027** Obfuscated Files or Information	**T1566** Phishing
T1082 System Information Discovery	**T1567** Exfiltration Over Web Service	**T1543** Create or Modify System Process	**T1489** Service Stop	**T1090** Proxy

Attacks Executed

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">LummaC2</td><td rowspan="6">LummaC2 is a rapidly evolving information-stealer sold as Malware-as-a- Service.It targets browser data, cryptocurrency wallets, and authentication tokens.It communicates with a C2 panel for exfiltration and victim tracking.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-31324, CVE-2025-61882, CVE-2021-35587</td></tr>
<tr><td></td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="4">Data Theft</td><td rowspan="2">SAP NetWeaver, Oracle E- Business Suite, Oracle Access Manager product of Oracle Fusion Middleware</td></tr>
<tr><td>Stealer</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)</td><td>https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html , https://www.oracle.com/security-alerts/alert-cve-2025-61882.html , https://www.oracle.com/security-alerts/ , https://support.oracle.com/support/?kmContentId=3106344 , https://www.oracle.com/security-alerts/cpujan2022.html</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">82cb239612d74eab70b12a0ca448bd82b3c5b418b8f05213d75ddddbbf0b4a5d, ca47c8710c4ffb4908a42bd986b14cddcca39e30bb0b11ed5ca16fe8922a468b</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">StealC</td><td rowspan="6">Stealc is an information-stealing malware offered as a Malware-as-a-Service by a threat actor known as Plymouth on Russian-speaking underground forums since early 2023. Developed in C and built on Windows API functions, it primarily targets sensitive data from web browsers, browser extensions, desktop cryptocurrency wallets, as well as messaging and email clients. To aid in data extraction, it leverages multiple legitimate third-party DLLs commonly associated with browser operations, enabling it to access stored credentials and other valuable information.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-31324, CVE-2025-61882, CVE-2021-35587</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="4">Data Theft</td><td>SAP NetWeaver, Oracle E- Business Suite, Oracle Access Manager product of Oracle Fusion Middleware</td></tr>
<tr><td>Stealer</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html , https://www.oracle.com/security-alerts/alert-cve-2025-61882.html , https://www.oracle.com/security-alerts/ , https://support.oracle.com/support/?kmContentId=3106344 , https://www.oracle.com/security-alerts/cpujan2022.html</td></tr>
<tr><td>Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">dc5fc48cbd764acf7dd28c385279cf8b4296fb2d1e7b9aca3bc2352893194c94, 4630f2e42c67690b34c187feee43eabe447c935dea079b5bf1c480de070d097c</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">Vidar</td><td rowspan="6">Vidar is a widely recognized information-stealing malware family engineered to quietly extract sensitive data from compromised systems. It primarily targets credentials stored in web browsers, cryptocurrency wallet details, session cookies, authentication tokens, autofill entries, and saved payment information, along with files that may contain valuable data. Operating largely in memory, Vidar minimizes its on-disk footprint and maintains communication with remote command-and-control servers, allowing it to discreetly collect and exfiltrate information without triggering obvious signs of compromise.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-31324, CVE-2025-61882, CVE-2021-35587</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Stealer</td><td rowspan="3">Data Theft</td><td>SAP NetWeaver, Oracle E- Business Suite, Oracle Access Manager product of Oracle Fusion Middleware</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)</td><td>https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html , https://www.oracle.com/security-alerts/alert-cve-2025-61882.html , https://www.oracle.com/security-alerts/ , https://support.oracle.com/support/?kmContentId=3106344 , https://www.oracle.com/security-alerts/cpujan2022.html</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">1e92acabf037a60e7fbb97c0ba73e997bb4b602ad51333871423b778cae4f0b1 , 0e90c63363265f75f8637c1a3e9ec277a1ea1a8436dd7561fff59cfb722c6612</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">RedLine</td><td rowspan="6">RedLine Stealer is a versatile malware that can be purchased either as a standalone product or on a subscription basis. It is designed to collect a wide range of information from browsers, including saved credentials, autocomplete data, and credit card details. RedLine Stealer have expanded their capabilities to include the theft of cryptocurrency.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-31324, CVE-2025-61882, CVE-2021-35587</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td rowspan="2">TYPE</td><td rowspan="4">Data Theft</td><td>SAP NetWeaver, Oracle E- Business Suite, Oracle Access Manager product of Oracle Fusion Middleware</td></tr>
<tr><td>PATCH LINK</td></tr>
<tr><td>Stealer</td><td rowspan="2">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html , https://www.oracle.com/security-alerts/alert-cve-2025-61882.html , https://www.oracle.com/security-alerts/ , https://support.oracle.com/support/?kmContentId=3106344 , https://www.oracle.com/security-alerts/cpujan2022.html</td></tr>
<tr><td>ASSOCIATED ACTOR</td></tr>
<tr><td>Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)</td><td colspan="3"></td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">7ac90091d7037384ca3dc9a7a0459e3875e976496b3afd9a6a81ad6ace0ba002, a1d9659e8f9df7dbcfebec0faafadeec8b43e0e5d0818aab0d63d0815490bce5,</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">Meduza</td><td rowspan="6">The Meduza Stealer malware has an objective of comprehensive data theft. It pilfers users' browsing activities, extracting a wide array of browser-related data. From critical login credentials to browsing history and curated bookmarks, no digital artifact is safe. Even crypto wallet extensions, password managers, and 2FA extensions are vulnerable, making Meduza Stealer a significant threat to users' financial and personal data.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-31324, CVE-2025-61882, CVE-2021-35587</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="4">Data Theft</td><td>SAP NetWeaver, Oracle E- Business Suite, Oracle Access Manager product of Oracle Fusion Middleware</td></tr>
<tr><td>Stealer</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html , https://www.oracle.com/security-alerts/alert-cve-2025-61882.html , https://www.oracle.com/security-alerts/ , https://support.oracle.com/support/?kmContentId=3106344 , https://www.oracle.com/security-alerts/cpujan2022.html</td></tr>
<tr><td>Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">9e2b8c3888b8a93e8ebab39e7a6b636f921888edb7d15a6ab56b2e119693aaa8</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">Rhadamanthys</td><td rowspan="8">Rhadamanthys is information-stealing malware distributed through large-scale phishing campaigns. It is designed to exfiltrate sensitive data from infected systems, including credentials and financial information. Targeting various sectors globally has been observed, often masquerading as legitimate communications to deceive victims.</td><td>Exploiting Vulnerabilities</td><td>CVE-2025-31324, CVE-2025-61882, CVE-2021-35587</td></tr>
<tr><td></td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="6">Data Theft</td><td rowspan="2">SAP NetWeaver, Oracle E- Business Suite, Oracle Access Manager product of Oracle Fusion Middleware</td></tr>
<tr><td>Stealer</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td rowspan="3">Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)</td><td rowspan="3">https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html , https://www.oracle.com/security-alerts/alert-cve-2025-61882.html , https://www.oracle.com/security-alerts/ , https://support.oracle.com/support/?kmContentId=3106344 , https://www.oracle.com/security-alerts/cpujan2022.html</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">5db892a52fbebbf0298d3b5b2cf0c3ed7f9612a9d337c56bb168be336d28cadb, b9ad234abeb1490f2c2d28dd2387f0575ba5128ebb799741b1f3179622204175</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Nexcorium	Nexcorium follows a design closely aligned with Mirai-based malware, incorporating elements such as XOR-encoded configuration tables, a watchdog component, and a built-in DDoS attack module. Upon execution, it begins by decoding its embedded configuration using XOR, revealing critical details including the command-and-control server domain and port, persistence-related shell commands, a hard-coded brute-force credential list, attack instructions fetched from the C2 server, and integrated exploit code used to expand its reach.	Exploiting Vulnerabilities	CVE-2024-3721 CVE-2017-17215
