

Date of Publication
July 01, 2026



HiveForce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

JUNE 2026

Table Of Contents

[Summary](#)..... 03

[Insights](#)..... 04

[Threat Distribution](#)..... 05

[Celebrity Vulnerabilities](#)..... 06

[Vulnerabilities Summary](#)..... 09

[Attacks Summary](#)..... 15

[Adversaries Summary](#)..... 19

[Targeted Products](#)..... 21

[Targeted Countries](#)..... 25

[Targeted Industries](#)..... 26

[Top MITRE ATT&CK TTPs](#)..... 27

[Top Indicators of Compromise \(IOCs\)](#)..... 28

[Vulnerabilities Exploited](#)..... 31

[Attacks Executed](#)..... 55

[Adversaries in Action](#)..... 85

[MITRE ATT&CK TTPs](#)..... 95

[Top 5 Takeaways](#)..... 105

[Recommendations](#)..... 106

[Appendix](#)..... 107

[Indicators of Compromise \(IoCs\)](#)..... 108

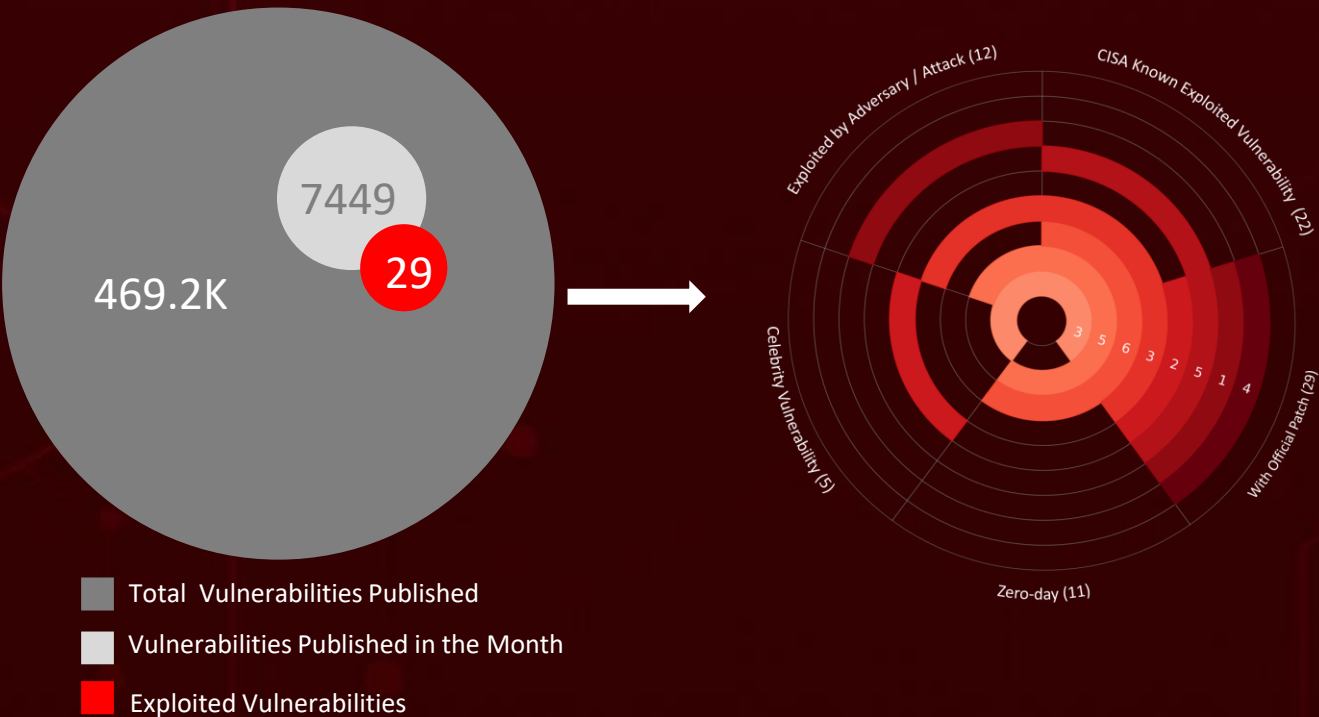
[What Next?](#)..... 120

Summary

June proved just how fast attackers can outpace patches, with **eleven zero-days** actively exploited across the month. Cisco disclosed **CVE-2026-20245**, an unpatched flaw in Catalyst SD-WAN Manager's CLI that lets an authenticated netadmin-level attacker upload a crafted file, trigger command injection, and seize root on the management plane. Check Point wasn't spared either: **CVE-2026-50751** let attackers bypass authentication on its Remote Access VPN and Mobile Access products entirely, with at least one intrusion traced back to a **Qilin** ransomware affiliate. Oracle PeopleSoft users faced their own reckoning as **ShinyHunters** exploited **CVE-2026-35273** before a patch existed, using it to infiltrate networks, harvest data, and move laterally with ease.

Espionage activity kept pace with the exploitation surge. **UNC6508**, a PRC-nexus actor, compromised externally facing REDCap research servers and deployed custom malware, **INFINITERED**, purpose-built to harvest legitimate credentials. Social engineering also had a strong month: attackers spread obfuscated VBScript files through compromised WhatsApp accounts disguised as financial documents, while the **Edgecution** campaign impersonated IT support over Microsoft Teams to lure victims into installing a malicious browser extension backed by a Python-based host.

ClickFix campaigns rounded out the month by tricking users into pasting malicious commands directly into Windows, each variant delivering a different loader. One, Lorem Ipsum Loader, tied to the **Rapid Brigantine** group, installed a backdoor chain leading through Oyster, Supper, and MeowBackConn before culminating in Rhysida ransomware. Taken together, June is a clear reminder that patching alone isn't enough; layered defenses and faster detection are now table stakes.



In **June 2026**, a geopolitical cybersecurity landscape unfolds, revealing the **United States, Singapore, Vietnam, Canada, and Brazil** as the top-targeted countries

Highlighted in **June 2026** is a cyber battleground encompassing the **Financial, Education, Government, Technology, and Healthcare** sectors, designating them as the top industries

No credentials, no problem: **CVE-2026-50751** lets attackers walk past Check Point's VPN, and **Qilin's** already walked in

ShinyHunters didn't wait for a patch; **CVE-2026-35273** gave them unauthenticated, remote control of Oracle PeopleSoft first

Sinobi doesn't knock; it walks in through stolen SonicWall VPN creds, blinds your EDR, and gives you 7 days before your data goes on sale

One bad memory access, zero days to exploit: Chrome's **CVE-2026-11645** is already being weaponized

233 million records, one sector on the front line: healthcare's brutal year as critical infrastructure's biggest target

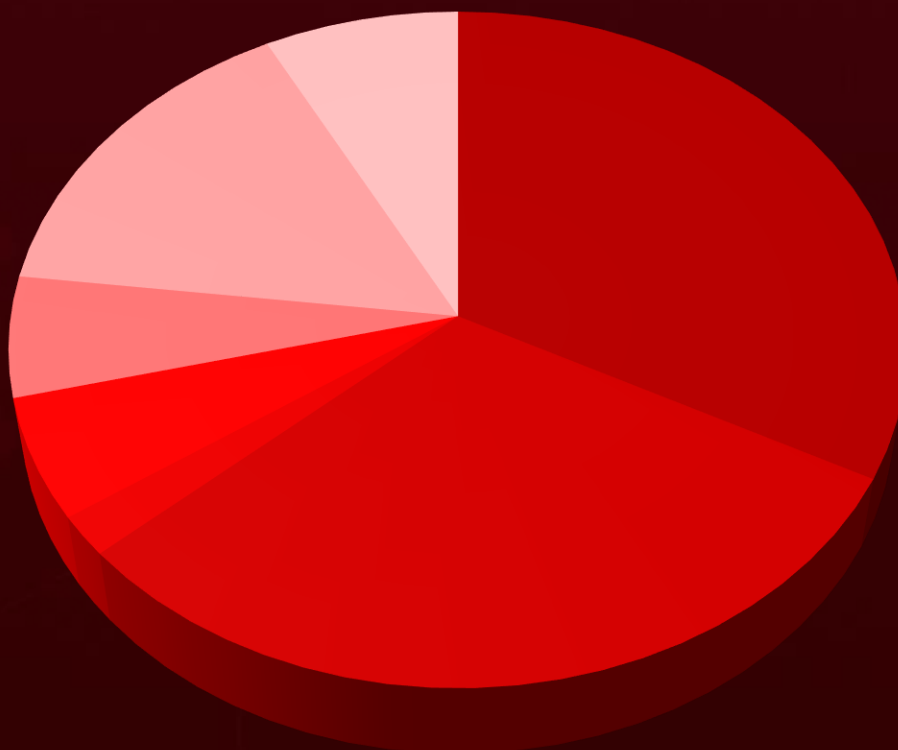
Behind **ClickFix's** curtain: **Potemkin** builds the illusion, **BabaDeda** hides the payload, **Lorem** Ipsum fills the blanks

Surfaced in April, run by one name, **Prinz Eugen** proves ransomware doesn't need a crew, just **ROOTBOY** and Go code

UNC6508 didn't hack REDCap's research; it hacked REDCap's front door, planting **INFINITERED** to quietly harvest the keys



Threat Distribution



- Malware Attacks
- Social Engineering
- Supply Chain Attacks
- Man-in-the-Middle Attack
- Denial-of-Service Attack
- Injection Attacks
- Password Attack

Celebrity Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2021-34473</u>	PROXYSHELL	Microsoft Exchange Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	GodPotato Chisel
Microsoft Exchange Server Remote Code Execution Vulnerability		ASSOCIATED TTPs	PATCH LINK
	CWE ID		
	CWE-918	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2021-34523</u>	PROXYSHELL	Microsoft Exchange Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	GodPotato Chisel
Microsoft Exchange Server Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34523

