Date of Publication
June 15, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

08 to 14 JUNE 2026

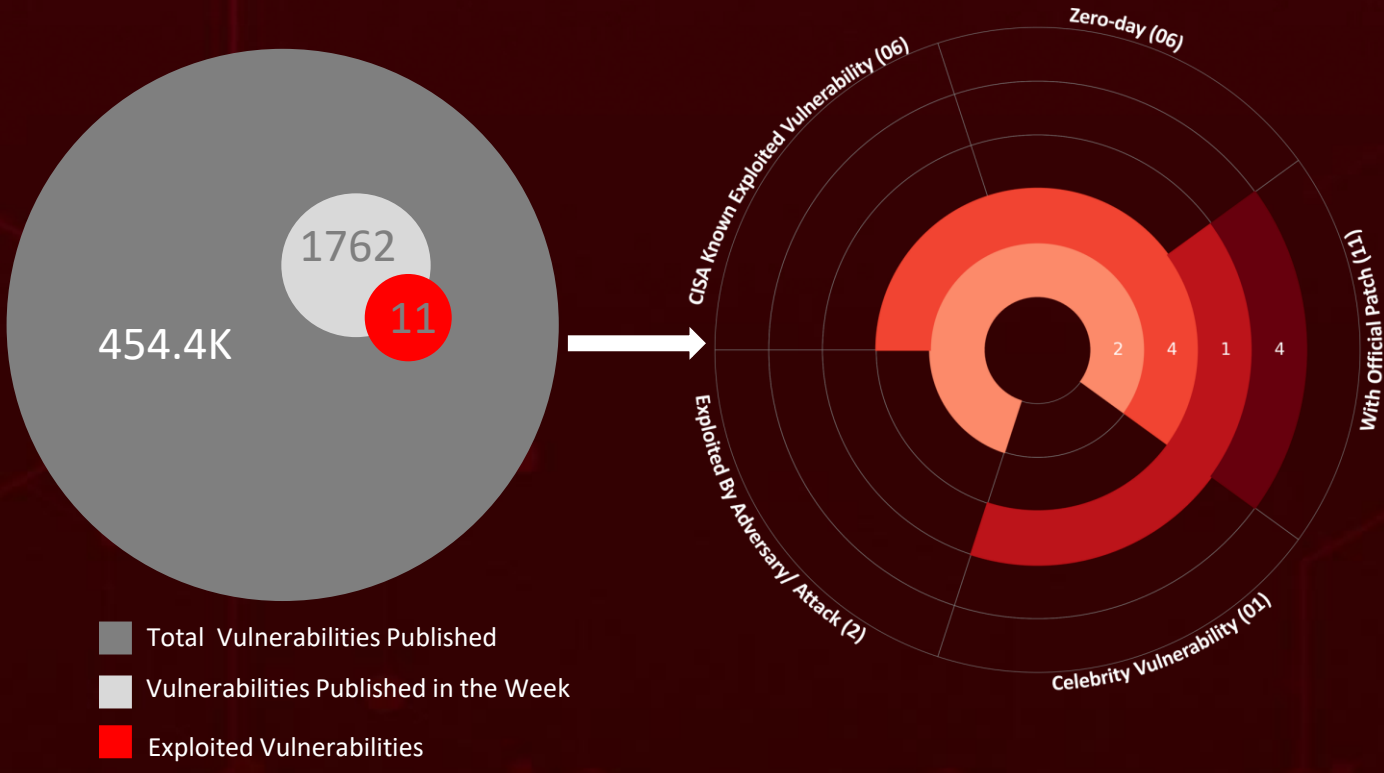
Table Of Contents

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, **11** major attacks were detected, **11** critical vulnerabilities were publicly disclosed, and **two** active threat actor groups were monitored, signaling a concerning escalation in malicious activity.

Notable vulnerabilities included an actively exploited **zero-day in Cisco Catalyst SD-WAN Manager** (**CVE-2026-20245**) that chains earlier auth-bypass flaws to turn netadmin access into root and fleet-wide impact, and a legacy-IKEv1 authentication-bypass zero-day in Check Point's VPN products (**CVE-2026-50751**) already linked to a **Qilin ransomware** affiliate.

On the tooling and actor side, a new ransomware operator, **CMD Organization**, emerged with a novel public crypto-bidding model that auctions stolen data alongside negotiations, and a new modular post-exploitation backdoor, **MLTBackdoor**, surfaced using a ClickFix delivery chain. This underscores the need for disciplined security updates and sustained monitoring in response to rapidly evolving attack methodologies.