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	TBK DVR-4104, TBK DVR-4216, Huawei HG532
Botnet			PATCH LINK
ASSOCIATED ACTOR			EOL
-			
IOC TYPE	VALUE		
SHA256	37132e804ccb3fc4ba1f72205da70c3d7a6e66b43178707a9d8ee1156d815c21, e4789416c35b345e75c023a8c07c207c79937c6a5444e1c29d85d18d2f660d8c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Lotus Wiper	"Lotus Wiper" is a destructive malware designed to render infected systems irrecoverable by disabling recovery mechanisms, overwriting data on physical drives, and systematically deleting files across all accessible volumes. Through this multi-stage wiping process, it ensures that both system functionality and stored data are permanently destroyed, leaving little to no chance for restoration.	-	-
		IMPACT	AFFECTED PLATFORM
TYPE		Wipes Data	-
Wiper			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	405177294F6F9268432A43998049AD0D4A61C6909216533B8713C911BC430755, 9D05854C95C6AFA68911BD28AF12282185E0FE34F2E58FDDBC503AB22D1508D7		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LOTUSLITE backdoor (v1.1)	The LOTUSLITE backdoor (v1.1) reflects a clear evolution from its earlier iteration, with notable changes in code structure and command-and-control communication. One of the most visible shifts appears in the DLL export table, while version 1.0 exposed 16 functions with DataImporterMain acting as the primary entry point, v1.1 expands this to 22 exports and replaces it with DnxMain at the same ordinal. Overall, the update marks a transition from a monolithic architecture to a more modular design, where responsibilities are distributed across multiple dedicated functions, improving flexibility and potentially making analysis and detection more challenging.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise	Windows
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
Mustang Panda			
IOC TYPE	**VALUE**		
SHA256	856476340706411772621 1ff8f89555e5a3b2b70bc9667032abd69cbe53b5216		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SNOWBELT	SNOWBELT is a malicious Chromium browser extension, distributed via social engineering rather than the official Chrome Web Store, that serves as the initial foothold in the attack chain. Disguised as legitimate extensions like “MS Heartbeat” or “System Heartbeat,” it acts as a JavaScript-based backdoor, maintaining persistence through the browser’s extension framework and techniques like Service Worker Alarms and keep-alive tab injection. Its primary role is to capture attacker commands and forward them to the SNOWBASIN component for execution, effectively enabling continuous monitoring and control.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Intercept commands, Maintain persistence	Windows, Linux
			PATCH LINK
ASSOCIATED ACTOR			-
UNC6692			
IOC TYPE	**VALUE**		
SHA256	7f1d71e1e079f3244a69205588d504ed830d4c473747bb1b5c520634cc5a2477, ca390b86793922555c84abc3b34406da2899382c617f9dcf83a74ac09dd18190		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SNOWGLAZE	SNOWGLAZE is a Python-based tunneling component deployed after initial access to handle external communications. Designed to run on both Windows and Linux systems, it establishes a secure, authenticated WebSocket tunnel between the compromised network and the attacker's command-and-control infrastructure, often hosted on services like Heroku. Through this channel, it enables SOCKS proxy functionality, allowing arbitrary TCP traffic to be routed through the infected host for further operations.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Masks malicious traffic	Windows, Linux
Tunneler			**PATCH LINK**
ASSOCIATED ACTOR			-
UNC6692			
IOC TYPE	**VALUE**		
SHA26	2fa987b9ed6ec6d09c7451abd994249dfaba1c5a7da1c22b8407c461e62f7e49		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SNOWBASIN	SNOWBASIN is a Python-based bindshell that provides hands-on control over the compromised system once access is established. Operating as a persistent backdoor, it typically runs a local HTTP server on port 8000, allowing attackers to execute commands via cmd.exe or PowerShell, capture screenshots, and stage data for exfiltration, effectively enabling direct interaction with the infected host.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Execute Commands	Windows, Linux
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
UNC6692			
IOC TYPE	**VALUE**		
SHA256	c8940de8cb917abe158a826a1d08f1083af517351d01642e6c7f324d0bba1eb8		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
EntryShell	EntryShell is a custom backdoor attributed to the Tropic Trooper threat group, historically deployed in espionage operations targeting Chinese-speaking individuals. An EntryShell sample was hosted on the staging server. The sample reused the hardcoded AES-128 ECB key documented in an earlier Tropic Trooper campaign. Its presence on actor infrastructure, combined with the reuse of known watermarks, loaders, and post-exploitation TTPs such as VS Code tunnel abuse, served as a key attribution indicator.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise	Windows
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
Tropic Trooper			
IOC TYPE	**VALUE**		
IPv4	158[.]247[.]193[.]100		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AdaptixC2 Beacon agent	AdaptixC2 is an open-source command-and-control (C2) framework that provides operators with a Beacon agent and configurable Beacon Listeners for managing compromised hosts, similar in concept to commercial offensive security tools like Cobalt Strike. Its agents encrypt C2 traffic using a 16-byte RC4 session key generated at initialization, and standard deployments rely on HTTP or TCP listeners for tasking and exfiltration.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Encrypt Traffic	Windows
Beacon agent			**PATCH LINK**
ASSOCIATED ACTOR			-
Tropic Trooper			
IOC TYPE	**VALUE**		
SHA256	aeec65bac035789073b567753284b64ce0b95bbae62cf79e1479714238af0eb7, 7a95ce0b5f201d9880a6844a1db69aac7d1a0bf1c88f85989264caf6c82c6001		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">TOSHIS loader</td><td rowspan="6">TOSHIS is a custom shellcode loader attributed to the Tropic Trooper threat group, originally observed in the TAOTH campaign. The loader is delivered through trojanized legitimate binaries, most recently a backdoored SumatraPDF reader, where the threat actor hijacks the executable's control flow by redirecting the _security_init_cookie function to execute malicious code, a departure from earlier variants that modified the entry point to jump to the payload.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>TYPE</td><td rowspan="3">Loads Payload</td><td>Windows</td></tr>
<tr><td>Loader</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">-</td></tr>
<tr><td>Tropic Trooper</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">47c7ce0e3816647b23bb180725c7233e505f61c35e7776d47fd448009e887857</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
The Gentlemen	The Gentlemen ransomware-as-a-service (RaaS) operation is quickly gaining traction, drawing in multiple affiliates and claiming over 320 victims, with a significant surge of attacks observed in early 2026. Its toolkit includes a diverse set of lockers written in Go for Windows, Linux, NAS, and BSD systems, along with a C-based variant targeting ESXi, enabling broad coverage across enterprise environments. In a recent incident response case, an affiliate attempted to deploy SystemBC, a proxy malware commonly used in human-operated ransomware campaigns for stealthy tunneling and payload delivery. The group also operates an onion-based leak site to publish stolen data from non-paying victims, while ransom negotiations are handled separately via affiliate-specific Tox IDs, leveraging the decentralized, end-to-end encrypted messaging protocol for secure communication.	Exploiting Vulnerabilities	CVE-2024-55591 CVE-2023-27532 CVE-2024-37085 CVE-2025-7771
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data encryption, Data Exfiltration	Windows, Linux, NAS, BSD, and VMware ESXi
Ransomware			**PATCH LINK**
ASSOCIATED ACTOR			https://fortiguard.fortinet.com/psirt/FG-IR-24-535 , https://www.veeam.com/kb4424 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505
-			