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2021-31207</u>	PROXYSHELL	Microsoft Exchange Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	GodPotato Chisel
Microsoft Exchange Server Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1190: Exploit Public- Facing Application; T1556: Modify Authentication Process	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-49975</u>	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 KEY	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
<u>CVE-2026-47729</u>	Squidbleed	Squid Web Proxy (all versions in default configuration prior to the upstream fix)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:squid-cache:squid:*:*:*:*:*:*	-
Squid Proxy Memory Leak Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1212: Exploitation for Credential Access, T1528: Steal Application Access Token, T1588: Obtain Capabilities, T1588.006: Vulnerabilities	https://github.com/squid-cache/squid/releases

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-42897	Microsoft Exchange Server Cross-Site Scripting Vulnerability	Microsoft Exchange Server			
CVE-2026-0257	Palo Alto Networks PAN-OS Authentication Bypass Vulnerability	Palo Alto Networks PAN OS			
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server			
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server			
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	Microsoft Exchange Server			
CVE-2025-32372	DotNetNuke Server-Side Request Forgery Vulnerability	DotNetNuke.Core			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2024-55591	Fortinet FortiOS Authorization Bypass Vulnerability	FortiOS			
CVE-2024-21762	Fortinet FortiOS SSL- VPN Out-of Bounds Write Vulnerability	FortiOS			
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication Cloud Connect			
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver Visual Composer			
CVE-2026-20230	Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability	Cisco Unified Communications Manager (Unified CM) and Unified CM SME			
CVE-2026-20245	Cisco Catalyst SD-WAN Manager Authenticated Privilege Escalation Vulnerability	Cisco Catalyst SD WAN			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-20182	Cisco Catalyst SD WAN Controller Authentication Bypass Vulnerability	Cisco Catalyst SD-WAN			
CVE-2026-20127	Cisco Catalyst SD WAN Controller And Manager Authentication Bypass Vulnerability	Cisco Catalyst SD-WAN Controller & SD-WAN Manager			
CVE-2026-50751	Check Point Security Gateway Improper Authentication Vulnerability	Check Point Mobile Access / SSL VPN, Remote Access VPN, Spark Firewall			
CVE-2026-11645	Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	Google Chrome			
CVE-2026-49160	HTTP.sys Denial of Service Vulnerability	Windows, Windows Server			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-45586	Windows Collaborative Translation Framework (CTFMON) Elevation of Privilege Vulnerability	Windows, Windows Server			
CVE-2026-50507	Windows BitLocker Security Feature Bypass Vulnerability	Windows, Windows Server			
CVE-2026-47291	HTTP.sys Remote Code Execution Vulnerability	Windows, Windows Server			
CVE-2026-49975	HTTP/2 Bomb (Apache HTTP Server Denial-Of Service Vulnerability)	Apache HTTP Server (httpd) with mod_http2 and HTTP/2 enabled			
CVE-2026-35273	Oracle PeopleSoft PeopleTools Remote Code Execution Vulnerability	Oracle PeopleSoft Enterprise PeopleTools			
CVE-2026-10520	Ivanti Sentry OS Command Injection Vulnerability	Ivanti Sentry (Before R10.5.2 / R10.6.2 / R10.7.1)			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-20262	Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability	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)			
CVE-2024-53704	SonicWall SonicOS SSLVPN Authentication Bypass Vulnerability	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			
CVE-2024-40766	SonicWall SonicOS Improper Access Control Vulnerability	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			
CVE-2026-54420	LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability	LiteSpeed cPanel Plugin (user-end) (Before 2.4.8), as distributed in LiteSpeed WHM Plugin (Before 5.3.2.0)			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2026-47729	Squid Proxy Memory Leak Vulnerability	Squid Web Proxy (all versions in default configuration prior to the upstream fix)			
CVE-2026-12569	PTC Windchill and FlexPLM Improper Input Validation Vulnerability	PTC Windchill PDMLink and FlexPLM - all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030			



Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
XenoRAT	RAT	-	Windows	-	Phishing
GodPotato	Tool	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2025-32372	Microsoft Exchange Server, DotNetNuke (DNN)		Exploiting Vulnerabilities
Chisel	Tool	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2025-32372	Microsoft Exchange Server, DotNetNuke (DNN)		Exploiting Vulnerabilities
AZUREVEIL	Adaptix C2 Agent	-	Windows	-	Phishing
RUSTCLOAK	Loader	-	Windows	-	Phishing
PhantomRelay	RAT	-	Microsoft Windows, Android	-	Social Engineering
FallSpy	Android spyware	-	Microsoft Windows, Android	-	Social Engineering
LegionRelay	RAT	-	Microsoft Windows, Android	-	Social Engineering
LOOKVALPS	Loader	-	Microsoft Windows, Android	-	Social Engineering
LOOKVALJS	Loader	-	Microsoft Windows, Android	-	Social Engineering

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
DAYLIGHT	Loader	-	Microsoft Windows, Android	-	Social Engineering
TEASOUP	Loader	-	Microsoft Windows, Android	-	Social Engineering
Qilin	Ransomwar e	CVE-2024-55591 CVE-2024-21762 CVE-2023-27532 CVE-2025-31324 CVE-2026-50751	Fortinet FortiOS, Veeam Backup & Replication Cloud Connect, SAP NetWeaver Visual Composer, Check Point Mobile Access / SSL VPN, Remote Access VPN, Spark Firewall		Exploiting Vulnerabilities
CMD Organization	Ransomwar e	-	Windows	-	SEO Poisoning, Malvertising
StealC	Infostealer	-	Windows	-	SEO Poisoning, Malvertising
Meow	Backdoor	-	Windows	-	SEO Poisoning, Malvertising
Interlock	Ransomwar e	-	-	-	Social Engineering
Medusa	Ransomwar e	-	-	-	Social Engineering
Anubis	Ransomwar e	-	-	-	Social Engineering
Rhadamanth ys	Infostealer	-	-	-	Social Engineering
AsyncRAT	RAT	-	-	-	Social Engineering

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Lumma	Infostealer	-	Windows	-	Social Engineering, Loader chains, cracked software
MLTBackdoor	Backdoor	-	-	-	ClickFix
SPECTRALVIPER	Backdoor	-	Windows	-	DLL Side Loading
Sinobi Ransomware	Ransomware	CVE-2024-53704 CVE-2024-40766	Windows		Compromised SonicWall SSL VPN credentials
INFINITERED	Backdoor	-	REDCap servers; Google Workspace	-	Post compromise, via web shell
DarkKomet	Backdoor	-	Windows	-	Steam Workshop, Wallpaper Engine
Vidar	Infostealer	-	Windows	-	Loaders, cracked game installers
RenEngine	Loader	-	Windows	-	Steam Workshop, Wallpaper Engine
Potemkin	Loader	-	Windows	-	ClickFix
RMMProject	RAT	-	Windows	-	ClickFix
EtherRAT	RAT	-	Windows	-	ClickFix

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
BabaDeda Loader	Loader	-	Windows	-	ClickFix
Lorem Ipsum Loader	Loader	-	Windows	-	ClickFix
Edgecution	Web Browser Extension	-	Microsoft Edge, Microsoft Teams, Microsoft Outlook	-	Social Engineering
Gaslight	Infostealer	-	macOS	-	-
TinyRCT	Backdoor	-	Windows	-	Web shells
Prinz Eugen	Ransomware	-	Windows	-	RDP credentials

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
SideCopy	Information theft and espionage	Pakistan	-	XenoRAT	Windows
GREYVIBE	Information theft and espionage	Russia	-	PhantomRelay (variants: PhantomRelayLite, PhantomRelayV1, PhantomRelayV2), FallSpy, LegionRelay, LOOKVALPS, LOOKVALJS, DAYLIGHT, TEASOUP	Web browsers (Chromium based), Telegram Desktop, WhatsApp Desktop, Remote Desktop Protocol (RDP) targeted during post compromise activity
TeamPCP	Espionage, Sabotage, Disruption, Financial Gains	-	-	-	-
ShinyHunters	Financial gain	-	CVE-2026-35273	-	Oracle PeopleSoft Enterprise PeopleTools
OceanLotus	Espionage and Information Theft	Vietnam	-	SPECTRAL VIPER	FireAnt Metakit; Microsoft SQL Server

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
UNC6508	Espionage and Information Theft	China (PRC-nexus)	-	INFINITER ED	REDCap (Research Electronic Data Capture); Google Workspace content compliance rules
Insomnia	Financial Gain	-	-	-	-
Rapid Brigantine	Financial Gain	-	-	Lorem Ipsum Loader, Oyster, Supper, MeowBackConn, Rhysida Ransomware	Google Chrome, Mozilla Firefox, Microsoft Edge, Microsoft Defender, WordPress
CL-STA-1062	Espionage and Information Theft	China	-	TinyRCT	Windows
ROOTBOY	Financial Gain	-	-	Prinz Eugen	Windows



Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Network Security	Palo Alto Networks PAN OS 10.2 (Before 10.2.7 h34 / 10.2.10-h36 / 10.2.13-h21 / 10.2.16-h7 / 10.2.18-h6), PAN-OS 11.1 (Before 11.1.4-h33 / 11.1.6-h32 / 11.1.7-h6 / 11.1.10-h25 / 11.1.13-h5 / 11.1.15), PAN-OS 11.2 (Before 11.2.4-h17 / 11.2.7-h14 / 11.2.10-h7 / 11.2.12), PAN-OS 12.1 (Before 12.1.4-h6 / 12.1.7), Prisma Access 10.2 (Before 10.2.10-h36), Prisma Access 11.2 (Before 11.2.7-h13)
 Microsoft	Software (OS, Cloud, Productivity)	Microsoft Exchange Server
	Content Management System (CMS)	DotNetNuke.Core Version Prior to 9.13.8
	Network Security	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; Fortinet FortiOS versions: 7.4.0 through 7.4.2 7.2.0 through 7.2.6 7.0.0 through 7.0.13 6.4.0 through 6.4.14 6.2.0 through 6.2.15 6.0 all versions
	Backup & Data Recovery Software	Veeam Backup & Replication Cloud Connect
	Enterprise Resource Planning (ERP)	SAP NetWeaver Visual Composer