High Level Statistics

11
Attacks Executed

11
Vulnerabilities Exploited

2
Adversaries in Action

- CMD Organization
- StealC
- Meow
- Interlock
- Medusa
- Anubis
- Rhadamanthys
- AsyncRAT
- Lumma
- Qilin
- MLTBackdoor

- CVE-2026-20245
- CVE-2026-20182
- CVE-2026-20127
- CVE-2026-50751
- CVE-2026-11645
- CVE-2026-49160
- CVE-2026-45586
- CVE-2026-50507
- CVE-2026-47291
- CVE-2026-49975
- CVE-2026-35273

- TeamPCP
- ShinyHunters

Insights

38% and Climbing: CMD Organization's Aggressive Push into US Healthcare

190 Million and Counting: Healthcare's Year on the Critical Infrastructure Frontline

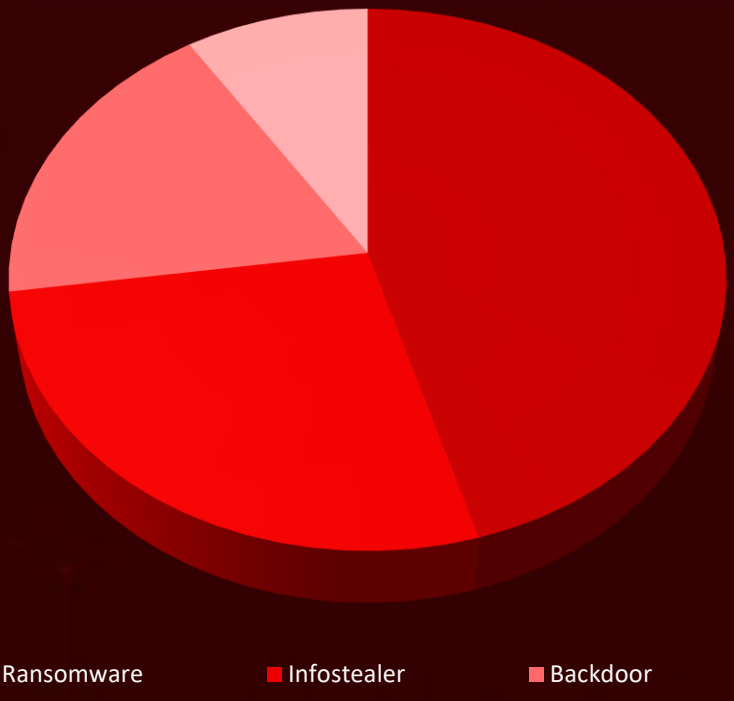
Root on the Management Plane: Cisco's Actively-Exploited SD-WAN Flaw

Copy, Paste, Compromised: Inside the MLTBackdoor ClickFix Campaign

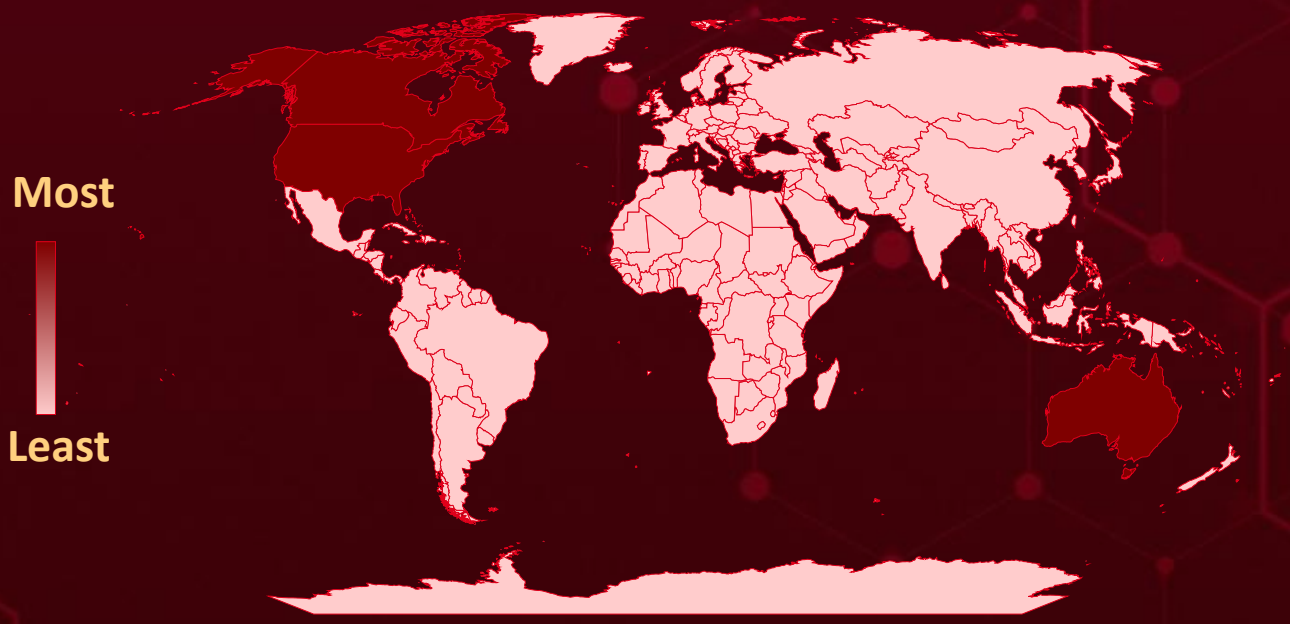
Out of Bounds, Out of Control: The Chrome Flaw (CVE-2026-11645) Exploited in the Wild