IOC TYPE	VALUE
SHA256	025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a, 22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">SystemBC</td><td rowspan="6">SystemBC is a proxy malware deployed on compromised hosts to establish covert network access for attackers. It creates SOCKS5 tunnels within the victim’s environment and communicates with its command-and-control server using a custom RC4-encrypted protocol. In addition to tunneling, it can download and execute further payloads, either by writing them to disk or injecting them directly into memory for stealthier execution.</td><td>Exploiting Vulnerabilities</td><td>CVE-2024-55591
CVE-2023-27532
CVE-2024-37085
CVE-2025-7771</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>TYPE</td><td rowspan="4">System Compromise</td><td>Windows, Linux, NAS, BSD, and VMware ESXi</td></tr>
<tr><td>Backdoor</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">https://fortiguard.fortinet.com/psirt/FG-IR-24-535 , https://www.veeam.com/kb4424 , https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505</td></tr>
<tr><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">992c951f4af57ca7cd8396f5ed69c2199fd6fd4ae5e93726da3e198e78bec0a5</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-34197	✗	Apache ActiveMQ Broker (Before 5.19.4, 6.0.0 Before 6.2.3), Apache ActiveMQ (Before 5.19.4, 6.0.0 before 6.2.3)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:activemq:*:*:*:*:*:*:*:* cpe:2.3:a:apache:activemq_broker:*:*:*:*:*:*:*:*	-
Apache ActiveMQ Improper Input Validation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20, CWE-94	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://activemq.apache.org/download.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-31324	✗	SAP NetWeaver	Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sap:netweaver:7.50:*:*:*:*:*:*:*	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys
SAP NetWeaver Unrestricted File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-434	T1059: Command and Scripting Interpreter	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-61882	✗	Oracle E- Business Suite Versions 12.2.3- 12.2.14	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:concurrent_processing:*:*:*:*:*:*:*:*	Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)
Oracle E-Business Suite Unspecified Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-287	T1071: Application Layer Protocol	https://www.oracle.com/security-alerts/alert-cve-2025-61882.html , https://www.oracle.com/security-alerts/ , https://support.oracle.com/support/?kmContentId=3106344