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Networking Hardware / Security	Cisco Unified Communications Manager (Unified CM) and Unified CM SME, release 14 (before 14SU6) and release 15 (before 15SU5 / COP1), with WebDialer enabled
		Cisco Catalyst SD WAN 20.18.2.1 and earlier
		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
		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
		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)
	Network Security	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)
	Web Browser	Google Chrome (Before 149.0.7827.103)
	Web Server	Windows 11 Version 23H2, 10 Version 22H2; Windows Server 2025, 2022, 2019, 2016

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Operating System	Windows Server 2012 R2, 2019, 2016 (Server Core installation), 2025; Windows 10 Version 1607; Windows 11 Version 26H1 for ARM64 based Systems
		Windows Server 2012, 2016, 2019, 2022, 2025; Windows 10 Version 1607; Windows 11 Version 26H1
		Windows Server 2012, 2016, 2025, 2022, 2019; Windows 10 Version 1607; Windows 11 Version 26H1; Windows 10 Version 22H2
	Web Server	Apache HTTP Server (httpd) with mod_http2 and HTTP/2 enabled, prior to mod_http2 v2.0.41
	Database / Enterprise Software	Oracle PeopleSoft Enterprise PeopleTools (versions 8.61, 8.62)
	IT Asset & Endpoint Management / Security	Ivanti Sentry (Before R10.5.2 / R10.6.2 / R10.7.1)
	Network Security	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
		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
	Web Server	LiteSpeed cPanel Plugin (user-end) (Before 2.4.8), as distributed in LiteSpeed WHM Plugin (Before 5.3.2.0)

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Caching Proxy Server	Squid Web Proxy (all versions in default configuration prior to the upstream fix)
	Product Data Management (PDM) / PLM software	PTC Windchill PDMLink and FlexPLM - all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030

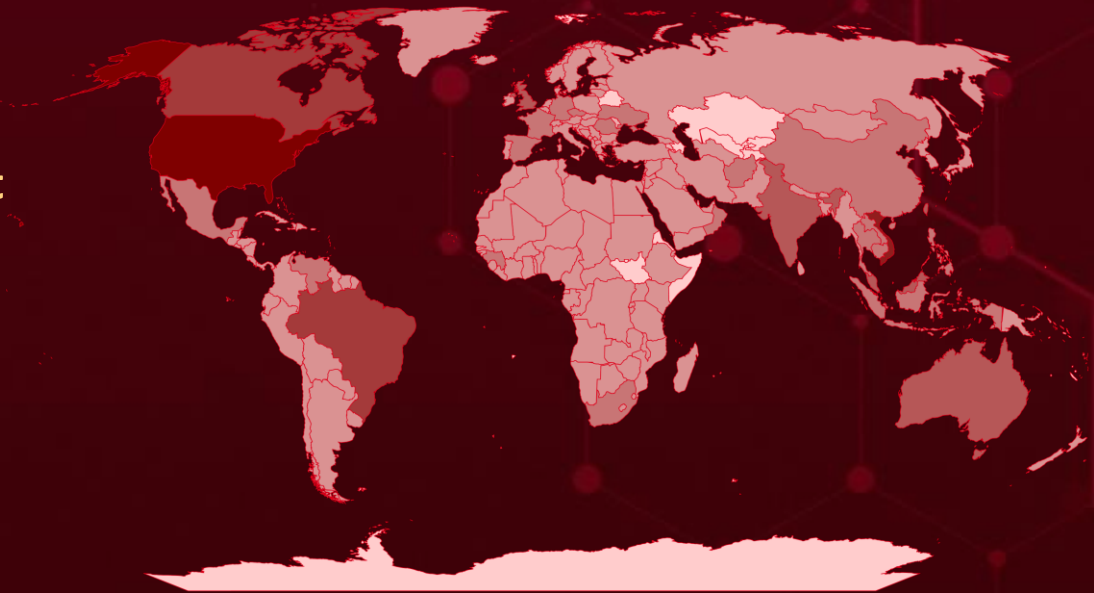


Targeted Countries

Most



Least



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
	United States		Thailand		Cayman Islands		Curacao		Equatorial Guinea
	Singapore		Mexico		Saint Maarten		Sweden		Peru
	Vietnam		Ukraine		Central African Republic		Cyprus		Estonia
	Canada		Oman		Sri Lanka		Togo		Puerto Rico
	Brazil		Germany		Chad		Anguilla		Ethiopia
	United Kingdom		Philippines		Tunisia		Uganda		Russia
	Taiwan		Romania		Chile		Democratic Republic of Congo		Faroe Islands
	Australia		Laos		Burundi		Bulgaria		Saint Kitts and Nevis
	India		Afghanistan		Angola		Denmark		Fiji
	Malaysia		Republic of Ireland		Mozambique		Barbados		Samoa
	Timor-Leste		Mongolia		Colombia		Djibouti		Finland
	South Africa		Tanzania		Nicaragua		Montserrat		Senegal
	Guinea		American Samoa		Comoros		Dominica		Antigua and Barbuda
	Hong Kong		North Macedonia		Belgium		Dominican Republic		Bermuda
	Czech Republic		Cameroon		Congo-Brazzaville		Netherlands		French Guiana
	Cambodia		Seychelles		Poland		Ecuador		South Korea
	France		Andorra		Costa Rica		Nigeria		Gabon
	Indonesia		Algeria		Saba		Egypt		Suriname
	China		Canada Quebec		Croatia		Northern Ireland		Georgia
	Venezuela				Saudi Arabia		El Salvador		Syria
	Spain								Argentina
	Brunei								Tibet

Targeted Industries

Most



Financial



Education



Government



Technology



Healthcare



Energy



Legal



Defence



Construction



Manufacturing



Consumers



Hospitality



Professional Services



Non-Profit



Media



Agriculture



Research Organizations



Food products



Transportation



Insurance



Real Estate



Aerospace



Gaming



Religious



Automotive



Retail



NGOs



BPO



IT Services



Pharmaceutical



Aviation



FinTech



Banking



Electrical



Industrials & Engineering



Raw Material



Chemical



Jewelry



High-Tech



Cryptocurrency



Travel



Think-Tanks



FMCG



Oil & Gas



Engineering



Online



Biomedical



Political Entities



Entertainment



E-commerce



Maritime



Logistics



Sports



Extractive



Telecommunications



Fashion



Utilities

Least

TOP 25 MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1190

Exploit Public-Facing Application

T1071

Application Layer Protocol

T1027

Obfuscated Files or Information

T1071.001

1
Web Protocols

T1036

Masquerading

T1204

User Execution

T1021

Remote Services

T1078

Valid Accounts

T1573

Encrypted Channel

T1041

Exfiltration Over C2 Channel

T1036.005

Match Legitimate Name or Location

T1082

System Information Discovery

T1083

File and Directory Discovery

T1059.001

PowerShell

T1588

Obtain Capabilities

T1090

Proxy

T1105

Ingress Tool Transfer

T1005

Data from Local System

T1583

Acquire Infrastructure

T1218

System Binary Proxy Execution

T1140

Deobfuscate/Dencode Files or Information

T1588.006

Vulnerabilities

T1059.003

Windows Command Shell

T1204.002

Malicious File



Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>GodPotato</u>	Filename	gp_v6_exec.py
<u>Chisel</u>	Filename	/opt/c2/payloads/
<u>Qilin</u>	Tor Leak Site	ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]]onion
	SHA256	d82069cfc9395a240b9c140d283367ab470d587326c5e256aba78eb2c5a9ea85, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6, 516927b55038c1702bc8a6a0262a39d5fe45f4b07527fdc42415533a9665264a, 43691290ac03ebb26754203f1cc3940b32f036babb7cfab3cb14fe2128389c0c, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6
	Ransom Note Filename	README-RECOVER-[rand].txt, README-RECOVER-[rand]_2.txt, [Unique ID]-RECOVER-README.txt
<u>Interlock</u>	SHA256	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f, 4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9, 33dc991e61ba714812aa536821b073e4274951a1e4a9bc68f71a802d034f4fb9, b85586f95412bc69f3dceb0539f27c79c74e318b249554f0eace45f3f073c039, a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642, 0fff8fb05cee8dc4a4f7a8f23fa2d67571f360a3025b6d515f9ef37dfdb4e2ea, e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1, f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e, a68074efeee105c46bd5d86143d183c61bcf1732265f78d9f684fa82715423d3, 2f8a9258c9a5d1dfc93ea99c9990ab728595400a51aa4128f2f7254a98e03fdb, 8940ee45d67adba9c01ef415cb3a71c219799ecba55557e64867b4d8b3a50c54, 6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f

Attack Name	TYPE	VALUE
<u>Medusa</u>	SHA256	4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb32467505 4ea023b12ab6, 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba 9c66d59677980, 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38 cf2810eeb9cb95, 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2 024a8a3115669, 736de79e0a2d08156bae608b2a3e63336829d59d38d6190764 2149a566ebd270, d1e1eb0e0aaedb01df8cc2b98b0119c4aef8c1c2a3930ea0c45 5f0491e3161eb, c08591a1363993e2fb1fceb28168033fe66c6027531cc051c00f d82e0eb32fc8, fbf6c8f0857d888385f6bc0d46523ebcc1634e06d0e96411fc43 a8ae4213d1f3, e871d8936d3b3a98d2b8dc607eadf784e1b3a20c798f3ff217d 80257a67917e3, 1d009f5217c2de63ec09f5d459085a2175d5b5d2460da42257c fc52cc323f501, 5ff8acd652cc134b84213865aa3f74667c09a331cfa9affd2a266 8ce78751516, 7eb39ff9ed4007b4d42dc769c8f0d8199bd8153372a07a175d8 84a41990839a7, 6d000a159fe10af1b29ddf4e4015931a9e9d0a020aeeef0c602d8 c5419b5966e6, 1bad2b6e8ab16c5a692b2d05f68f7924a73a5818ddf3a9678ca 8caab3568a78e, c9abfc3e4da474e18795f5261f77e60c44e7b3353771281e430 4e7506d56fdb4, 3a6d5694eec724726efa3327a50fad3efdc623c08d647b51e51c d578bddda3da, 15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8 f02c53fad9a10
<u>Anubis</u>	SHA256	98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc 932ce385c8ed
<u>Sinobi</u>	SHA256	1b2a1e41a7f65b8d9008aa631f113cef36577e912c13f223ba88 34bbefa4bd14, 676dc8e28c90e64000a998ec257c014cb1152e7a5bdccab3916 d8fba401853da, 9432b065c803baa54f1fefac20d97affce212dec2bb9a597fc0100 64d391fc24, 8bb8c6e72d20e9b07bb55e0b0d168efe99d0088122131ae96d 13fa01d3325a17,