No Password, No Problem: Check Point's VPN Zero-Day Lets Attackers Walk In

Threat Distribution

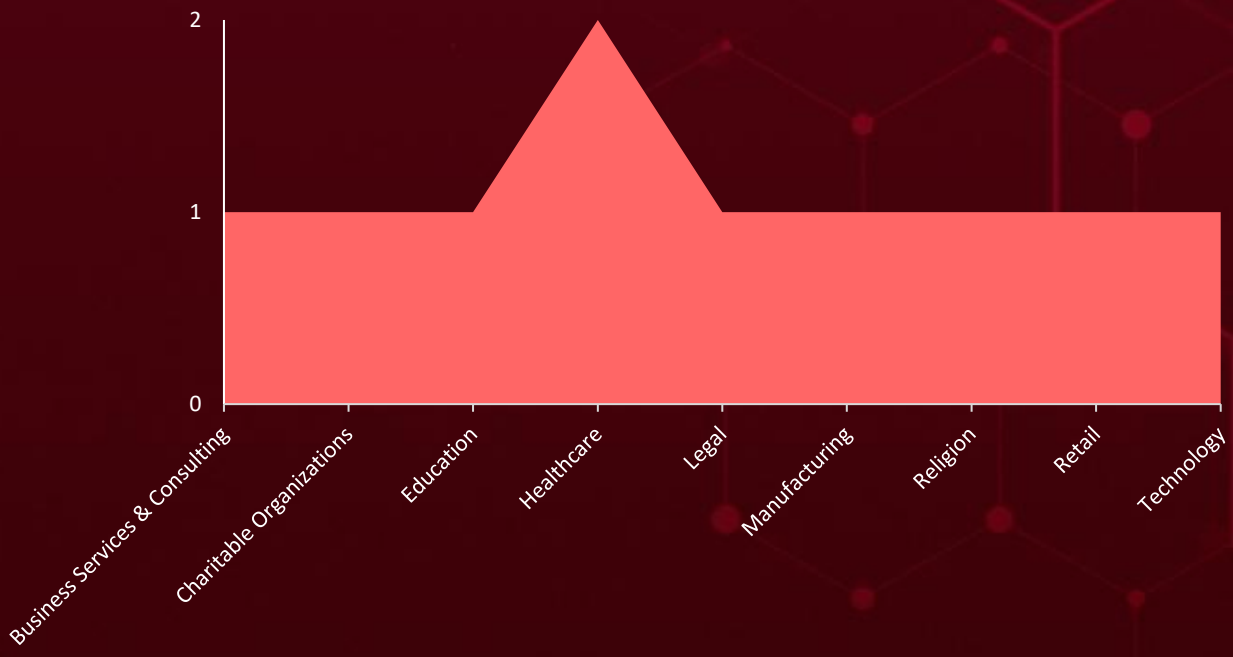


Targeted Countries



Countries	Countries	Countries	Countries
Australia	Belarus	Moldova	Sweden
Canada	Myanmar	Cambodia	Cyprus
United States	Belgium	Morocco	Tanzania
Oman	Nigeria	Cameroon	Czechia
Afghanistan	Belize	Nauru	Tonga
South Korea	Panama	Algeria	Democratic Republic of the Congo
Angola	Benin	Nicaragua	
Mongolia	Romania	Central African Republic	Turkmenistan
Antigua and Barbuda	Bhutan	North Macedonia	Denmark
Saint Lucia	Sao Tome and Principe	Chad	United Arab Emirates
Argentina	Bolivia	Palau	Djibouti
Tunisia	Slovenia	Chile	Venezuela
Armenia	Bosnia and Herzegovina	Paraguay	Dominica
Malta		China	Zimbabwe
Albania	Sudan	Portugal	Dominican Republic
Netherlands	Botswana	Colombia	Lithuania
Austria	Timor-Leste	Rwanda	Ecuador
Philippines	Brazil	Comoros	Madagascar
Azerbaijan	Uganda	Samoa	Egypt
Seychelles	Brunei	Congo	Malaysia
Bahamas	Yemen	Senegal	El Salvador
Syria	Bulgaria	Costa Rica	Mali
Bahrain	Luxembourg	Singapore	Equatorial Guinea
Uzbekistan	Burkina Faso	Côte d'Ivoire	Marshall Islands
Bangladesh	Maldives	Somalia	Eritrea
Malawi	Burundi	Croatia	Mauritius
Barbados	Mauritania	Spain	Estonia
Mexico	Cabo Verde	Cuba	Micronesia

