Date of Publication
June 22, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

15 to 21 June 2026

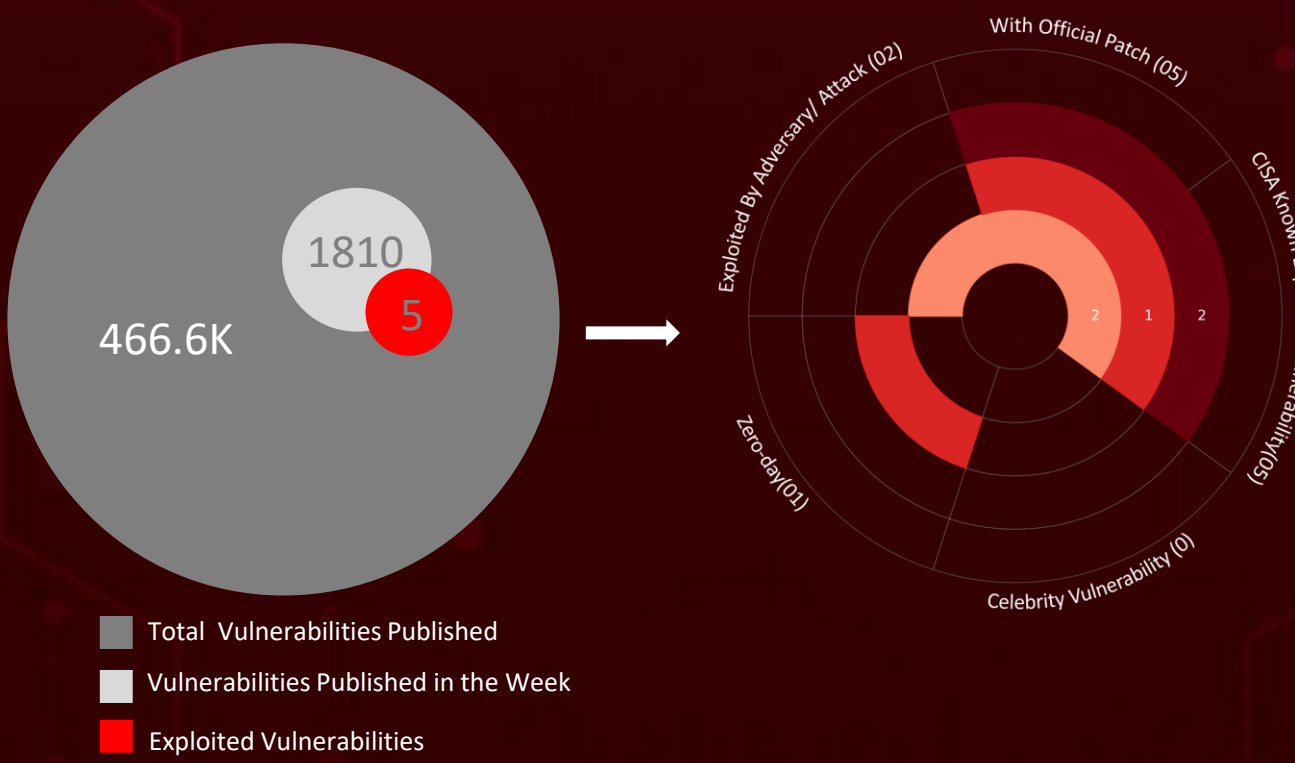
Table Of Contents

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, **seven** major attacks were detected, **five** critical vulnerabilities were actively exploited, and **three** threat actors were closely monitored, reflecting an alarming escalation in malicious activities.

CVE-2026-10520 Ivanti Sentry Critical pre-authentication command injection flaw allowing remote attackers to execute arbitrary commands as root through a single crafted request, with public proof-of-concept code rapidly driving mass exploitation of exposed appliances. **Sinobi Ransomware** closed vetted-affiliate ransomware-as-a-service operation assessed as a successor to Lynx, gaining entry through compromised SonicWall SSL VPN credentials, stripping EDR and exfiltrating data before deploying a Curve25519 locker that deletes shadow copies and enforces double extortion.