Attack Name	TYPE	VALUE
<u>Sinobi</u>	SHA256	82cd0af26bc1e9e3b0bfcfe6c61cf467992367a31d87e6bd7e2efa8e9fecbb25, d4919a7402d7ae02516589fbdfb3cc436749544052843a37b5d36ac4b7385b18
	File Extension	.SINOBI
	Tor Domains	sinobi7yuoppj76qnkiobwfc2qve2xkv2ckvzyyjbldw7ucpptl62ad[.]onion/login, sinobi57mfegeov2naiufkidlkpze263jtbldokimfjqmk2mye6s4yqd[.]onion/login, sinobibjqytwqxjw24zuerqcjyd3hoow6zia7z6kzvwawivamu7nqayd[.]onion/login, sinobicrh73ongfujajmlyyhalvkhlcgttxkxaxz3gvsgdcgf76uiqd[.]onion/login, sinobi6ftrg27d6g4sjdt65malds6cfptlnjyw52rskakqjda6uvb7yd[.]onion, sinobi6rlec6f2bgn6rd72xo7hvds4a5ajiu2if4oub2sut7fg3gomqd[.]onion, sinobi6ywgmmvg2gj2yygkb2hxbimaxpqkyk27wti5zjwhfcldhackid[.]onion, sinobi7l3wet3uqn4cagjiessuomv75aw3bvgh4jppj43od7xndb7kadd[.]onion, sinobi7sukclb3ygtorysbtrodgdbnrmgbhov45rwzipubbbzhiu5jvqd[.]onion, sinobi23i75c3znmqqxyuzqvhnjsar7actgvc4nqeuahgc5yvz3zqd[.]onion, sinobia6mw6ht2wcdjphessyzpy7ph2y4dyqbd74bgobgju4ybytmkqd[.]onion,
<u>INFINITERED</u>	SHA256	8f0158855a656b629ca76ebca565f18bc25563ded34b65d6771632c20edb68ec, 51a57bfc9ed3eb6451c1c289607814d59e1698c666fb97ac5f694c398f23d045
	Session ID prefix	xc32038474a
	GUID delimiter	b49e334d-9c01-463e-9bc5-00a6920fb66e
<u>Potemkin</u>	SHA256	2abe5dd3a057fdef935722e50e9251c272d29fd26113187b853a1f9a9cb89d9b, 79f7b67ce8b39070f3e1c2b90fce0ce84134782a7dedcccc1edac197ee9e089b
<u>RMMProject</u>	SHA256	3b7ae925e2d64522b4f69b56285b05aeca8c5aab5ab46a9c02c4fafb69d881ce
<u>BabaDeda Loader</u>	SHA256	0098b2c38a69132bfde02d329d6c1c6e2b529d32d7b775a2ac78a369c0d10853, 062f019515bff366fcbf49cca3f776c21e2beb81c043a45eea81044a9391fd97



Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-42897</u>		Microsoft Exchange Server 2016 (all update levels), Microsoft Exchange Server 2019 (all update levels), Microsoft Exchange Server Subscription Edition (all update levels)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:exchange_server:2016:-:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:-:*:*:*:subscription:*:*:*	-
Microsoft Exchange Server Cross-Site Scripting Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1190: Exploit Public-Facing Application; T1059.007: JavaScript; T1566: Phishing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-0257</u>		Palo Alto Networks PAN- OS 10.2 (Before 10.2.7- h34 / 10.2.10- h36 / 10.2.13-h21 / 10.2.16-h7 / 10.2.18-h6), PAN-OS 11.1 (Before 11.1.4-h33 / 11.1.6-h32 / 11.1.7- h6 / 11.1.10-h25 / 11.1.13-h5 / 11.1.15), PAN-OS 11.2 (Before 11.2.4-h17 / 11.2.7-h14 / 11.2.10-h7 / 11.2.12), PAN-OS 12.1 (Before 12.1.4-h6 / 12.1.7), Prisma Access 10.2 (Before 10.2.10-h36), Prisma Access 11.2 (Before 11.2.7-h13)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*	-
Palo Alto Networks PAN- OS Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-565	T1190: Exploit Public-Facing Application; T1550: Use Alternate Authentication Material	https://security.paloaltonetworks.com/CVE-2026-0257

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2025-32372</u>		DotNetNuke.Core Version Prior to 9.13.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:dnnsoftware:dotnetnuke:*:*:*:*:*:*	GodPotato Chisel
DotNetNuke Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application	https://github.com/dnnsoftware/Dnn.Platform/releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-55591</u>		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 KEY	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*	Qilin Ransomware
Fortinet FortiOS Authorization Bypass Vulnerability		cpe:2.3:o:fortinet:fortios:*:*:*:*:*	
	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
<u>CVE-2024-21762</u>		Fortinet FortiOS versions: 7.4.0 through 7.4.2 7.2.0 through 7.2.6 7.0.0 through 7.0.13 6.4.0 through 6.4.14 6.2.0 through 6.2.15 6.0 all versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:fortinet:fortios:*:*.*.*.*.*	Qilin Ransomware
Fortinet FortiOS SSL- VPN Out-of-Bounds Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1203: Exploitation for Client Execution, T1588.005: Exploits, T1059.007: JavaScript	https://fortiguard.fortinet.com/psirt/FG-IR-24-015

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2023-27532</u>		Veeam Backup & Replication Cloud Connect	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*	Qilin Ransomware
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
<u>CVE-2025-31324</u>		SAP NetWeaver Visual Composer	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:sap:netweaver:7.50: *.~*~*~*~*~*	Qilin Ransomware
SAP NetWeaver Unrestricted File Upload Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	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
<u>CVE-2026-20230</u>		Cisco Unified Communications Manager (Unified CM) and Unified CM SME, release 14 (before 14SU6) and release 15 (before 15SU5 / COP1), with WebDialer enabled	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY		
Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability		cpe:2.3:a:cisco:unified_communications_manager:*:*:*:*:*:* cpe:2.3:a:cisco:unified_communications_manager_session_management_edition:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-20245</u>		Cisco Catalyst SD- WAN 20.18.2.1 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	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
<u>CVE-2026-20127</u>		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 KEY	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
<u>CVE-2026-50751</u>		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
<u>CVE-2026-49160</u>		Windows 11 Version 23H2, 10 Version 22H2; Windows Server 2025, 2022, 2019, 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	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
<u>CVE-2026-45586</u>		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 KEY	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
<u>CVE-2026-50507</u>		Windows Server 2012, 2016, 2019, 2022, 2025; Windows 10 Version 1607; Windows 11 Version 26H1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	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
<u>CVE-2026-47291</u>		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 KEY	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-2026-35273		Oracle PeopleSoft Enterprise PeopleTools (versions 8.61, 8.62)	ShinyHunters (aka UNC6240)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	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 , https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-10520</u>		Ivanti Sentry (Before R10.5.2 / R10.6.2 / R10.7.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-20262</u>		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)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1505: Server Software Component, T1078: Valid Accounts	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2024-53704</u>		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 KEY	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
<u>CVE-2026-54420</u>		LiteSpeed cPanel Plugin (user-end) (Before 2.4.8), as distributed in LiteSpeed WHM Plugin (Before 5.3.2.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:litespeedtech:litespeed_cpanel_plugin:*:*:*:*:*:* cpe:2.3:a:litespeedtech:litespeed_whm_plugin:*:*:*:*:*:*	-
LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-61	T1078: Valid Accounts, T1068: Exploitation for Privilege Escalation, T1611: Escape to Host	https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-12569</u>		PTC Windchill PDMLink and FlexPLM - all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ptc:windchill_pdmlink:*.~.*.*.*.*.*.*.*	-
PTC Windchill and FlexPLM Improper Input Validation Vulnerability		cpe:2.3:a:ptc:flexplm:*.~.*.*.*.*.*.*.*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20 CWE-502	T1190: Exploit Public-Facing Application,T1059: Command and Scripting Interpreter,T1505: Server Software Component,T1505.003: Web Shell	https://www.ptc.com/en/support/article/CS473270 , https://support.ptc.com/appserver/cs/view/solution.jsp?n=CS473270

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>XenoRAT</u>	Xeno RAT is an open-source Remote Access Trojan (RAT) that is widely abused by threat actors to establish persistent access to compromised systems and conduct post-exploitation activities. Once executed, it connects to attacker-controlled infrastructure through encrypted command-and-control (C2) channels, enabling remote command execution, file manipulation, and network tunneling via SOCKS5 proxies. The malware can gather system information, monitor user activity, capture keystrokes, screenshots, clipboard data, and webcam or microphone input, while maintaining stealth through encrypted communications and persistence mechanisms such as Scheduled Tasks and Registry Run keys. Its ability to load assemblies directly into memory, operate covertly, and remove itself after use makes it a versatile tool for long-term surveillance and unauthorized system control.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		System Compromise	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>GodPotato</u>	GodPotato is a Windows privilege escalation utility commonly leveraged by threat actors to abuse the SeImpersonatePrivilege permission and elevate access from a low-privileged account to SYSTEM-level privileges. In observed intrusions, the tool is used to execute commands with elevated rights, enabling attackers to gain full control over compromised systems. Analysis of accompanying documentation suggests that earlier execution methods relying on PowerShell-encoded wrappers were abandoned due to compatibility issues, with attackers instead opting for direct command execution. The binary is typically stored on attacker-controlled infrastructure and retrieved during runtime, allowing it to be deployed on demand as part of a broader post-exploitation workflow.	Exploiting Vulnerabilities	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2025-32372
TYPE		IMPACT	AFFECTED PLATFORM
Tool		Execute commands	-
ASSOCIATED ACTOR			PATCH LINKS
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34523 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207 , https://github.com/dnnsoftware/Dnn.Platform/releases/