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1071** Application Layer Protocol	**T1021** Remote Services	**T1078** Valid Accounts
T1027 Obfuscated Files or Information	**T1036** Masquerading	**T1071.001** Web Protocols	**T1036.005** Match Legitimate Resource Name or Location	**T1573** Encrypted Channel
T1204 User Execution	**T1083** File and Directory Discovery	**T1573.002** Asymmetric Cryptography	**T1189** Drive-by Compromise	**T1583** Acquire Infrastructure
T1486 Data Encrypted for Impact	**T1543** Create or Modify System Process	**T1018** Remote System Discovery	**T1583.001** Domains	**T1021.001** Remote Desktop Protocol

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CMD Organization	CMD Organization is a ransomware operator running a double-extortion model, augmented by a novel public crypto-bidding platform that auctions stolen data alongside victim negotiations. The group demands ransoms of 7–8 BTC and deploys an MSVC++ ChaCha20+RSA locker via Group Policy, following IAB-sourced access, StealC credential harvesting, and 'Meow' backdoor persistence.	SEO Poisoning, Malvertising	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Credential compromise, Persistent access, Financial Loss	Windows
Ransomware			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
IOC TYPE	**VALUE**		
SHA1	07c14b82f673ba5caa8c1188f052ea31583f0af7		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
StealC	StealC is a commodity infostealer sold as malware-as-a-service since 2023 is used to harvest browser credentials, session cookies, and cryptocurrency wallet data, which were then handed off to operators in a pattern consistent with initial access brokers.	SEO Poisoning, Malvertising	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Credential exposure, Session hijacking and MFA bypass	Windows
Infostealer			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
IOC TYPE	**VALUE**		
URLs	hxxp[:]//213[.]165[.]47[.]49/b0c9ed38f2b14c119546[.]php, hxxp[:]//167[.]99[.]233[.]78/mbd		

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 CVEs
Meow	The 'Meow' backdoor established persistence via a DLL (observed as Netdrv.dll) that beaconed over HTTPS, using HKCU Run-key entries disguised as fake Microsoft Teams update installers with iterative version numbers.	SEO Poisoning, Malvertising	-
		IMPACT	AFFECTED PRODUCT
TYPE		Persistent, Covert C2 hidden in normal traffic	Windows
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA1	463554c76a0aa472daf9b42e9414942910b4ac54		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Interlock	INTERLOCK is a ransomware group known for its technical sophistication, using C/C++-compiled malware targeting both Windows and Linux systems. The group employs refined double-extortion tactics and runs a leak site called “Worldwide SecretsBlog” to publish stolen data and pressure victims into negotiations.	Social Enginerring	-
		IMPACT	AFFECTED PRODUCT
TYPE		Information Theft, Financial Loss	-
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	8940ee45d67adba9c01ef415cb3a71c219799ecba55557e64867b4d8b3a50c54, 6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f		

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
Medusa	Medusa ransomware employs a multi-extortion approach via its Medusa Blog, disclosing victim data and pressuring non-compliant organizations. Operating as a ransomware-as-a-service approach involves a multi-extortion strategy, offering victims options like time extensions, data deletion, or full data download, each with associated costs.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Information Theft, Financial Loss	-
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	3a6d5694eec724726efa3327a50fad3efdc623c08d647b51e51cd578bddda3da, 15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Anubis	Anubis is a destructive ransomware threat that, offers both file encryption and an optional wiper mode that renders data unrecoverable. Distributed via phishing, stolen credentials, and access brokers, it operates under a ransomware-as-a-service (RaaS) model.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Information Theft, Financial Loss	-
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc932ce385c8ed		

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
Rhadamanthys	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.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Information theft, Financial Loss	-
Infostealer			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4, aae017e7a36e016655c91bd01b4f3c46309bbe540733f82cce29392e72e9bd1f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AsyncRAT	AsyncRAT is an open-source Windows RAT, ranked 6th in global prevalence in 2024. Its capabilities include keylogging, screenshot capture, credential theft, and ransomware deployment.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Information theft, Financial Loss	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	48ee878fefc7d5d9df66fc978dfaafcfb61129acf92b1143e1b865ab292be9f0		

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
Lumma	Lumma Stealer is a potent info-stealing malware that evadesdetection by injecting itself intomemory, employing multiplelayers of encryption andobfuscation. The payload,cleverly disguised as a Base64-encoded DLL concealed within ablock of French text, isspecifically crafted to bypassmost antivirus defenses.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Information theft, Financial Loss	-
Infostealer			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	ca47c8710c4ffb4908a42bd986b14cddcca39e30bb0b11ed5ca16fe8922a468b, f0668ce925f36ff7f3359b0ea47e3fa243af13cd6ad9661dfccc9ff79fb4f1cc		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Qilin	Qilin is a prolific Ransomware-as-a-Service operation whose affiliates use double extortion encrypting victims' files and stealing sensitive data to threaten public release unless a ransom is paid. In a notable evolution, affiliates now run a Linux ransomware variant on Windows hosts by abusing legitimate remote-management tools like AnyDesk, ScreenConnect, and Splashtop evading Windows-focused defenses and improving stealth in mixed-OS environments.	Exploiting Vulnerability	CVE-2026-50751
		IMPACT	AFFECTED PRODUCT
TYPE		System Compromise, Encrypt Data	Check Point Mobile Access / SSL VPN, Remote Access VPN, Spark Firewall
Ransomware			PATCH LINK
ASSOCIATED ACTOR			https://support.checkpoint.com/results/sk/sk185033
-			
IOC TYPE	VALUE		
SHA256	43691290ac03ebb26754203f1cc3940b32f036babb7cfab3cb14fe2128389c0c, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6		