Meanwhile, **SPECTRALVIPER**, the signature backdoor of Vietnam-aligned actor **OceanLotus**, planted through a compromised stock-trading update server and a targeted infrastructure intrusion to sustain covert espionage access for up to fifteen months. **Insomnia** Data-theft-only extortion group operating without an encryptor, entering through infostealer-harvested credentials and authentication bypass and publishing stolen US healthcare records on a Tor leak site to coerce victims. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

7
Attacks Executed

5
Vulnerabilities Exploited

3
Adversaries in Action

- SPECTRALVIPER
- Sinobi Ransomware
- INFINITERED
- DarkKomet
- Lumma
- Vidar
- RenEngine

- CVE-2026-10520
- CVE-2026-20262
- CVE-2024-53704
- CVE-2024-40766
- CVE-2026-54420

- OceanLotus
- UNC6508
- Insomnia

Insights

Insomnia No encryptor, no recovery: this extortion crew steals US healthcare records and dumps them free on Tor, with one dermatology breach alone exposing 160,000+ people.

Sinobi Ransomware Lynx successor breaks in through compromised SonicWall SSL VPN credentials, kills EDR, and has scaled to 250+ leak-site victims by May 2026 under a 7-day double-extortion deadline.

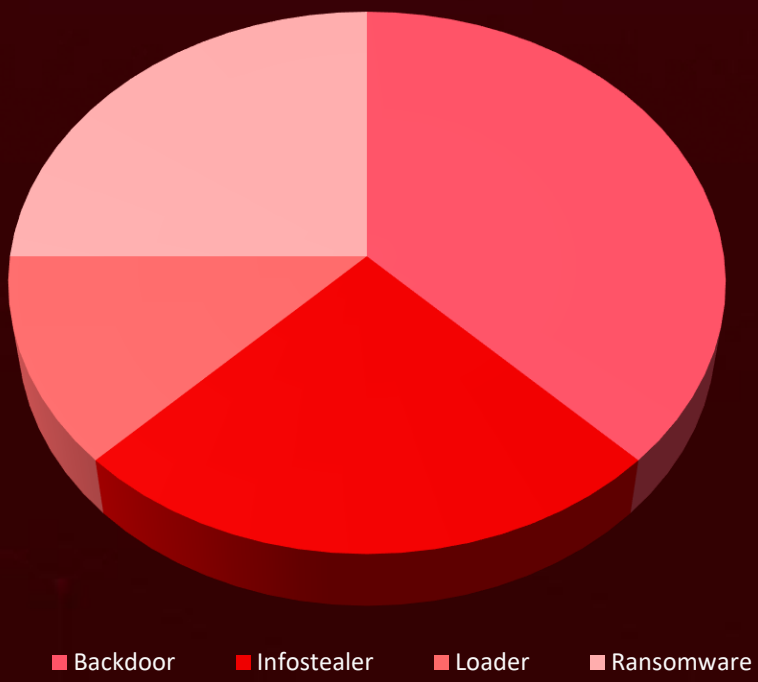
SPECTRALVIPER **OceanLotus** turned inward, riding a poisoned stock-trading update server to sit undetected for up to 15 months while watching individual Vietnamese investors.

INFINITERED PRC-nexus UNC6508 lurked on research servers for over a year, then abused domain mail-compliance rules to silently BCC sensitive defense and research email to its own mailbox.