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Chisel</u>	Chisel is a lightweight tunneling utility frequently used by threat actors to create encrypted communication channels that bypass network restrictions and firewall controls. Forwarding traffic through secure tunnels, it enables covert access to internal systems and supports lateral movement within compromised environments. In the observed intrusion, the presence of a dedicated gov.om subdirectory within the /scripts folder containing custom Python scripts.	Exploiting Vulnerabilities	CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2025-32372
TYPE		IMPACT	AFFECTED PLATFORM
Tool		Lateral Movement	-
ASSOCIATED ACTOR			PATCH LINKS
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34523 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207 , https://github.com/dnnsoftware/Dnn.Platform/releases/

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AZUREVEIL	AZUREVEIL is a 64-bit DLL malware implant built as an Adaptix C2 agent in MinGW C++. It uses runtime API resolution with djb2 hashing to dynamically load Windows APIs and evade analysis. Instead of a traditional C2 server, it uses Microsoft Azure Blob Storage as a dead-drop channel, retrieving encrypted commands, executing them on the victim system, and uploading encrypted results back to the cloud.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Adaptix C2 Agent		Execute command	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>RUSTCLOAK</u>	RUSTCLOAK is a Rust-based loader designed to advance the infection chain and deploy the final payload on compromised systems. The malware contains an operational security oversight, as a plaintext Rust build path embedded within the binary exposes details from the developer's environment, including the Windows username dell2 and references to libraries used for SM4 encryption and Base64 encoding. To evade detection, RUSTCLOAK performs anti-analysis checks by retrieving the host's computer name and comparing it against a hardcoded list of more than 100 known sandbox and security researcher machine names, terminating or altering execution when an analysis environment is suspected.	Phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Loads AZUREVEIL	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
PhantomRelay	PhantomRelay is a modular PowerShell-based remote access trojan (RAT) that operates through a two-stage execution chain, beginning with a system fingerprinting component before launching the primary RAT client. The malware communicates with its command-and-control (C2) infrastructure over WebSockets and enables attackers to execute PowerShell scripts and Windows commands remotely. While its native functionality is relatively limited, PhantomRelay can dynamically expand its capabilities by downloading and executing additional PowerShell modules delivered by the C2 server. Researchers have identified multiple variants of the malware, including PhantomRelayLite, PhantomRelayV1, and PhantomRelayV2, each reflecting different stages of development and operational use.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		System Compromise	Microsoft Windows, Android
ASSOCIATED ACTOR			PATCH LINK
GREYVIBE			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
FallSpy	FallSpy is an Android spyware strain first identified in August 2025 and has since been linked to multiple GREYVIBE-associated campaigns, including PrincessClub and Nebo. The malware displays benign decoy content to avoid raising suspicion while secretly collecting a wide range of sensitive information from infected devices. Its data theft capabilities include harvesting contacts, call logs, installed applications, SIM-linked phone numbers, device and network details, Wi-Fi information, location data, public IP addresses, and media files.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
Android spyware		Data Theft	Microsoft Windows, Android
ASSOCIATED ACTOR			PATCH LINK
GREYVIBE			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LegionRelay	LegionRelay is a lightweight PowerShell-based remote access trojan (RAT) that communicates with its command-and-control (C2) infrastructure through REST API requests. While the malware's native functionality is primarily limited to executing attacker-issued PowerShell commands, its capabilities can be significantly expanded through additional scripts deployed during post-compromise operations. Observed activity shows operators using LegionRelay to perform file discovery and exfiltration, capture screenshots, steal browser-stored data, collect information from messaging applications such as Telegram and WhatsApp, establish remote desktop access, and carry out other actions aimed at maintaining access and extracting sensitive information from compromised environments.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Execute Commands, Data Theft	Microsoft Windows, Android
ASSOCIATED ACTOR			PATCH LINK
GREYVIBE			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>LOOKVALPS</u>	LOOKVALPS is a custom PowerShell-based loader that uses obfuscation techniques to conceal malicious payloads and hinder analysis. The tool has been observed delivering and executing both initial access payloads and post-compromise tooling, helping threat actors evade detection and complicate incident response efforts.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Loads additional payloads	Microsoft Windows, Android
ASSOCIATED ACTOR			PATCH LINK
GREYVIBE			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>LOOKVALJS</u>	LOOKVALJS is a custom JavaScript-based loader that employs obfuscation techniques to conceal malicious payloads and evade detection. It has been observed delivering and executing malware during various stages of an intrusion, enabling threat actors to deploy additional tooling while masking malicious activity. Beginning in March 2026, LOOKVALJS was largely succeeded by TEASOUP, a newer JavaScript-based loader that continued to serve a similar role in payload delivery and execution.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Loads additional payloads	Microsoft Windows, Android
ASSOCIATED ACTOR			PATCH LINK
GREYVIBE			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>DAYLIGHT</u>	DAYLIGHT is a custom PowerShell-based loader that employs obfuscation, that has been actively used since October 2025 to conceal malicious payloads and evade security controls. The tool is designed to obscure script content and execution flow, making analysis and detection more difficult while facilitating the delivery of additional malware during different stages of an intrusion. Based on observed activity, DAYLIGHT likely replaced LOOKVALPS.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Loads additional payloads	Microsoft Windows, Android
ASSOCIATED ACTOR			PATCH LINK
GREYVIBE			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>TEASOUP</u>	TEASOUP is a custom JavaScript-based loader and that uses obfuscation, observed in threat actor operations since March 2026. Designed to conceal malicious code and complicate analysis, it enables the delivery and execution of payloads while helping attackers evade detection. TEASOUP appears to have succeeded LOOKVALJS as the threat actor's primary JavaScript-based loader, indicating a continued effort to refine its tooling and improve the stealth and effectiveness of its malware deployment techniques.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Loads additional payloads	Microsoft Windows, Android
ASSOCIATED ACTOR			PATCH LINK
GREYVIBE			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>CMD Organization</u>	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	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Credential compromise, Persistent access, Financial Loss	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

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	-
TYPE		IMPACT	AFFECTED PLATFORM
Infostealer		Credential exposure, Session hijacking and MFA bypass	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Meow	The 'Meow' backdoor established persistence via a DLL (observed as Netdrv.dll) that beacons over HTTPS, using HKCU Run-key entries disguised as fake Microsoft Teams update installers with iterative version numbers.	SEO Poisoning, Malvertising	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent, Covert C2 hidden in normal traffic	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Interlock</u>	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 Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Information Theft, Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Medusa</u>	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	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Information Theft, Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Anubis</u>	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	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Information Theft, Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Rhadamanth</u> <u>vs</u>	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	-
TYPE		IMPACT	AFFECTED PLATFORM
Infostealer		Information theft, Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Information theft, Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Qilin</u>	Qilin (aka Agenda, Water Galura, Phantom Mantis, Gold Feather), is a prolific Ransomware-as-a-Service operation that supplies its encryption toolkit to affiliate actors, who commonly employ double-extortion tactics: they both encrypt victims’ files and steal sensitive data to threaten public release unless a ransom is paid. Beyond the usual RaaS playbook, a major evolution lets affiliates run a Linux ransomware variant on Windows hosts by abusing legitimate remote-management and file-transfer tools such as AnyDesk, ScreenConnect, and Splashtop; this cross-platform trick evades many Windows-focused detection controls and improves stealth inside mixed-OS environments, making Qlin attacks harder to spot and more damaging when they succeed.	Exploiting Vulnerabilities	CVE-2024-55591 CVE-2024-21762 CVE-2023-27532 CVE-2025-31324 CVE-2026-50751
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		System Compromise, Encrypt Data	Fortinet FortiOS, Veeam Backup & Replication Cloud Connect, SAP NetWeaver Visual Composer, Check Point Mobile Access / SSL VPN, Remote Access VPN, Spark Firewall
ASSOCIATED ACTOR			PATCH LINKS
-			https://fortiguard.fortinet.com/psirt/FG-IR-24-535 , https://fortiguard.fortinet.com/psirt/FG-IR-24-015 , https://www.veeam.com/kb4424 , https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html , https://support.checkpoint.com/results/sk/sk185033