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2021-35587	✗	Oracle Access Manager product of Oracle Fusion Middleware affected are 11.1.2.3.0, 12.2.1.3.0 and 12.2.1.4.0.	Scattered Spider, ShinyHunters, and LAPSUS$ (operating collectively as Scattered LAPSUS$ Hunters / SLH / SLSH)
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:access_manager:*:*:*:*:*:*:*:*	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys
Oracle Fusion Middleware Unspecified Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1071: Application Layer Protocol	https://www.oracle.com/security-alerts/cpujan2022.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-3721	✗	TBK DVR-4104 and DVR-4216 up to 20240412	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:tbkvision:tbk-dvr4216:*:*:*:*:*:*:*:* cpe:2.3:h:tbkvision:tbk-dvr4104:*:*:*:*:*:*:*:*	Nexcorium
TBK DVR OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2017-17215	✗	Huawei HG532	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:huawei:hg532_firmware:-:*:*:*:*:*:*:* cpe:2.3:h:huawei:hg532:-:*:*:*:*:*:*:*	Nexcorium
Huawei HG532 Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-20	T1059: Command and Scripting Interpreter	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-55591	✗	FortiOS Versions 7.0.0 through 7.0.16, FortiProxy Versions 7.2.0 through 7.2.12, FortiProxy Versions 7.0.0 through 7.0.19	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*	Gentlemen Ransomware, SystemBC
Fortinet FortiOS Authorization Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1133: External Remote Services	https://fortiguard.fortinet.com/psirt/FG-IR-24-535

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2023-27532	✗	Veeam Backup & Replication Cloud Connect	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*:*	Gentlemen Ransomware, SystemBC
Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1212: Exploitation for Credential Access	https://www.veeam.com/kb4424

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-37085	✗	VMware ESXi	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:vmware:esxi:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*	Gentlemen Ransomware, SystemBC
VMware ESXi Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287 CWE-305	T1068 : Exploitation for Privilege Escalation, T1136.002 : Domain Account	https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/release-notes/esxi-update-and-patch-release-notes/vsphere-esxi-803-release-notes.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-7771	✗	TechPowerUp ThrottleStop.sys version 3.0.0.0 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:techpowerup:throttlestop:*:*:*:*:*:*:*:*	Gentlemen Ransomware, SystemBC
TechPowerUp ThrottleStop Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-782	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting	✗

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Scattered Spider (aka UNC3944, 0ktapus, Muddled Libra, Scatter Swine, Storm-0875, Octo Tempest, LUCR-3, Star Fraud)	Suspected UK and US	Airline, Aviation, Retail, Telecommunications, Financial Services, Banking, Insurance, Technology, Hospitality, Gaming, Education, Media, Food and Beverage, Automotive, Manufacturing, FinTech, Government, Energy, Professional Services, Healthcare, Casino & Gambling, Transportation, Real Estate, Charitable Organizations, Legal	United States, United Kingdom, France, Australia, Italy, Netherlands, South Korea, Spain, Chile, Uruguay, Canada, Brazil, Israel, Ireland, Singapore, Germany, Belgium
	MOTIVE		
	Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-31324, CVE-2025-61882, CVE-2021-35587	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys	SAP NetWeaver, Oracle E-Business Suite, Oracle Access Manager product of Oracle Fusion Middleware