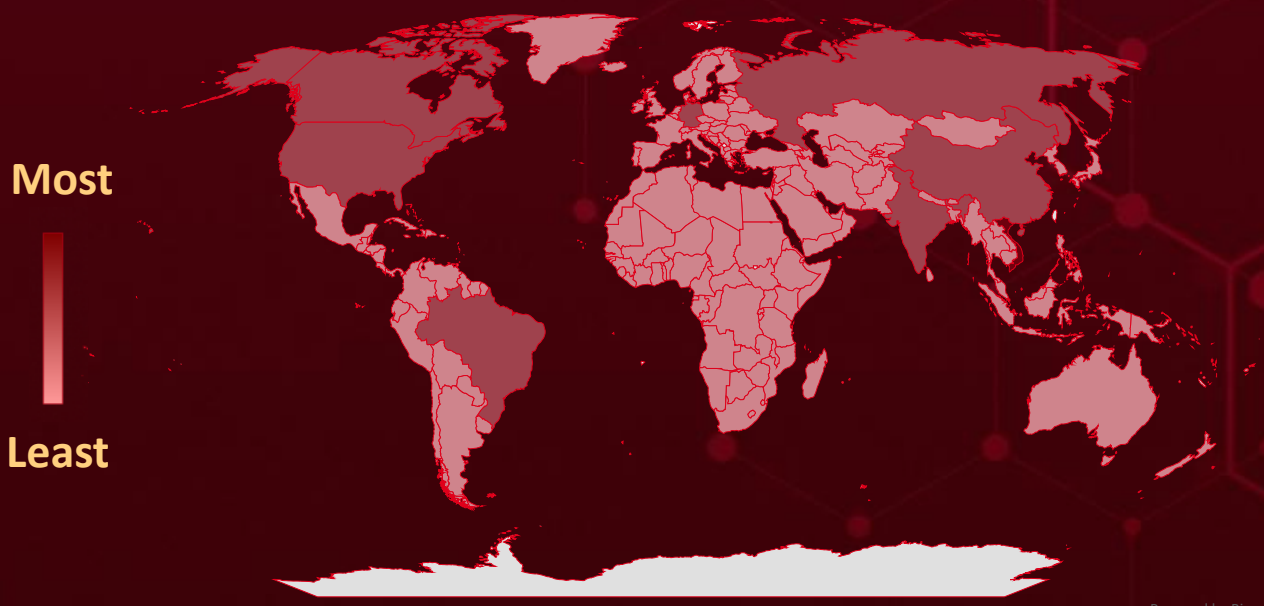
CVE-2026-54420 LiteSpeed cPanel A mishandled symlink lets any user with FTP or web shell access escalate to root and shatter CageFS isolation across every tenant on a shared host.

CVE-2026-10520 Ivanti Sentry Pre-auth command injection gives root through a single crafted request, and a public PoC turned it into mass exploitation of exposed appliances within days.