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>MLTBackdoor</u> r	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	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Information theft, Stealthy execution	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SPECTRALVIPER</u>	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.	DLL side-loading	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Covert espionage access	Windows
ASSOCIATED ACTOR			PATCH LINK
OceanLotus			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Sinobi Ransomware</u>	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.	Compromised SonicWall SSL VPN credentials	CVE-2024-53704 CVE-2024-40766
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Anti-recovery encryption, double extortion	Windows
ASSOCIATED ACTOR			PATCH LINKS
-			https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003 , https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>INFINITERED</u>	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.	Post-compromise, via web shell	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Domain admin, data theft	REDCap servers; Google Workspace
ASSOCIATED ACTOR			PATCH LINK
UNC6508			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>DarkKomet</u>	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	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote access, Steam hijacking	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Lumma</u>	Lumma Stealer is a potent info-stealing malware that evades detection by injecting itself into memory, employing multiple layers of encryption and obfuscation. The payload, cleverly disguised as a Base64- encoded DLL concealed within a block of French text, is specifically crafted to bypass most antivirus defenses.	Social Engineering, Loader chains, cracked software	-
TYPE		IMPACT	AFFECTED PLATFORM
Infostealer		Information theft, Financial Loss	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Vidar</u>	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	-
TYPE		IMPACT	AFFECTED PLATFORM
Infostealer		Data theft	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>RenEngine</u>	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	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Stealer deployment, data theft	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Potemkin	Potemkin loader which is a purpose-built loader with a deterministic Domain Generation Algorithm (DGA), a custom byte cipher, and a reflective module loader, but its entire command vocabulary is a single task code.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Resilient C2 communication, Modular extensibility	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RMMProject	RMMProject is a remote access trojan (RAT) built around an embedded LuaJIT scripting engine, giving operators a flexible, programmable platform for executing malicious tasks. It supports 15 distinct task types, making it a versatile tool for a wide range of intrusion activities.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Full remote compromise, Browser credential and cookie theft	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>EtherRAT</u>	EtherRAT serves as the resilient backbone of an intrusion: a blockchain-anchored backdoor designed to survive domain takedowns and other disruption efforts that would typically sever an attacker's foothold.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Takedown-resistant C2, Persistent remote access	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>BabaDeda Loader</u>	BabaDeda was previously known for hiding malicious payloads inside legitimate-looking installer packages, disguising its activity as trustworthy software. This new framework preserves that same underlying code lineage but evolves it into a far more capable loader—engineered for stealth, evasion, and flexible payload delivery.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Deceptive delivery, Stealth and evasion	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Lorem Ipsum Loader	The Lorem Ipsum Loader is a multi-stage malware loader operated by the financially motivated threat group Rapid Brigantine (a.k.a. Vanilla Tempest). Its defining technical signature is a substitution-cipher routine that reconstructs executable payloads at runtime from encoded text strings of innocuous-looking words mapped to byte values making static and signature-based detection difficult.	ClickFix	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Registry persistence, Backdoor deployment, Credential theft	Microsoft Windows
ASSOCIATED ACTOR			PATCH LINK
Rapid Brigantine			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Edgecution</u>	Edgecution is a malicious Microsoft Edge browser extension that abuses the Chrome native messaging protocol to escape the browser sandbox and interact directly with the host system. It has two components: the Edge extension, which beacons to a C2 server over WebSockets, and a Python-based backdoor that handles privileged host-level operations including filesystem access, arbitrary code execution, and PowerShell command execution.	Social Engineering	-
TYPE		IMPACT	AFFECTED PLATFORM
Browser Hijacker		Sandbox escape, Code execution, Credential harvesting	Microsoft Edge, Microsoft Teams, Microsoft Outlook
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Gaslight</u>	Gaslight is a Rust-based macOS implant and information stealer attributed with high confidence to DPRK-aligned activity. Its defining feature is an embedded 3.5 KB Markdown-fenced payload of 38 fabricated "system" messages designed as a prompt-injection cascade that targets LLM-assisted malware triage pipelines rather than conventional sandboxes, attempting to make the analyst's AI tooling abort, truncate, or refuse analysis.	-	-
TYPE		IMPACT	AFFECTED PLATFORM
Infostealer		Persistent backdoor, Browser harvesting, Credential exfiltration	macOS
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>TinyCT</u>	TinyRCT is a lightweight, C#-based remote access Trojan built to quietly take control of Windows systems. Once executed, it acts as a full-featured backdoor, running arbitrary commands, enumerating and exfiltrating files, capturing screenshots, and giving attackers hands-on remote management of the compromised host. What sets it apart is its evasion-first design: before doing anything else, TinyRCT checks whether it's running from %LOCALAPPDATA%, and if it isn't, say, in a sandbox or on an analyst's machine, it shuts itself down immediately.	ASPX web shells	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		System Compromise, command execution, screen capture	Windows
ASSOCIATED ACTOR			PATCH LINK
CL-STA-1062			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Prinz Eugen</u>	Prinz Eugen is a financially motivated, Go-based ransomware operation that surfaced publicly in April 2026, with its encryptor first analyzed hands-on the following month. It runs a deliberately quiet double-extortion playbook, stealing data first, encrypting second, but skips the usual ransom note entirely, instead pushing all victim communication out-of-band through direct email and a dedicated Tor leak portal. The operation carries a distinct anti-forensic footprint, prioritizing freshly modified files during encryption to maximize damage fast.	Compromised RDP credentials	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Encrypt Data, Data theft	Windows
ASSOCIATED ACTOR			PATCH LINK
ROOTBOY			-

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 SideCopy (alias UNC2269, White Dev 55, Mocking Draco, TAG-140)	Pakistan	Government, Finance, and public administration	Afghanistan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	XenoRAT	Windows
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0042: Resource Development; T1566: Phishing; T1566.001: Spearphishing Attachment; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.007: JavaScript; T1129: Shared Modules; T1106: Native API; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1027.011: Fileless Storage; T1620: Reflective Code Loading; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1055: Process Injection; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1070: Indicator Removal; T1070.004: File Deletion; T1012: Query Registry; T1082: System Information Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1056: Input Capture; T1056.001: Keylogging; T1113: Screen Capture; T1115: Clipboard Data; T1123: Audio Capture; T1125: Video Capture; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1095: Non-Application Layer Protocol; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1090: Proxy T1090.002: External Proxy; T1568: Dynamic Resolution; T1583: Acquire Infrastructure; T1583.001: Domains; T1584: Compromise Infrastructure			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 GREYVIBE	Russia	Military, Government, Defense, Energy, Civilian individuals, NGOs, Business entities, Software supplier	Ukraine, Moldova, Romania, Brazil, Venezuela, Guinea
	MOTIVE		
	Information theft, and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	PhantomRelay (variants: PhantomRelayLite, PhantomRelayV1, PhantomRelayV2), FallSpy, LegionRelay, LOOKVALPS, LOOKVALIS, DAYLIGHT, TEASOUP	Web browsers (Chromium-based), Telegram Desktop, WhatsApp Desktop, Remote Desktop Protocol (RDP) targeted during post-compromise activity

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002:Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0008: Lateral Movement; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1583.001: Domains; T1584: Compromise Infrastructure; T1584.001: Domains; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1585.002: Email Accounts; T1587: Develop Capabilities; T1587.001: Malware; T1588: Obtain Capabilities; T1588.002: Tool; T1608: Stage Capabilities; T1608.001: Upload Malware; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1566.003: Spearphishing via Service; T1091: Replication Through Removable Media; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1204.004: Malicious Copy and Paste; T1204: User Execution; T1204.004: Malicious Copy and Paste; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.007: JavaScript; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1202: Indirect Command Execution; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1136: Create Account; T1136.001: Local Account; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1547: Boot or Logon Autostart Execution; T1547.009: Shortcut Modification; T1027: Obfuscated Files or Information; T1027.006: HTML Smuggling; T1140: Deobfuscate/Decode Files or Information; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1070: Indicator Removal; T1070.003: Clear Command History; T1497: Virtualization/Sandbox Evasion; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1564.002: Hidden Users; T1218: System Binary Proxy Execution; T1218.003: CMSTP; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1480: Execution Guardrails; T1003: OS Credential Dumping; T1003.002: Security Account Manager; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1539: Steal Web Session Cookie; T1056: Input Capture; T1056.001: Keylogging; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1083: File and Directory Discovery; T1016: System Network Configuration Discovery; T1518: Software Discovery; T1113: Screen Capture; T1005: Data from Local System; T1119: Automated Collection; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1123: Audio Capture; T1125: Video Capture; T1636: Protected User Data; T1636.003: Contact List; T1636.002: Call Log; T1430: Location Tracking; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1102: Web Service; T1102.001: Dead Drop Resolver; T1132: Data Encoding; T1132.001: Standard Encoding; T1572: Protocol Tunneling; T1090: Proxy; T1219: Remote Access Software; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1021.002: SMB/Windows Admin Shares; T1041: Exfiltration Over C2 Channel; T1496: Resource Hijacking; T1496.001: Compute Hijacking

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/RANSOM WARE	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			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>ShinyHunters</u> (aka UNC6240)	-	All	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2026-35273	-	Oracle PeopleSoft Enterprise PeopleTools
TTPs			
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			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>OceanLotus</u> (alias <u>APT32</u>, <u>SeaLotus</u>, <u>APT-C-00</u>, <u>Ocean Buffalo</u>, <u>Tin Woodlawn</u>, <u>ATK 17</u>, <u>SectorF01</u>, <u>Pond Loach</u>, <u>APT-LY-100</u>, <u>Lotus Bane</u>)	Vietnam	Financial services, Stock investors, Infrastructure, Transport, Construction	Vietnam (domestic); historically China and Southeast Asia
	MOTIVE		
	Espionage and Information Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	SPECTRALVIPER	FireAnt Metakit; Microsoft SQL Server
TTPs			
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			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UNC6508	China (PRC-nexus)	Medical and clinical research, academic research centers, military health institutions, health regulatory bodies, professional advocacy groups, defense	North America
	MOTIVE		
	Espionage and Information Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	INFINITERED	REDCap (Research Electronic Data Capture); Google Workspace content compliance rules
TTPs			
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			

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/RANSOM WARE	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			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Rapid Brigantine</u> <u>(aka Vanilla</u> <u>Tempest, Vice</u> <u>Society, Vice</u> <u>Spider, DEV-</u> <u>0832)</u>	-	Education, Financial Services, Architecture, Legal Services, Non-profit, Construction Technology, Content Publishing	Worldwide
	MOTIVE		
	Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Lorem Ipsum Loader, Oyster, Supper, MeowBackConn, Rhysida Ransomware	Google Chrome, Mozilla Firefox, Microsoft Edge, Microsoft Defender, WordPress
TTPs			
TA0043: 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; TA0040: Impact; T1584: Compromise Infrastructure; T1584.006: Web Services; T1608: Stage Capabilities; T1608.004: Drive-by Target; T1608.001: Upload Malware; T1583: Acquire Infrastructure; T1583.008: Malvertising; T1588: Obtain Capabilities; T1588.003: Code Signing Certificates; T1189: Drive-by Compromise; T1204: User Execution; T1204.004: Malicious Copy and Paste; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.007: JavaScript; T1059.003: Windows Command Shell; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1218.007: Msiexec; T1106: Native API; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1562: Impair Defenses T1562.001: Disable or Modify Tools; T1112: Modify Registry; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1620: Reflective Code Loading; T1574: Hijack Execution Flow; T1574.001: DLL; T1055: Process Injection; T1055.001: Dynamic-link Library Injection; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1497: Virtualization/Sandbox Evasion; T1480: Execution Guardrails; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1539: Steal Web Session Cookie; T1518: Software Discovery; T1518.001: Security Software Discovery; T1082: System Information Discovery; T1087: Account Discovery; T1057: Process Discovery; T1021: Remote Services; T1021.002: SMB/Windows Admin Shares; T1021.006: Windows Remote Management; T1047: Windows Management Instrumentation; T1570: Lateral Tool Transfer; T1113: Screen Capture; T1560: Archive Collected Data; T1005: Data from Local System; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1568: Dynamic Resolution; T1568.002: Domain Generation Algorithms; T1102: Web Service; T1102.001: Dead Drop Resolver; T1102.002: Bidirectional Communication; T1572: Protocol Tunneling; T1090: Proxy; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1486: Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>CL-STA-1062</u>	China	Government, Critical Energy Infrastructure, State-Owned Enterprises	Southeast Asia
	MOTIVE		
	Espionage and Information Theft		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	TinyRCT	Windows