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1583.006: Web Services; T1566: Phishing; T1566.002: Spearphishing Link; T1566.004: Spearphishing Voice; T1078: Valid Accounts; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1195: Supply Chain Compromise; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1136: Create Account; T1136.003: Cloud Account; T1098: Account Manipulation; T1098.005: Device Registration; T1068: Exploitation for Privilege Escalation; T1134: Access Token Manipulation; T1578: Modify Cloud Compute Infrastructure; T1578.005: Modify Cloud Compute Configurations; T1550: Use Alternate Authentication Material; T1550.001: Application Access Token; T1110: Brute Force; T1111: Multi-Factor Authentication Interception; T1528: Steal Application Access Token; T1539: Steal Web Session Cookie; T1555: Credentials from Password Stores; T1555.006: Cloud Secrets Management Stores; T1552: Unsecured Credentials; T1552.001: Credentials in Files; T1003: OS Credential Dumping; T1003.003: NTDS; T1518: Software Discovery; T1526: Cloud Service Discovery; T1210: Exploitation of Remote Services; T1213: Data from Information Repositories; T1119: Automated Collection; T1074: Data Staged; T1074.002: Remote Data Staging; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1090: Proxy; T1090.003: Multi-hop Proxy; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1041: Exfiltration Over C2 Channel; T1020: Automated Exfiltration; T1657: Financial Theft; T1565: Data Manipulation; T1486: Data Encrypted for Impact; T1498: Network Denial of Service

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 ShinyHunters	-	Airline, Aviation, Retail, Telecommunications, Financial Services, Banking, Insurance, Technology, Hospitality, Gaming, Education, Media, Food and Beverage, Automotive, Manufacturing, FinTech, Government, Energy, Professional Services, Healthcare, Casino & Gambling, Transportation, Real Estate, Charitable Organizations, Legal	United States, United Kingdom, France, Australia, Italy, Netherlands, South Korea, Spain, Chile, Uruguay, Canada, Brazil, Israel, Ireland, Singapore, Germany, Belgium
	MOTIVE		
	Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2025-31324, CVE-2025-61882, CVE-2021-35587	LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys	SAP NetWeaver, Oracle E-Business Suite, Oracle Access Manager product of Oracle Fusion Middleware

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1583.006: Web Services; T1566: Phishing; T1566.002: Spearphishing Link; T1566.004: Spearphishing Voice; T1078: Valid Accounts; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1195: Supply Chain Compromise; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1136: Create Account; T1136.003: Cloud Account; T1098: Account Manipulation; T1098.005: Device Registration; T1068: Exploitation for Privilege Escalation; T1134: Access Token Manipulation; T1578: Modify Cloud Compute Infrastructure; T1578.005: Modify Cloud Compute Configurations; T1550: Use Alternate Authentication Material; T1550.001: Application Access Token; T1110: Brute Force; T1111: Multi-Factor Authentication Interception; T1528: Steal Application Access Token; T1539: Steal Web Session Cookie; T1555: Credentials from Password Stores; T1555.006: Cloud Secrets Management Stores; T1552: Unsecured Credentials; T1552.001: Credentials in Files; T1003: OS Credential Dumping; T1003.003: NTDS; T1518: Software Discovery; T1526: Cloud Service Discovery; T1210: Exploitation of Remote Services; T1213: Data from Information Repositories; T1119: Automated Collection; T1074: Data Staged; T1074.002: Remote Data Staging; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1090: Proxy; T1090.003: Multi-hop Proxy; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1041: Exfiltration Over C2 Channel; T1020: Automated Exfiltration; T1657: Financial Theft; T1565: Data Manipulation; T1486: Data Encrypted for Impact; T1498: Network Denial of Service