Threat Distribution

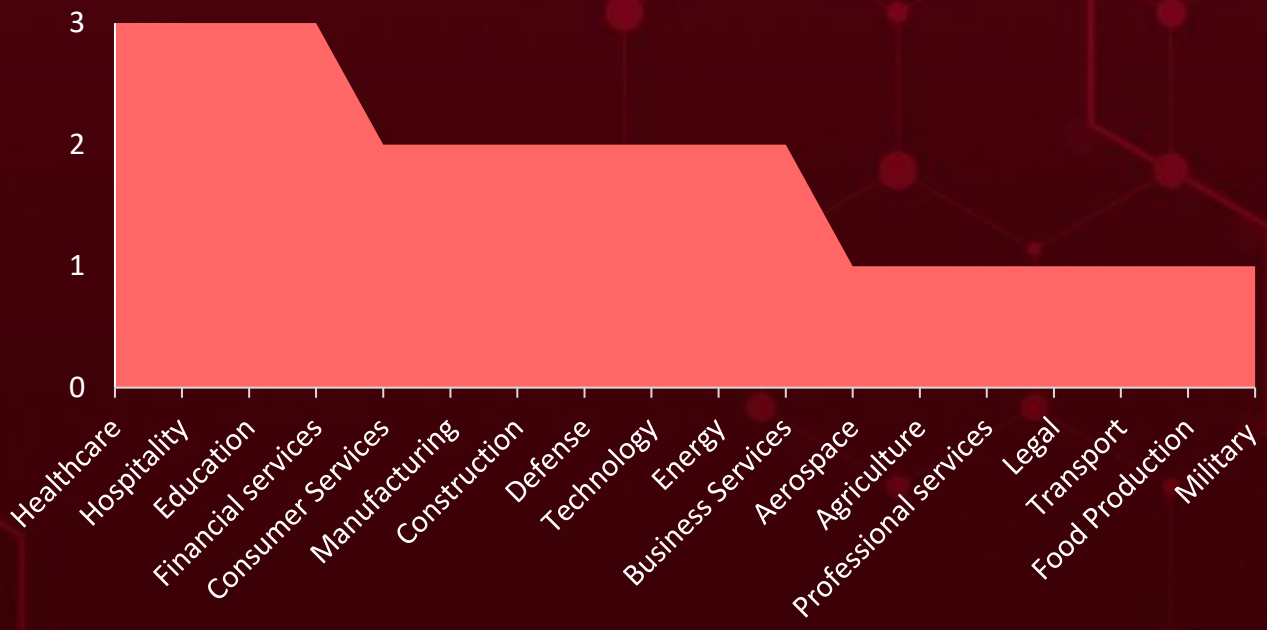


Targeted Countries



Countries	Countries	Countries	Countries
Singapore	Nigeria	Saint Lucia	Chad
Vietnam	Belarus	Bulgaria	Poland
China	Romania	Sierra Leone	Chile
United States	Belgium	Burkina Faso	Rwanda
Germany	St. Vincent & Grenadines	Sweden	China
Brazil	Belize	Burundi	Saudi Arabia
Russia	Turkmenistan	Tonga	Colombia
Canada	Benin	Cabo Verde	Sierra Leone
India	Liechtenstein	United Arab Emirates	Comoros
Papua New Guinea	Bhutan	Cambodia	Solomon Islands
Malawi	Malta	Zimbabwe	Costa Rica
Tanzania	Bolivia	Cameroon	South Sudan
Azerbaijan	Mongolia	Luxembourg	Côte d'Ivoire
Myanmar	Bosnia and Herzegovina	Angola	Suriname
Bahamas	Netherlands	Maldives	Croatia
Saudi Arabia	Botswana	Central African Republic	Tanzania
Bahrain	Oman	Mauritania	Cuba
Uzbekistan	Andorra	Chad	Tonga
Bangladesh	Poland	Moldova	Cyprus
Mexico	Brunei	Chile	Tuvalu
Barbados	Switzerland	Morocco	Czech Republic
		Papua New Guinea	United Kingdom
			Denmark
			Venezuela

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1133
External Remote Services

T1190
Exploit Public-Facing Application

T1204
User Execution

T1588
Obtain Capabilities

T1486
Data Encrypted for Impact

T1068
Exploitation for Privilege Escalation

T1555
Credentials from Password Stores

T1071
Application Layer Protocol

T1082
System Information Discovery

T1078
Valid Accounts

T1027
Obfuscated Files or Information

T1505
Server Software Component

T1083
File and Directory Discovery

T1072
Software Deployment Tools

T1059.001
PowerShell

T1204.001
Malicious Link

T1588.006
Vulnerabilities

T1505.003
Web Shell

T1071.001
Web Protocols

Attacks Executed

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">SPECTRALVIPER</td><td rowspan="6">SPECTRALVIPER is a heavily obfuscated x64 backdoor tied to the OceanLotus cluster, used for espionage-focused intrusions. It supports PE loading, file upload and download, and token impersonation, communicating with operators over named pipes. It provides long-term covert access and a channel for follow-on payload delivery.</td><td>DLL side-loading</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Covert espionage access</td><td rowspan="2">Windows</td></tr>
<tr><td>Backdoor</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>OceanLotus</td><td>-</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>IPv4</td><td colspan="3">38[.]60[.]245[.]37,
139[.]99[.]33[.]239,
139[.]162[.]11[.]152,
139[.]180[.]128[.]42,
142[.]91[.]98[.]77</td></tr>
<tr><td>SHA256</td><td colspan="3">2bfaf9773b7fac658ab439b9b763a92e144e5388301ca03021ef56501be3036a</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">Sinobi Ransomware</td><td rowspan="6">Sinobi Ransomware is a double-extortion ransomware operation assessed as a successor in the INC and Lynx lineage at medium confidence. It gains access through compromised SonicWall SSL VPN credentials, then destroys shadow copies and disables endpoint defenses before encrypting with Curve-25519. Stolen data is published on a dedicated leak site to pressure victims.</td><td>Compromised SonicWall SSL VPN credentials</td><td>CVE-2024-53704
CVE-2024-40766</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Anti-recovery encryption, double extortion</td><td>Windows</td></tr>
<tr><td>Ransomware</td><td>PATCH LINKS</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003,
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015</td></tr>
<tr><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">1b2a1e41a7f65b8d9008aa631f113cef36577e912c13f223ba8834bbefa4bd14,
676dc8e28c90e64000a998ec257c014cb1152e7a5bdccab3916d8fba401853da,
9432b065c803baa54f1fefac20d97affce212dec2bb9a597fc010064d391fc24,
8bb8c6e72d20e9b07bb55e0b0d168efe99d0088122131ae96d13fa01d3325a17,
82cd0af26bc1e9e3b0bfcfe6c61cf467992367a31d87e6bd7e2efa8e9fecbb25,
d4919a7402d7ae02516589fbdfb3cc436749544052843a37b5d36ac4b7385b18</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">INFINITERED</td><td rowspan="6">INFINITERED is a custom backdoor used by the PRC-nexus actor UNC6508 against North American medical research institutions running REDCap. Deployed roughly three months after initial foothold, following a help.php web shell, it provides persistent covert access. The operators reached domain administrator and harvested email and research data.</td><td>Post-compromise, via web shell</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Domain admin, data theft</td><td rowspan="2">REDCap servers; Google Workspace</td></tr>
<tr><td>Backdoor</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>UNC6508</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">51a57bfc9ed3eb6451c1c289607814d59e1698c666fb97ac5f694c398f23d045,
8f0158855a656b629ca76ebca565f18bc25563ded34b65d6771632c20edb68ec</td></tr>
<tr><td>GUID delimiter</td><td colspan="3">b49e334d-9c01-463e-9bc5-00a6920fb66e</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
DarkKomet	DarkKomet is a backdoor distributed through malicious Wallpaper Engine packages on Steam Workshop. In the NTRaholic sample it drops as Synaptics.exe behind a working game front, while a modified AggregatorHost.dll hunts stored Steam credentials and hijacks active sessions. It gives operators persistent remote access and harvests credentials.	Steam Workshop, Wallpaper Engine	-
		IMPACT	AFFECTED PRODUCT
TYPE		Remote access, Steam hijacking	Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	287cfee849fb039c74d55222db58512d597381c3c30fbd2f1bb1a2500e9a7129