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">MLTBackdoor</td><td rowspan="6">MLTBackdoor is a sophisticated post-exploitation tool, likely used by a ransomware-linked actor to establish a foothold and enable lateral movement. It's delivered via a multi-stage ClickFix chain: a lure on an automotive-themed site tricks the victim into copying, pasting, and executing malicious content, which downloads a compressed archive from a DGA-generated domain, decrypts an RC4 payload, and sideloads the backdoor through a legitimate signed Microsoft Defender executable</td><td>ClickFix</td><td>-</td></tr>
<tr><td rowspan="2">TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td rowspan="3">Backdoor</td><td rowspan="3">Information theft, Stealthy execution</td><td>-</td></tr>
<tr><td rowspan="2">ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td rowspan="2">-</td><td rowspan="2">-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">d34e4038c5c80728f9648ba84833f69bc1ccea82e2e8e748b7b7f02fb687b92b,
9e52cc90cff150abe21f0a6440e86e0a99ff383b81061b96def8948e21d0ac66</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-2026-20245	✗	Cisco Catalyst SD-WAN 20.18.2.1 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Manager Authenticated Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-116	T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1059: Command & Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-20182	✗	Cisco Catalyst SD-WAN before 20.9.9.1, before 20.12.7.1, before 20.12.5.4, 20.12.6.2, before 20.15.5.2, before 20.15.4.4, before 20.18.2.2, before 26.1.1.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:catalyst_sd-wan_controller:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1059: Command & Scripting Interpreter, T1098: Account Manipulation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-20127	✗	Cisco Catalyst SD-WAN Controller & SD-WAN Manager Before 20.9.8.2, 20.12.5.3, 20.12.6.1, 20.15.4.2, 20.18.2.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:catalyst_sd-wan_controller:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Controller And Manager Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1059: Command & Scripting Interpreter, T1098: Account Manipulation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-50751	✗	Check Point Mobile Access / SSL VPN, Remote Access VPN, Spark Firewall (R80.20.X, R80.40, R81, R81.10, R81.10.X, R81.20, R82, R82.00.X, R82.10)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:checkpoint:remote_access_vpn:*:*:*:*:*:*:*:* cpe:2.3:a:checkpoint:security_gateway:*:*:*:*:*:*:*:*	Qilin Ransomware
Check Point Security Gateway Improper Authentication Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1583: Acquire Infrastructure, T1190: Exploit Public-Facing Application, T1133: External Remote Services	https://support.checkpoint.com/results/sk/sk185033

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-11645	✗	Google Chrome (Before 149.0.7827.103)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125, CWE-787	T1203: Exploitation for Client Execution, T1189: Drive-by Compromise	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-49160	✗	Windows 11 Version 23H2, 10 Version 22H2; Windows Server 2025, 2022, 2019, 2016	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
HTTP.sys Denial of Service Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-400	T1499: Endpoint Denial of Service	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-49160

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-45586	✗	Windows Server 2012 R2, 2019, 2016 (Server Core installation), 2025; Windows 10 Version 1607; Windows 11 Version 26H1 for ARM64-based Systems	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Collaborative Translation Framework (CTFMON) Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-59	T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-45586

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-50507	✗	Windows Server 2012, 2016, 2019, 2022, 2025; Windows 10 Version 1607; Windows 11 Version 26H1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows BitLocker Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1005: Data from Local System	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-50507

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-47291	✗	Windows Server 2012, 2016, 2025, 2022, 2019; Windows 10 Version 1607; Windows 11 Version 26H1; Windows 10 Version 22H2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
HTTP.sys Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122 CWE-190	T1190: Exploit Public-Facing Application, T1059: Command & Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-47291

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-49975	HTTP/2 Bomb	Apache HTTP Server (httpd) with mod_http2 and HTTP/2 enabled, prior to mod_http2 v2.0.41	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*	-
HTTP/2 Bomb (Apache HTTP Server Denial-Of-Service Vulnerability)	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-400	T1499: Endpoint Denial of Service	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=49ba7b515c4c0719b866d16f068e62d16a8a3dd1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-35273	✗	Oracle PeopleSoft Enterprise PeopleTools (versions 8.61, 8.62)	ShinyHunters (aka UNC6240)
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:*:*:*:*:*:*:*:*	-
Oracle PeopleSoft PeopleTools Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=bbb5d8746381c82f7e0fb6171094d375b492f266