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 

LAPSUS$ (aka DEV-0537, Strawberry Tempest, Slippy Spider)</td><td>Brazil</td><td rowspan="3">Airline, Aviation, Retail, Telecommunications, Financial Services, Banking, Insurance, Technology, Hospitality, Gaming, Education, Media, Food and Beverage, Automotive, Manufacturing, FinTech, Government, Energy, Professional Services, Healthcare, Casino & Gambling, Transportation, Real Estate, Charitable Organizations, Legal</td><td rowspan="3">United States, United Kingdom, France, Australia, Italy, Netherlands, South Korea, Spain, Chile, Uruguay, Canada, Brazil, Israel, Ireland, Singapore, Germany, Belgium</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-31324, CVE-2025-61882, CVE-2021-35587</td><td>LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys</td><td>SAP NetWeaver, Oracle E-Business Suite, Oracle Access Manager product of Oracle Fusion Middleware</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1583.006: Web Services; T1566: Phishing; T1566.002: Spearphishing Link; T1566.004: Spearphishing Voice; T1078: Valid Accounts; T1190: Exploit Public-Facing Application; T1133: External Remote Services; T1195: Supply Chain Compromise; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1136: Create Account; T1136.003: Cloud Account; T1098: Account Manipulation; T1098.005: Device Registration; T1068: Exploitation for Privilege Escalation; T1134: Access Token Manipulation; T1578: Modify Cloud Compute Infrastructure; T1578.005: Modify Cloud Compute Configurations; T1550: Use Alternate Authentication Material; T1550.001: Application Access Token; T1110: Brute Force; T1111: Multi-Factor Authentication Interception; T1528: Steal Application Access Token; T1539: Steal Web Session Cookie; T1555: Credentials from Password Stores; T1555.006: Cloud Secrets Management Stores; T1552: Unsecured Credentials; T1552.001: Credentials in Files; T1003: OS Credential Dumping; T1003.003: NTDS; T1518: Software Discovery; T1526: Cloud Service Discovery; T1210: Exploitation of Remote Services; T1213: Data from Information Repositories; T1119: Automated Collection; T1074: Data Staged; T1074.002: Remote Data Staging; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1090: Proxy; T1090.003: Multi-hop Proxy; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1041: Exfiltration Over C2 Channel; T1020: Automated Exfiltration; T1657: Financial Theft; T1565: Data Manipulation; T1486: Data Encrypted for Impact; T1498: Network Denial of Service</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Mustang Panda (aka Bronze President, Earth Preta, Stately Taurus, TEMP.Hex, HoneyMyte, Red Lich, Camaro Dragon, PKPLUG, Twill Typhoon, Hive0154)</td><td>China</td><td rowspan="2">Banking and Financial Services, Government, Diplomatic, and Policy Organizations</td><td rowspan="2">India, South Korea</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>LOTUSLITE backdoor (v1.1)</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1566.001: Spear-Phishing Attachment; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1218: System Binary Proxy Execution; T1218.001: Compiled HTML File; T1204: User Execution; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1574: Hijack Execution Flow; T1574.001: DLL; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1106: Native API; T1027: Obfuscated Files or Information; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC6692	-	All	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	SNOWBELT, SNOWGLAZE, SNOWBASIN	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0042: Resource Development; TA0040: Impact; T1566: Phishing; T1566.002: Spearphishing Link; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1059.001: PowerShell; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.006: Python; T1059.007: JavaScript; T1059.010: AutoHotKey & AutoIT; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1559: Inter-Process Communication; T1569: System Services; T1569.002: Service Execution; T1176: Browser Extensions; T1176.001: Browser Extensions; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1547.009: Shortcut Modification; T1068: Exploitation for Privilege Escalation; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1027.015: Compression; T1070: Indicator Removal; T1070.004: File Deletion; T1112: Modify Registry; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1140: Deobfuscate/Decode Files or Information; T1202: Indirect Command Execution; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1562.001: Disable or Modify Tools; T1622: Debugger Evasion; T1003: OS Credential Dumping; T1003.001: LSASS Memory; T1003.002: Security Account Manager; T1003.003: NTDS; T1110: Brute Force; T1110.001: Password Guessing; T1110.003: Password Spraying; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1016: System Network Configuration Discovery; T1018: Remote System Discovery; T1046: Network Service Discovery; T1087: Account Discovery; T1087.001: Local Account; T1007: System Service Discovery; T1012: Query Registry; T1033: System Owner/User Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1083: File and Directory Discovery; T1518: Software Discovery; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1021.002: SMB/Windows Admin Shares; T1005: Data from Local System; T1074: Data Staged; T1113: Screen Capture; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1020: Automated Exfiltration; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1090: Proxy; T1105: Ingress Tool Transfer; T1572: Protocol Tunneling; T1608: Stage Capabilities; T1608.002: Upload Tool; T1608.005: Link Target; T1489: Service Stop

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Tropic Trooper (aka APT23, Earth Centaur, KeyBoy, Bronze Hobart, Pirate Panda, Iron)	China	Government institutions, Military/Navy agencies, Hospitals, Banks, Transportation, High-tech, Healthcare	Taiwan, South Korea, Japan, Philippines, Hong Kong
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	EntryShell backdoor, AdaptixC2 Beacon agent, TOSHIS loader	-

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1585: Establish Accounts; T1585.003: Cloud Accounts; T1587: Develop Capabilities; T1587.001: Malware; T1588: Obtain Capabilities; T1588.001: Malware; T1588.002: Tool; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.002: Upload Tool; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1106: Native API; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1547: Boot or Logon Autostart Execution; T1547.004: Winlogon Helper DLL; T1036: Masquerading; T1036.001: Invalid Code Signature; T1036.004: Masquerade Task or Service; T1620: Reflective Code Loading; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.013: Encrypted/Encoded File; T1127: Trusted Developer Utilities Proxy Execution; T1016: System Network Configuration Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.002: Bidirectional Communication; T1219: Remote Access Tools; T1219.001: IDE Tunneling; T1105: Ingress Tool Transfer; T1132: Data Encoding; T1132.001: Standard Encoding; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1573.002: Asymmetric Cryptography; T1567: Exfiltration Over Web Service; T1567.001: Exfiltration to Code Repository; T1041: Exfiltration Over C2 Channel