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Lumma	Lumma is a malware-as-a-service information stealer sold on underground forums, harvesting browser credentials, cookies, session tokens, and cryptocurrency wallet data. In this period it appears as an early-stage payload distributed by the RenEngine loader.	Loader chains, cracked software	-
		IMPACT	AFFECTED PRODUCT
TYPE		Credential and wallet theft	Windows
Infostealer			
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	f0668ce925f36ff7f3359b0ea47e3fa243af13cd6ad9661dfccc9ff79fb4f1cc

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
Vidar	Vidar is a widely used information stealer that exfiltrates saved passwords, cookies, autofill data, and wallet contents. It is delivered as a later-stage payload in the RenEngine loader chain and sends collected data to attacker infrastructure.	Loaders, cracked game installers	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data theft	Windows
Infostealer			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	0e90c63363265f75f8637c1a3e9ec277a1ea1a8436dd7561fff59cfb722c6612		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RenEngine	RenEngine is a multi-stage loader bundled inside malicious Steam Workshop wallpaper packages, executed when the application wallpaper is applied. It unpacks and runs additional payloads while presenting a functional front to avoid suspicion.	Steam Workshop, Wallpaper Engine	-
		IMPACT	AFFECTED PRODUCT
TYPE		Stealer deployment, data theft	Windows
Loader			
ASSOCIATED ACTOR			PATCH LINK
-			-

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 PRODUCTS	ASSOCIATED ACTOR
CVE-2026-10520		Ivanti Sentry (Before R10.5.2 / R10.6.2 / R10.7.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:standalone_sentry:*:*:*:*:*:*:*:*	-
Ivanti Sentry OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523?language=en_US

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="4">CVE-2026-20262</td><td>  </td><td rowspan="2">Cisco Catalyst SD-WAN Manager (releases 20.9.9.1 and earlier, 20.12.7.1 and earlier, 20.15.4.4 and earlier, 20.15.5.2 and earlier, 20.18.3, and 26.1.1.1 and earlier)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-22</td><td>T1190: Exploit Public-Facing Application, T1505: Server Software Component, T1078: Valid Accounts</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-53704		SonicWALL Gen7 NSv Version Prior to 7.0.1-5165, SonicWALL Gen7 Firewalls Version Prior to 7.1.3-7015, SonicWALL TZ80 Version Prior to 8.0.0-8037	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:sonicwall:sonicos:*:*:*:*:*:*:*:*	Sinobi Ransomware
SonicWall SonicOS SSLVPN Authentication Bypass Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-287	T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1078: Valid Accounts	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-40766	✗	SonicWall SonicOS SOHO (Gen 5) version 5.9.2.14-12o and older, Gen6, Firewalls Version 6.5.4.14-109n and older, Gen7 Firewalls SonicOS build version 7.0.1-5035 and older	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:sonicwall:sonicos:*:*:*:*:*:*:*:*	Sinobi Ransomware
SonicWall SonicOS Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1078: Valid Accounts, T1499: Endpoint Denial of Service	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-54420</td><td>✗</td><td rowspan="2">LiteSpeed cPanel Plugin (user-end) (Before 2.4.8), as distributed in LiteSpeed WHM Plugin (Before 5.3.2.0)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:litespeedtech:litespeed_cpanel_plugin:*:*:*:*:*:*:*:* cpe:2.3:a:litespeedtech:litespeed_whm_plugin:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-61</td><td>T1078: Valid Accounts, T1068: Exploitation for Privilege Escalation, T1611: Escape to Host</td><td>https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/</td></tr>
</table>