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 TeamPCP (aka PCPcat, ShellForce, DeadCatx3, CipherForce, Persy_PCP, UNC6780)	-	Healthcare	United States
	MOTIVE		
	Espionage, Sabotage, Disruption, Financial Gains		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	-	-

TTPs
TA0001: Initial Access; T1190: Exploit Public-Facing Application; TA0003: Persistence, T1505: Server Software Component, T1505.003: Web Shell, T1543: Create or Modify System Process, T1543.003: Windows Service, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, TA0002: Execution, T1569: System Services, T1569.002: Service Execution, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, TA0005: Defense Evasion, T1574: Hijack Execution Flow, T1574.001: DLL, T1140: Deobfuscate/Decode Files or Information, T1562: Impair Defenses, T1027: Obfuscated Files or Information, T1055: Process Injection, T1014: Rootkit, T1036: Masquerading, T1036.005: Match Legitimate Resource Name or Location, TA0006: Credential Access, T1078: Valid Accounts, T1078.002: Domain Accounts, TA0008: Lateral Movement, T1021: Remote Services, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
ShinyHunters (aka UNC6240)</td><td>-
MOTIVE
Financial gain</td><td>All</td><td>Worldwide</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2026-35273</td><td>-</td><td>Oracle PeopleSoft Enterprise PeopleTools</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, T1059.004: Unix Shell, TA0005: Defense Evasion, T1036: Masquerading, T1036.005: Match Legitimate Name or Location Discovery, T1018: Remote System Discovery, T1083: File and Directory Discovery, TA0008: Lateral Movement, T1021: Remote Services, T1021.004: SSH, TA0011: Command and Control, T1219: Remote Access Software, T1071: Application Layer Protocol, T1071.001: Web Protocols, TA0009: Collection, T1560: Archive Collected Data, T1560.001: Archive via Utility, TA0010: Exfiltration, T1048: Exfiltration Over Alternative Protocol, TA0040: Impact, T1491: Defacement, T1491.001: Internal Defacement, T1657: Financial Theft</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a driver to force security teams to prioritize the **11 exploitable vulnerabilities** and block the indicators related to the threat actors **TeamPCP, ShinyHunters,** and malware **CMD Organization, StealC, Meow, Interlock, Medusa, Anubis, Rhadamanthys, AsyncRAT, Lumma, Qilin, MLTBackdoor.**

Uni5 Users

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

- Run a Scan to discover the assets impacted by the **11 exploitable vulnerabilities.**
- Test the efficacy of their security controls by simulating the attacks related to the threat actor **TeamPCP** and malware **Interlock, Medusa, Anubis, Rhadamanthys, AsyncRAT, Lumma Stealer, Qilin Ransomware, and MLTBackdoor** in Breach and Attack Simulation(BAS).

Threat Advisories

New CMD Organization Ransomware Hits U.S. Healthcare with Auction Extortion

Cisco Catalyst SD-WAN Manager Zero-Day Actively Exploited in the Wild

Code Blue: U.S. Healthcare Under Cyber Siege

From Zero-Day to Ransomware: Check Point VPN Bug Fuels Real-World Attacks

Google Rushes Patch for In-the-Wild Chrome V8 Zero-Day (CVE-2026-11645)

Microsoft's June 2026 Patch Tuesday

MLTBackdoor: ClickFix to Ransomware Foothold

HTTP/2 Bomb CVE-2026-49975: A Flaw Detonates Apache HTTP Server

Oracle PeopleSoft Under Siege: Zero-Day CVE-2026-35273 Fuels ShinyHunters Intrusions

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
Meow	SHA1	463554c76a0aa472daf9b42e9414942910b4ac54
	IPv4	188[.]190[.]2[.]165[:]666
CMD Organization	SHA1	07c14b82f673ba5caa8c1188f052ea31583f0af7
	Email	Cmd2official[@]onionmail[.]org, Cmdhtmnjksgkuhilrtrh[@]onionmail[.]org, MitsueWhite[@]onionmail[.]org, JedAdams[@]onionmail[.]org
	Domain	cmdofficial[.]com
	Onion address	cmdnkiqjije2tllr3biee2sjgj3i4robg2cbtilbnytdhh2wy3syrlyd[.]onion
StealC	IPv4	213[.]165[.]47[.]49, 167[.]99[.]233[.]78
	URLs	hxxp[:]//213[.]165[.]47[.]49/b0c9ed38f2b14c119546[.]php, hxxp[:]//167[.]99[.]233[.]78/mbd
Rhadamanthys	SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9, 5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8,

Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	6f92b2cdb8b5f68d20dbc7ca23c3a3ec78c4ef1859001940dfa22e38ce459d30, 6d240a48b5e2d1cf761a8b48b146d20729d0a7a3a557e31e75ed4c120ce71aea, c7d4e119149a7150b7101a4bd9fffbf659fba76d058f7bf6cc73c99fb36e8221, 2657fe9b88321d255fc56a81b2df4b0109ab7c525442f31765c94d75c37347aa, 124c02ed924e11b06b74e1b8c1290adbb1e50dfa2a7bcf95104c6425a1f82ef5, 3c4df2d02e4b6f4acf7b19238211892db501ee6faa04065dd11b25b56483f9c4, 9a7bc24bd814ab755a8ad67e1aeebc05ff139771928f0eae883daff6f4ae161d, 65d6130ed7d3d822e1b08e7bed8e3adca4188d787d6805935213369c05eb2a99, b9ad234abeb1490f2c2d28dd2387f0575ba5128ebb799741b1f3179622204175, 7faeb3f847830a2c52322565d8e73e07000003ccb54310790e10756cd3b2ff6b, c7ca2f9065557a6d8fb0c02c75804d386b77ffca4466678b201c09e916afa096, a432bf6943599e53a12d5615f91fe3d636a6820073b60a7068fa9508849806b4, 30b5b1d6877df251f4007725df4e043f704d80a55b4ebd7c952b4f24b7806712, 8404cb4a740d169256e49e3a22b2af1a61b2606e71cdca4f39deeccd5d461c91, 138c86d9c22182dc809f2747d012d792ed391a84081e513c7c93d8786801d5f7, b579df3a8607cb6b251ee319bdc8c1005ca3a6ed1e360eedf2433b3f6151d856, 1d8e82d9abda58c9f4a0def2940e9f75921e2dce89a07b337a075ca363176cd4, 4130ce135fbfab00618f261a0397e88479d2f61e1ed0d09ebcde525439774f3e, cc830ff08b6c66fb562a8e90c9512cadd6dbe715eb31d09e7d6afcc0e9fbee68, 70debce3a545cacca8b0bdb6008945852084b36e9160424fb63479c2991dcade, a4b6a1619cf4ff65770be120cc415de1e8897c2378610171f3c48ff0fa38e9fe, 00dd5c97e86646df73973ba24085ebb32db19de258f37ed50b5c333087bb6b5c,

Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	df65e93cddf79b31b474f39477aa3038cb6669653116760 96d9e02a5b5cf7523, 233a2666a23ab1bae19296ee7f66ce3cdf6284db1ca4caaeb121530126419b42, d5b6cfe15a5bf959152889d8ff4fc220f0c055327c57a83c4877316af50d3a4d, f62527a0f56252621a8c7c18e0f5131bb53b4a5312dba42b4188b52345cc94a2, f9d387135a7a4e49eb96fc29d3da8f412d870417bf684b5e8ae91c4a1fbcc6d5, df66fe18ba387caa8cb295c5f35bb0a8d208ddadea7a05cef77090cc09a681b1, bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33, 6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2, 50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2, 01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d, a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63, ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b, f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb, ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16, fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e, a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476, 3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0, ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62, 5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9,

Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7, f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4, aae017e7a36e016655c91bd01b4f3c46309bbe540733f82cce29392e72e9bd1f
AsyncRAT	SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afcff20ef524, 7bb7c893fdf7f7ccd998610969d23993c50fc0b693e67930b6f98d8dbd003ee3, ececf197bee885791a9b13cd48c131eec76d8431f1907f9d55b6c9330b57a85e, 346e8e54578f206200f7815d0e315e6bfb58198b5ff96d8bcec02863e5b42cc7, 0c0b5dfb2e01c5ddd043ac32e2f7176b4ba439d4e3ea37ca04e4b17aa283d4e7, 4c6c9ec88d00a3b77e6288afc4ee9974ac07a2c73012c3e1a017c457dcf22d87, 48ee878fefc7d5d9df66fc978dfaafcfb61129acf92b1143e1b865ab292be9f0
Lumma Stealer	SHA256	515ad6ad76128a8ba0f005758b6b15f2088a558c7aa761c01b312862e9c1196b, dfce2d4d06de6452998b3c5b2dc33eaa6db2bd37810d04e3d02dc931887cfddd, 01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f, 65e1a8e550df1000eb91a7b679cf586efab0f24385b810f50349d50eb80ae806, 5ecafa1ecbc54d9a7b0e2e5c646578057215a246aeec2132fe7605a078aa43ec, d0e7a341fe199dbabb5f0798dba0564e9b60e4736a405c46eafc7232cc10dc40, 8a80210b1f6382cdbff2afc0c9a30092fc13687a33f293e36a9dbc0263a45101, a90294b602b51fff7b04e72deeb3e88fb200272321c939f00e13bde1d49ff1a3, 257bcb2bac99fe5e876857ec4511cada759e7f515de629e43cbb0f839575e7fc, 8bfdd127054e1ee93f58148677961929bb9265bb6ba9648f517118c1dfca6504, 78785ab759dd61f4a9fb561faef90234fb0a78696523d1df53312c7a3eff99fe, a4ea760306249b07d5af054b5fc82d5fd9dcab5e5cb6eab3c8e8eb9132ebf882,