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **ten exploited vulnerabilities** and block the indicators related to the threat actors **Scattered Spider, ShinyHunters, LAPSUS$, Mustang Panda, UNC6692, Tropic Trooper,** and malware **LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys, Nexcorium, Lotus Wiper, LOTUSLITE, SNOWBELT, SNOWGLAZE, SNOWBASIN, EntryShell, AdaptixC2 Beacon agent, TOSHIS loader, The Gentlemen,** and **SystemBC.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Run a Scan to discover the assets impacted by the **ten exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Scattered Spider, LAPSUS$, Mustang Panda, Tropic Trooper,** and malware **LummaC2, StealC, Vidar, RedLine, Meduza, Rhadamanthys, Nexcorium, Lotus Wiper, LOTUSLITE, SNOWBASIN, TOSHIS loader, The Gentlemen,** and **SystemBC** in Breach and Attack Simulation(BAS).

Threat Advisories

CVE-2026-34197: Jolokia Exposure Enables RCE in ActiveMQ

Brand Hijack in Cybercrime: Who Is Pretending to Be ShinyHunters?

Nexcorium: IoT Botnet Campaign Exploiting TBK DVR Devices

Lotus Wiper: Silent Sabotage Targeting Venezuela's Energy Sector

LOTUSLITE v1.1: Enhanced Evasion Meets Banking-Themed Social Engineering

April 2026 Linux Patch Roundup

UNC6692 Social Engineering Campaign Deploying SNOW Malware Suite

Tropic Trooper Shifts Tradecraft to Open-Source Offensive Frameworks

The Gentlemen Ransomware: A Rapidly Scaling RaaS Threat

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
LummaC2	SHA256	82cb239612d74eab70b12a0ca448bd82b3c5b418b8f05213d75ddddbbf0b4a5d, ca47c8710c4ffb4908a42bd986b14cddcca39e30bb0b11ed5ca16fe8922a468b
StealC	SHA256	dc5fc48cbd764acf7dd28c385279cf8b4296fb2d1e7b9aca3bc2352893194c94, 4630f2e42c67690b34c187feee43eabe447c935dea079b5bf1c480de070d097c, 5dda23dea89feea09086361d99a9dc1c04f1a2e552a2f5f52cb83d2d8e4e11f8, 9bc696c7c68c2c31cd431ed0af9264fe056942923399b1adb4c55241639bc835, a5f2f3c199df73e31969d96acc46694759792ba294c6311d37bb7b72f5e54fde
Vidar	SHA256	1e92acabf037a60e7fbb97c0ba73e997bb4b602ad51333871423b778cae4f0b1, 0e90c63363265f75f8637c1a3e9ec277a1ea1a8436dd7561fff59cfb722c6612
RedLine	SHA256	7ac90091d7037384ca3dc9a7a0459e3875e976496b3afd9a6a81ad6ace0ba002, a1d9659e8f9df7dbcfebec0faafadeec8b43e0e5d0818aab0d63d0815490bce5, 90522e6a880f6a97719035e3945da1c0c0384f154cf631732ea16a3a9f827b7c, 69587ec2c3e810dc6fca35c13341907fe7a96a24a4222589b72ef97b80e820f4, c1354dcaa9389550c2013e23418bb5c71474b6c368f8e68e51e31faa64ba4ea1

Attack Name	TYPE	VALUE
Meduza	SHA256	9e2b8c3888b8a93e8ebab39e7a6b636f921888edb7d15a6ab56b2e119693aaa8
Rhadamanthys	SHA256	5db892a52fbebbf0298d3b5b2cf0c3ed7f9612a9d337c56bb168be336d28cadb, b9ad234abeb1490f2c2d28dd2387f0575ba5128ebb799741b1f3179622204175, c7ca2f9065557a6d8fb0c02c75804d386b77ffca4466678b201c09e916afa096, b1c5d2eadbb2936f8b9644a5a4e24b5c54b163f0f2d6817c60edb3e5a73c6dc6, 0e94e5712d93d43423f3fec2f3a7f2b859d749411034c839c13e428f651f11a6, 3b9d0e62c06caeaf4244ff2fb275a1919fd9e14243fb436dce313c8d9b89faa4
Nexcorium	SHA256	37132e804ccb3fc4ba1f72205da70c3d7a6e66b43178707a9d8ee1156d815c21, e4789416c35b345e75c023a8c07c207c79937c6a5444e1c29d85d18d2f660d8c, 0b510f93f47590791626d2fa74ddd62ba6eb8a5a5bb7b8476c0ceffc7be94ebe, 9b805585c457811d2c5c5664ede9ee869b53e3c9999100505d7ee8de7f855fdf, 95d1eb12d58206319c514c7240d058c512bb22b31f6ea22ed8be3ae44305c9f7, 7c01d5b53861cd34e10a79fdea16dcf08bce9c78ed72abd6d6f3e9ce75a24734, 838e35b62a6b38675e467301166cdcc54f98d528fe43d56936caeffec88ac696, 2ccf23b8165e8c05899aa7ba4755b896ebf1d20d3b701cffdc768482486b0a74, 29404df12a7723ce46c8b199c88a808aa315dd8ff8fd1e06a34ccd3d16f4553b, b1274de00a7f3d7ab9792ec3456e9d5bf057738666f34183f1d72060e2d4f678, 721c7cb2109ec97c14413cb8b58ddce0ecf0c1f13f22ee4f72eed79b57592cf5, 89dae116c77b0035277d39dfe01043624427c119ddee8883a3ba54a42a6ae400
Lotus Wiper	MD5	0b83ce69d16f5ecd00f4642deb3c5895, c6d0f67db6a7dbf1f9394d98c1e13670, b41d0cd22d5b3e3bdb795f81421a11cb
	SHA256	405177294F6F9268432A43998049AD0D4A61C6909216533B8713C911BC430755, 9D05854C95C6AFA68911BD28AF12282185E0FE34F2E58FDDBC503AB22D1508D7, 1D6F374087087738B7699EBF91F1CFDB3B2A65C2E9BE72E106EE7C9814BE3274