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">OceanLotus (alias APT32, SeaLotus, APT-C-00, Ocean Buffalo, Tin Woodlawn, ATK 17, SectorF01, Pond Loach, APT-LY-100, Lotus Bane)</td><td>Vietnam</td><td rowspan="2">Financial services, Stock investors, Infrastructure, Transport, Construction</td><td rowspan="2">Vietnam (domestic); historically China and Southeast Asia</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage and Information Theft</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>SPECTRALVIPER</td><td>FireAnt Metakit; Microsoft SQL Server</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access, T1195: Supply Chain Compromise, T1195.002: Compromise Software Supply Chain, T1190: Exploit Public-Facing Application, TA0002: Execution, T1059: Command and Scripting Interpreter, T1204: User Execution, TA0003: Persistence, T1574: Hijack Execution Flow, T1574.001: DLL, TA0005: Defense Evasion, T1055: Process Injection, T1036: Masquerading, T1027: Obfuscated Files or Information, T1553: Subvert Trust Controls, T1553.002: Code Signing, TA0007: Discovery, T1082: System Information Discovery, TA0008: Lateral Movement, T1570: Lateral Tool Transfer, T1021: Remote Services, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1573: Encrypted Channel, T1105: Ingress Tool Transfer, TA0010: Exfiltration, T1041: Exfiltration Over C2 Channel</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UNC6508</td><td>China (PRC-nexus)</td><td rowspan="3">Medical and clinical research, academic research centers, military health institutions, health regulatory bodies, professional advocacy groups, defense</td><td rowspan="3">North America</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage and Information Theft</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>INFINITERED</td><td>REDCap (Research Electronic Data Capture); Google Workspace content compliance rules</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access, T1190: Exploit Public-Facing Application, TA0002: Execution, T1059: Command and Scripting Interpreter, TA0003: Persistence, T1505: Server Software Component, T1505.003: Web Shell, T1554: Compromise Host Software Binary, TA0006: Credential Access, T1056: Input Capture, T1056.003: Web Portal Capture, TA0007: Discovery, T1087: Account Discovery, TA0008: Lateral Movement, T1021: Remote Services, TA0004: Privilege Escalation, T1078: Valid Accounts, TA0009: Collection, T1074: Data Staged, T1074.001: Local Data Staging, T1114: Email Collection, T1114.003: Email Forwarding Rule, T1213: Data from Information Repositories, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1090: Proxy, T1090.002: External Proxy, TA0010: Exfiltration, T1567: Exfiltration Over Web Service, TA0005: Defense Evasion, T1027: Obfuscated Files or Information</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Insomnia	-	Healthcare, Business Services & Consulting, Manufacturing, Technology, Hospitality, Financial Services, Energy, Aerospace & Defense, Legal	United States, Singapore, Brazil
	MOTIVE		
	Financial Gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	-	-	-

TTPs
TA0042: Resource Development, T1650: Acquire Access, TA0001: Initial Access, T1078: Valid Accounts, T1190: Exploit Public-Facing Application, TA0008: Lateral Movement, T1072: Software Deployment Tools, TA0009: Collection, T1005: Data from Local System, TA0010: Exfiltration, T1567: Exfiltration Over Web Service, TA0040: Impact, T1657: Financial Theft

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actor **OceanLotus, UNC6508, Insomnia,** and malware **SPECTRALVIPER, Sinobi Ransomware, INFINITERED, DarkKomet, Lumma, Vidar, RenEngine.**

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

- Running a Scan to discover the assets impacted by the **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors malware **Sinobi Ransomware, SPECTRALVIPER, DarkKomet** in Breach and Attack Simulation(BAS).