Attack Name	TYPE	VALUE
Lumma Stealer	SHA256	3d1d2e2b702d493ddaad5d7deb780ee227eb24438e68b499839a4722e212f8fb, 1be53a1bc4d191e139afb7c053b8f54af43c0338ff1eee40cd1486dfe5b787b1, d0130399fd404226ae5b90897e8e3affe29b7d34081ee1bf11ecb3750ca342c5, d932ee10f02ea5bb60ed867d9687a906f1b8472f01fc5543b06f9ab22059b264, e4d5b043f5c9e0894a5f4a21c93cd7347a609a900da8f56f55a0dd84269e81f1, ce00c5433fb2481534577e90b23e61b164654ad41c5a0f14ba59735ed637e326, 4dc5588ac49fa183824ab585b69a491fd45d1d3b2b01f052adc5062b356e7434, 984a58b77a8657d009b7867d392f320f65bb8cb72b63d9960a90f5a94721f8fb, 43d0cfce7ab2b0c2f6f89f0fa93083f46f290047cef0f75a0ae3a0b8742d84d8, de6c4c3ddb3a3ddbcbea9124f93429bf987dcd8192e0f1b4a826505429b74560, 77460056386f07d96908455241b15091c3edecd9fd55fbf6ce7f3a061c7ac5cd, 3f86ca59335214a918870d86a47b21cc77f941dfcb32b7ba97620021621e7444, e63d29cda8af6ad95286c11996f0ac32a70ac24c1c2baa78d22593babd826a41, 82cb239612d74eab70b12a0ca448bd82b3c5b418b8f05213d75ddddbbf0b4a5d, ca47c8710c4ffb4908a42bd986b14cddcca39e30bb0b11ed5ca16fe8922a468b, f0668ce925f36ff7f3359b0ea47e3fa243af13cd6ad9661dfccc9ff79fb4f1cc
Interlock	SHA256	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f, 4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9, 33dc991e61ba714812aa536821b073e4274951a1e4a9bc68f71a802d034f4fb9, b85586f95412bc69f3dceb0539f27c79c74e318b249554f0eace45f3f073c039, a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642, 0fff8fb05cee8dc4a4f7a8f23fa2d67571f360a3025b6d515f9ef37dfdb4e2ea, e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1,

Attack Name	TYPE	VALUE
Interlock	SHA256	f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e, a68074efeee105c46bd5d86143d183c61bcf1732265f78d9f684fa82715423d3, 2f8a9258c9a5d1dfc93ea99c9990ab728595400a51aa4128f2f7254a98e03fdb, 8940ee45d67adba9c01ef415cb3a71c219799ecba55557e64867b4d8b3a50c54, 6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f
Medusa	SHA256	4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6, 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980, 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95, 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669, 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270, d1e1eb0e0aaedb01df8cc2b98b0119c4aef8c1c2a3930ea0c455f0491e3161eb, c08591a1363993e2fb1fceb28168033fe66c6027531cc051c00fd82e0eb32fc8, fbf6c8f0857d888385f6bc0d46523ebcc1634e06d0e96411fc43a8ae4213d1f3, e871d8936d3b3a98d2b8dc607eadf784e1b3a20c798f3ff217d80257a67917e3, 1d009f5217c2de63ec09f5d459085a2175d5b5d2460da42257cfc52cc323f501, 5ff8acd652cc134b84213865aa3f74667c09a331cfa9affd2a2668ce78751516, 7eb39ff9ed4007b4d42dc769c8f0d8199bd8153372a07a175d884a41990839a7, 6d000a159fe10af1b29ddf4e4015931a9e9d0a020aeef0c602d8c5419b5966e6, 1bad2b6e8ab16c5a692b2d05f68f7924a73a5818ddf3a9678ca8caab3568a78e, c9abfc3e4da474e18795f5261f77e60c44e7b3353771281e4304e7506d56fdb4, 3a6d5694eec724726efa3327a50fad3efdc623c08d647b51e51cd578bddda3da, 15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10

Attack Name	TYPE	VALUE
Anubis	SHA256	98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc932ce385c8ed
Qilin	SHA256	516927b55038c1702bc8a6a0262a39d5fe45f4b07527fdc42415533a9665264a, 43691290ac03ebb26754203f1cc3940b32f036babb7cfab3cb14fe2128389c0c, 37546b811e369547c8bd631fa4399730d3bdaff635e744d836332b74f44f56cf6
MLTBackdoor	Domains	carrolc[.]com, cwrtwright[.]com, thomphon[.]com
	SHA256	d34e4038c5c80728f9648ba84833f69bc1ccea82e2e8e748b7b7f02fb687b92b, 9e52cc90cff150abe21f0a6440e86e0a99ff383b81061b96def8948e21d0ac66

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 15, 2026 • 11:00 PM

More at www.hivepro.com