Attack Name	TYPE	VALUE
LOTUSLITE	SHA256	856476340706411772621 1ff8f89555e5a3b2b70bc9667032abd69cbe53b5216
SNOWBELT	SHA256	7f1d71e1e079f3244a69205588d504ed830d4c473747bb1b5c520634cc5a2477, ca390b86793922555c84abc3b34406da2899382c617f9dcf83a74ac09dd18190, 6e6dab993f99505646051d2772701e3c4740096ff9be63c92713bcb7fcddf9f7, de200b79ad2bd9db37baeba5e4d183498d450494c71c8929433681e848c3807f
	URL	cloudfront-021[.]s3[.]us-west-2[.]amazonaws[.]com
SNOWGLAZE	SHA256	2fa987b9ed6ec6d09c7451abd994249dfaba1c5a7da1c22b8407c461e62f7e49
	URL	wss[:]//sad4w7h913-b4a57f9c36eb[.]herokuapp[.]com/ws
SNOWBASIN	SHA256	c8940de8cb917abe158a826a1d08f1083af517351d01642e6c7f324d0bba1eb8
EntryShell	IPv4	158[.]247[.]193[.]100
AdaptixC2 Beacon agent	SHA256	aeec65bac035789073b567753284b64ce0b95bbae62cf79e1479714238af0eb7, 7a95ce0b5f201d9880a6844a1db69aac7d1a0bf1c88f85989264caf6c82c6001
TOSHIS loader	SHA256	47c7ce0e3816647b23bb180725c7233e505f61c35e7776d47fd448009e887857
The Gentlemen	SHA256	025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a, 22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67, 2ed9494e9b7b68415b4eb151c922c82c0191294d0aa443dd2cb5133e6bfe3d5d, 3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235, 48d9b2ce4fcd6854a3164ce395d7140014e0b58b77680623f3e4ca22d3a6e7fd, 62c2c24937d67fdeb43f2c9690ab10e8bb90713af46945048db9a94a465ffcb8, 860a6177b055a2f5aa61470d17ec3c69da24f1cdf0a782237055cba431158923, 87d25d0e5880b3b5cd30106853cbfc6ef1ad38966b30d9bd5b99df46098e546c, 8c87134c1b45e990e9568f0a3899b0076f94be16d3c40fa824ac1e6c6ee892db,

Attack Name	TYPE	VALUE
The Gentlemen	SHA256	91415e0b9fe4e7cbe43ec0558a7adf89423de30d22b00b985c2e4b97e75076b1, 994d6d1edb57f945f4284cc0163ec998861c7496d85f6d45c08657c9727186e3, 9f61ff4deb8afced8b1ecdc8787a134c63bde632b18293fbfc94a91749e3e454, a7a19cab7aab606f833fa8225bc94ec9570a6666660b02cc41a63fe39ea8b0ad, b67958afc982cafbe1c3f114b444d7f4c91a88a3e7a86f89ab8795ac2110d1e6, c46b5a18ab3fb5fd1c5c8288a41c75bf0170c10b5e829af89370a12c86dd10f8, c7f7b5a6e7d93221344e6368c7ab4abf93e162f7567e1a7bcb8786cb8a183a73, ec368ae0b4369b6ef0da244774995c819c63cffb7fd2132379963b9c1640ccd2, efaf8e7422ffd09c7f03f1a5b4e5c2cc32b05334c18d1ccb9673667f8f43108f, f736be55193c77af346dbe905e25f6a1dee3ec1aedca8989ad2088e4f6576b12, fc75ed2159e0c8274076e46a37671cfb8d677af9f586224da1713df89490a958, 5dc607c8990841139768884b1b43e1403496d5a458788a1937be139594f01dca, 788ba200f776a188c248d6c2029f00b5d34be45d4444f7cb89ffe838c39b8b19, 1eece1e1ba4b96e6c784729f0608ad2939cfb67bc4236dfababbe1d09268960c
SystemBC	SHA256	992c951f4af57ca7cd8396f5ed69c2199fd6fd4ae5e93726da3e198e78bec0a5

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a demo of **HivePro**.

REPORT GENERATED ON

April 28, 2026 • 4:00 AM

More at www.hivepro.com