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1204: User Execution; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1505: Server Software Component; T1505.003: Web Shell; T1574: Hijack Execution Flow; T1574.014: AppDomainManager; T1068: Exploitation for Privilege Escalation; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1497: Virtualization/Sandbox Evasion; T1070: Indicator Removal; T1070.004: File Deletion; T1070.009: Clear Persistence; T1027: Obfuscated Files or Information; T1003: OS Credential Dumping; T1082: System Information Discovery; T1083: File and Directory Discovery; T1016: System Network Configuration Discovery; T1087: Account Discovery; T1049: System Network Connections Discovery; T1046: Network Service Discovery; T1005: Data from Local System; T1113: Screen Capture; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1213: Data from Information Repositories; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1572: Protocol Tunneling; T1090: Proxy; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1030: Data Transfer Size Limits

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>ROOTBOY (also operates as avtokz; extortion aliases GERMANIA)</u>	-	Financial Services, Professional services, Education, and Automotive	South Africa, France, United States and the United Kingdom
	MOTIVE		
	Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Prinz Eugen Ransomware	Windows
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1583.001: Domains; T1078: Valid Accounts; T1133: External Remote Services; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1136: Create Account; T1136.001: Local Account; T1219: Remote Access Software; T1070: Indicator Removal; T1070.004: File Deletion; T1027: Obfuscated Files or Information; T1083: File and Directory Discovery; T1021: Remote Services; T1105: Ingress Tool Transfer; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel; T1486: Data Encrypted for Impact; T1657: Financial Theft			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1091: Replication Through Removable Media	
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
		T1566.003: Spearphishing via Service
TA0002: Execution	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.004: Unix Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.007: JavaScript
	T1072: Software Deployment Tools	

Tactic	Technique	Sub-technique
TA0002: Execution	T1106: Native API	
	T1129: Shared Modules	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution
TA0003: Persistence	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1133: External Remote Services	
	T1136: Create Account	T1136.001: Local Account
	T1176: Browser Extensions	
	T1197: BITS Jobs	
	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.001: Launch Agent
		T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.009: Shortcut Modification
	T1556: Modify Authentication Process	

Tactic	Technique	Sub-technique
TA0003: Persistence	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
TA0004: Privilege Escalation	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.012: Process Hollowing
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
	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
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1611: Escape to Host	
TA0005: Defense Evasion	T1014: Rootkit	
	T1027: Obfuscated Files or Information	T1027.006: HTML Smuggling
		T1027.007: Dynamic API Resolution
		T1027.010: Command Obfuscation

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.011: Fileless Storage
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.003: Rename System Utilities
		T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
		T1036.008 : Masquerade File Type
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.012: Process Hollowing
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.003: Clear Command History
		T1070.004: File Deletion
		T1070.009: Clear Persistence
	T1078: Valid Accounts	T1078.002: Domain Accounts
		T1078.003: Local Accounts
	T1112: Modify Registry	
	T1127: Trusted Developer Utilities Proxy Execution	
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1140: Deobfuscate/Decode Files or Information	
	T1197: BITS Jobs	
	T1202: Indirect Command Execution	
	T1211: Exploitation for Defense Evasion	

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1218: System Binary Proxy Execution	T1218.003: CMSTP
		T1218.004: InstallUtil
		T1218.005: Mshta
		T1218.007: Msiexec
		T1218.011: Rundll32
	T1480: Execution Guardrails	
	T1484: Domain or Tenant Policy Modification	T1484.001: Group Policy Modification
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1550: Use Alternate Authentication Material	
	T1553: Subvert Trust Controls	T1553.002: Code Signing
		T1553.005: Mark-of-the-Web Bypass
	T1556: Modify Authentication Process	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
		T1562.006: Indicator Blocking
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.002: Hidden Users
		T1564.003: Hidden Window
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1601: Modify System Image	T1601.001: Patch System Image

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.002: Security Account Manager
	T1056: Input Capture	T1056.001: Keylogging
		T1056.003: Web Portal Capture
	T1110: Brute Force	T1110.001: Password Guessing
		T1110.002: Password Cracking
		T1110.003: Password Spraying
	T1212: Exploitation for Credential Access	
	T1528: Steal Application Access Token	
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	T1552.004: Private Keys
	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
	T1556: Modify Authentication Process	
TA0007: Discovery	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1049: System Network Connections Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.001: Local Account
		T1087.002: Domain Account
	T1120: Peripheral Device Discovery	
	T1135: Network Share Discovery	
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1622: Debugger Evasion	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
		T1021.004: SSH
		T1021.006: Windows Remote Management
	T1072: Software Deployment Tools	
	T1080: Taint Shared Content	
	T1091: Replication Through Removable Media	
	T1550: Use Alternate Authentication Material	
	T1570: Lateral Tool Transfer	

Tactic	Technique	Sub-technique
TA0009: Collection	T1005: Data from Local System	
	T1039: Data from Network Shared Drive	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.003: Web Portal Capture
	T1074: Data Staged	T1074.001: Local Data Staging
	T1113: Screen Capture	
	T1114: Email Collection	T1114.003: Email Forwarding Rule
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1123: Audio Capture	
	T1125: Video Capture	
	T1213: Data from Information Repositories	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
TA0010: Exfiltration	T1030: Data Transfer Size Limits	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.002: External Proxy
		T1090.003: Multi-hop Proxy
	T1095: Non-Application Layer Protocol	

Tactic	Technique	Sub-technique
TA0011: Command and Control	T1102: Web Service	T1102.001: Dead Drop Resolver
		T1102.002: Bidirectional Communication
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1219: Remote Access Software	
	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
	T1571: Non-Standard Port	
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1491: Defacement	T1491.001: Internal Defacement
	T1496: Resource Hijacking	
	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	T1499.001: OS Exhaustion Flood
		T1499.003: Application Exhaustion Flood
		T1499.004: Application or System Exploitation
	T1565: Data Manipulation	

Tactic	Technique	Sub-technique
TA0040: Impact	T1657: Financial Theft	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.003: Virtual Private Server
		T1583.006: Web Services
		T1583.008 : Malvertising
	T1584: Compromise Infrastructure	T1584.001: Domains
		T1584.003: Virtual Private Server
	T1585: Establish Accounts	
	T1586: Compromise Accounts	T1586.001: Social Media Accounts
		T1586.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.004: Drive-by Target
		T1608.006: SEO Poisoning
	T1650: Acquire Access	
TA0043: Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1598: Phishing for Information	T1598.002: Spearphishing Attachment

Top 5 Takeaways

#1

In June 2026, 11 zero-day vulnerabilities surfaced, led by the “Three Celebrity Vulnerabilities,” including **PROXYSHELL**, **HTTP/2 Bomb**, and **Squidbleed**. These zero-days were found across products from Microsoft, Fortinet, SAP, Cisco, Check Point, Google Chrome, and Oracle.

#2

Newly identified malware active in June included a broad mix of Backdoors, RATs, and Loaders. Key discoveries were **AZUREVEIL**, **RUSTCLOAK**, **CMD Organization**, **MLTBackdoor**, **Potemkin**, **RMMProject**, **EtherRAT**, **BabaDeda Loader**, **Lorem Ipsum Loader**, **Edgecution**, **Gaslight**, and **TinyRCT**, each representing distinct capabilities ranging from stealthy persistence and credential theft to large-scale compromise.

#3

Cyberattacks concentrated heavily on the **United States**, **Singapore**, **Vietnam**, **Canada**, and **Brazil**, which absorbed the bulk of hostile activity. Espionage operations and financially motivated intrusions drove the surge, underscoring that no region remained insulated as adversaries expanded their operations worldwide.

#4

Financial, **Education**, **Government**, **Technology**, and **Healthcare** sectors absorbed the bulk of targeted activity, with ransomware operations, data theft, and espionage campaigns driving operational disruption. Attackers continued to refine techniques and expand pressure across these industries.

#5

Activity during the period was dominated by **TeamPCP**, **ShinyHunters**, **OceanLotus**, **UNC6508**, **Insomnia**, **Rapid Brigantine**, and **ROOTBOY**, all well-resourced groups known for sustained, high-impact operations. Their campaigns shaped a threat landscape defined by disciplined tradecraft, rapid exploitation cycles, and a clear focus on high-value targets across public and private sectors.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **29 significant vulnerabilities** and block the indicators related to the **10 active threat actors**, **38 active malware**, and **237 potential MITRE TTPs**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, who can get comprehensive insights into their threat exposure and take action easily through the HivePro Uni5 dashboard by:

- Running a scan to discover the assets impacted by the **29 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to **active threat actors**, **active malware**, and **potential MITRE TTPs** in Breach and Attack Simulation(BAS).

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 malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Social engineering: is an attack that relies on human interaction to persuade people into compromising security. It involves various strategies aimed at extracting specific information or performing illicit activities from a target.

Supply chain attack: Also known as a value-chain or third-party attack, occurs when an outside partner or provider with access to your systems and data infiltrates your system. The purpose is to gain access to source codes, development processes, or update mechanisms in order to distribute malware by infecting legitimate programs.

Eavesdropping: Often known as sniffing or spying, is a significant risk in cybersecurity. Passwords, credit card information, and other sensitive data are easily stolen during these attacks as they are transmitted from one device to another. This type of network attack often occurs when unsecured networks, such as public Wi-Fi connections or shared electronic devices, are used.