Threat Advisories

CVE-2026-10520: Critical Ivanti Sentry Flaw Triggers Exploitation Surge

OceanLotus Pivots to Domestic Espionage with SPECTRALVIPER

Cisco SD-WAN Under Fire: Exploited Path Traversal Bug Enables Root-Level Access

Sinobi Ransomware: A Fast-Rising Mid-Market Threat to Watch in 2026

China-Nexus Espionage: UNC6508 Strikes North America

CVE-2026-54420: LiteSpeed cPanel Flaw Actively Exploited for Root Access

Threat Actors Turn Steam Workshop Into a Malware Distribution Hub

Insomnia: Data-Theft Extortion Operation Targeting US Healthcare

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
SPECTRALVIPER	SHA256	2bfaf9773b7fac658ab439b9b763a92e144e5388301ca03021ef56501be3036a
	Domains	leadingfilipinoteams[.]com coachcybersecurity[.]com, gatewayrvcenter[.]com, mxprodesign[.]com financemachinelearning[.]com, power-sync-services[.]com
	IPv4	38[.]60[.]245[.]37, 139[.]99[.]33[.]239, 139[.]162[.]11[.]152, 139[.]180[.]128[.]42, 142[.]91[.]98[.]77

Attack Name	TYPE	VALUE
Sinobi	SHA256	1b2a1e41a7f65b8d9008aa631f113cef36577e912c13f223ba8834bbefa4bd14, 676dc8e28c90e64000a998ec257c014cb1152e7a5bdccab3916d8fba401853da, 9432b065c803baa54f1fefac20d97affce212dec2bb9a597fc010064d391fc24, 8bb8c6e72d20e9b07bb55e0b0d168efe99d0088122131ae96d13fa01d3325a17, 82cd0af26bc1e9e3b0bfcfe6c61cf467992367a31d87e6bd7e2efa8e9fecbb25, d4919a7402d7ae02516589fbdfb3cc436749544052843a37b5d36ac4b7385b18
	File Extension	.SINOBI
	Tor Domain	sinobi7yuoppj76qnkwiobwfc2qve2xkv2ckvzyyjblwd7ucpptl62ad[.]onion/login, sinobi57mfegeov2naiufkidlkpze263jtbldokimfjqmk2mye6s4yqd[.]onion/login, sinobibjqytwqxjw24zuerqcjyd3hoow6zia7z6kzvwawivamu7nqayd[.]onion/login, sinobicrh73ongfuxjajmlyyhalvkhlcgttxkxaxz3gvsgdcgf76uiqd[.]onion/login, sinobi6ftrg27d6g4sjdt65malds6cfptlnjyw52rskakqjda6uvb7yd[.]onion, sinobi6rlec6f2bgn6rd72xo7hvds4a5ajiu2if4oub2sut7fg3gomqd[.]onion, sinobi6ywgmmvg2gj2yygkb2hxbimaxpqkyk27wti5zjwhfcldhackid[.]onion, sinobi7l3wet3uqn4cagjiessuomv75aw3bvgah4jpj43od7xndb7kad[.]onion, sinobi7sukclb3ygtorysbtrodgdbnrmgbhov45rwzipubbzhiu5jvqd[.]onion, sinobi23i75c3znmqqxxyuzqvhxnjsar7actgvc4nqeuhgcn5yvz3zqd[.]onion, sinobia6mw6ht2wcdjphessyzpy7ph2y4dyqbd74bgobgju4ybytmkqd[.]onion,

Attack Name	TYPE	VALUE
INFINITERED	SHA256	8f0158855a656b629ca76ebca565f18bc25563ded34b65d6771632c20edb68ec, 51a57bfc9ed3eb6451c1c289607814d59e1698c666fb97ac5f694c398f23d045
	Session ID prefix	xc32038474a
	GUID delimiter	b49e334d-9c01-463e-9bc5-00a6920fb66e
DarkKomet	SHA256	287cfee849fb039c74d55222db58512d597381c3c30fbd2f1bb1a2500e9a7129
Lumma	SHA256	f0668ce925f36ff7f3359b0ea47e3fa243af13cd6ad9661dfccc9ff79fb4f1cc
Vidar	SHA256	0e90c63363265f75f8637c1a3e9ec277a1ea1a8436dd7561fff59cfb722c6612

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

June 22, 2026 • 09:30 PM

More at www.hivepro.com