Glossary:

CISA KEV - Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities

CVE - Common Vulnerabilities and Exposures

CPE - Common Platform Enumeration

CWE - Common Weakness Enumeration

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>XenoRAT</u>	SHA256	9AE3D785486022AF82EA92E51B26E3F55C1BBA88A7BE2AD9790F4240E8499D14
<u>GodPotato</u>	Filename	gp_v6_exec.py
<u>Chisel</u>	Filename	/opt/c2/payloads/
<u>AZUREVEIL</u>	SHA256	783661d0f7edb338d2d50be087764d82dbbc9ee7989ddc57db1801e4ec9045b0, d151a70fda42e8452a251e6e3861a399fe3e200f7385bf09bf9abb c0723ac824
<u>RUSTCLOAK</u>	SHA256	8ca1ab86f7cf9fc6db4d306edbcf2fa38c3bb1ea71dfe78a442aafe56f07e9b0, 5ed14c2b7f7433a1a72dd6b668413f935a217ba10b69d89b774a82990fa12fe1, 080ab9bc2893ba7bad354551604a667af40ed2ae2d042d2323c2bd9ad3122192, 1c56228cbd1bdebb9e5ea55c2749150fee06c865ede4a3754e8bd6843e51d2d4
<u>PhantomRelay</u>	SHA256	920e8a8e06a1559ba0b4a1be5f6c290ed8e305fd130675ceadc655c79c1cb369, db05db462a0e8ba40c656dd0b8bd11f6fdc85895b54904df1dc83bb0609e2ff2, ee144c883784c635ef84e0ae6a12b03553c1fd65646621f22d08511bd3e6d42a, 03beb07ce116a2a69f360dd3fab8c3aa55bb42ce580d43f1924642874e388efe, c716dabe228f89e58835d2c93dbaa5719dc77f62c9e84f3e3d54ef82ded621e1, 286de17c2e8017241bee12b0935ed5e1e5d5216f4311be781ca1a69ad81188b3, d814564ab8b905c3b9b7a42e757228d9d30f8ffd4fa6b3c48f4aa7e2b1e44594

Attack Name	TYPE	VALUE
<u>FallSpy</u>	SHA256	cbaf6cdb2acbd293d7e58cabe41449027a28b84223ba88f19e4463ec4176dad0, bcb9e99021f88b9720a667d737a3ddd7d5b9f963ac3cae6d26e74701e406dcdc, 87b8abb05c7ee5642a5e801e7825dfa5ee4c1393ac998e87470ab53cc75e1842, d9810fa6aa59864ceef509ed551da85fce31d69cfcd78f2f8b146c761387370e, 4e6f85802d365751fa25c7014002ae44329a2d037d7b21f4bc34091b0c01b7b7, 7db11cf6a0417d5e20cd6720687ba86045b2fb758a7b585a49f572df2dc40c5e
<u>LegionRelay</u>	SHA256	63047083db26ec6a8aa2d0d008ca4c067855a952a89f9e3e878b2215e26841cf, ee87fae14e3cc64d894f0a677af8832f8669f11853374c18b7110df1fc52f4e5
<u>LOOKVALPS</u>	SHA256	40f9399ea067d69c0985aecdc54beddbcb585d7f660606e5bb4be981811c28ba
<u>LOOKVALJS</u>	SHA256	8a7401444dd7c85b36ff7b1d0b36c5953692ef32dbeac7642fb7c1034bd8a726, 93111e523c38d98247a78a0d1d9ae163e9874acb70721f6fe0bf451c62fff283, c823a315c2c78d2fd345c9b38bb7fc31a8cbff96c534ce9cc66c4e54bc7935a2, e9634032df81334e9e960ab8b88ff05a0f7ec9c034dc012f816f09e23c18d41b, a695a70c2efd11e1daa93997c1aaf976a205476839f553f2c8e64fb73123b853
<u>TEASOUP</u>	SHA256	5115eca388860371d994457793f3a3c2c3d106da48ca12ecccb9432522c56cc3, 2abb318455960b446d034967c8403ec4339ba248b946f02cb1307ed7e6f4e327

Attack Name	TYPE	VALUE
<u>Qilin</u>	Tor Leak Site	ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmb4mcbccnsd7j2rekvqd[.]onion
	SHA256	d82069cfc9395a240b9c140d283367ab470d587326c5e256aba78eb2c5a9ea85, 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6, 516927b55038c1702bc8a6a0262a39d5fe45f4b07527fdc42415533a9665264a, 43691290ac03ebb26754203f1cc3940b32f036babb7cfab3cb14fe2128389c0c
	Ransom Note Filename	README-RECOVER-[rand].txt, README-RECOVER-[rand]_2.txt, [Unique ID]-RECOVER-README.txt
<u>Meow</u>	SHA1	463554c76a0aa472daf9b42e9414942910b4ac54
	IPv4	188[.]190[.]2[.]165[::]666
<u>CMD Organization</u>	SHA1	07c14b82f673ba5caa8c1188f052ea31583f0af7
	Email	Cmd2official[@]onionmail[.]org, Cmdhtmnjksgkuhiltrh[@]onionmail[.]org, MitsueWhite[@]onionmail[.]org, JedAdams[@]onionmail[.]org
	Domain	cmdofficial[.]com
	Onion address	cmdnkiqjije2tllr3biee2sjgj3i4robg2cbtilbnytdhh2wy3syrllyd[.]onion
<u>StealC</u>	IPv4	213[.]165[.]47[.]49, 167[.]99[.]233[.]78
	URLs	hxxp[:]//213[.]165[.]47[.]49/b0c9ed38f2b14c119546[.]php, hxxp[:]//167[.]99[.]233[.]78/mbd

Attack Name	TYPE	VALUE
<u>Rhadamanthys</u>	SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9, 5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8, 6f92b2cdb8b5f68d20dbc7ca23c3a3ec78c4ef1859001940dfa22e38ce459d30, 6d240a48b5e2d1cf761a8b48b146d20729d0a7a3a557e31e75ed4c120ce71aea, c7d4e119149a7150b7101a4bd9fffbf659fba76d058f7bf6cc73c99fb36e8221, 2657fe9b88321d255fc56a81b2df4b0109ab7c525442f31765c94d75c37347aa, 124c02ed924e11b06b74e1b8c1290adbb1e50dfa2a7bcf95104c6425a1f82ef5, 3c4df2d02e4b6f4acf7b19238211892db501ee6faa04065dd11b25b56483f9c4, 9a7bc24bd814ab755a8ad67e1aeebc05ff139771928f0eae883da ff6f4ae161d, 65d6130ed7d3d822e1b08e7bed8e3adca4188d787d6805935213369c05eb2a99, b9ad234abeb1490f2c2d28dd2387f0575ba5128ebb799741b1f3179622204175, 7faeb3f847830a2c52322565d8e73e07000003ccb54310790e10756cd3b2ff6b, c7ca2f9065557a6d8fb0c02c75804d386b77ffca4466678b201c09e916afa096, a432bf6943599e53a12d5615f91fe3d636a6820073b60a7068fa9508849806b4, 30b5b1d6877df251f4007725df4e043f704d80a55b4ebd7c952b4f24b7806712, 8404cb4a740d169256e49e3a22b2af1a61b2606e71cdca4f39deeccd5d461c91, 138c86d9c22182dc809f2747d012d792ed391a84081e513c7c93d8786801d5f7, b579df3a8607cb6b251ee319bdc8c1005ca3a6ed1e360eedf2433b3f6151d856, 1d8e82d9abda58c9f4a0def2940e9f75921e2dce89a07b337a075ca363176cd4,

Attack Name	TYPE	VALUE
<u>Rhadamanthy</u> <u>S</u>	SHA256	4130ce135fbfab00618f261a0397e88479d2f61e1ed0d09ebcde525439774f3e, cc830ff08b6c66fb562a8e90c9512cadd6dbe715eb31d09e7d6afc0e9fbee68, 70debce3a545cacca8b0bdb6008945852084b36e9160424fb63479c2991dcade, a4b6a1619cf4ff65770be120cc415de1e8897c2378610171f3c48ff0fa38e9fe, 00dd5c97e86646df73973ba24085ebb32db19de258f37ed50b5c333087bb6b5c, df65e93cddf79b31b474f39477aa3038cb666965311676096d9e02a5b5cf7523, 233a2666a23ab1bae19296ee7f66ce3cdf6284db1ca4caaeb121530126419b42, d5b6cfe15a5bf959152889d8ff4fc220f0c055327c57a83c4877316af50d3a4d, f62527a0f56252621a8c7c18e0f5131bb53b4a5312dba42b4188b52345cc94a2, f9d387135a7a4e49eb96fc29d3da8f412d870417bf684b5e8ae91c4a1fbcc6d5, df66fe18ba387caa8cb295c5f35bb0a8d208ddadea7a05cef77090cc09a681b1, bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33, 6ed3ac428961b350d4c8094a10d7685578ce02c6cd41cc7f98d8eeb361f0ee38, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2, 50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2, 01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d, a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63, ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b, f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb, ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16,

Attack Name	TYPE	VALUE
<u>Rhadamanthys</u>	SHA256	fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e, a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476, 3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0, ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62, 5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9, 2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7, f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4, aae017e7a36e016655c91bd01b4f3c46309bbe540733f82cce29392e72e9bd1f
<u>AsyncRAT</u>	SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91aff20ef524, 7bb7c893fdf7f7ccd998610969d23993c50fc0b693e67930b6f98d8dbd003ee3, ecec197bee885791a9b13cd48c131eec76d8431f1907f9d55b6c9330b57a85e, 346e8e54578f206200f7815d0e315e6bfb58198b5ff96d8bcece02863e5b42cc7, 0c0b5dfb2e01c5ddd043ac32e2f7176b4ba439d4e3ea37ca04e4b17aa283d4e7, 4c6c9ec88d00a3b77e6288afc4ee9974ac07a2c73012c3e1a017c457dcf22d87, 48ee878fetc7d5d9df66fc978dfaafcfb61129acf92b1143e1b865ab292be9f0
<u>Lumma Stealer</u>	SHA256	515ad6ad76128a8ba0f005758b6b15f2088a558c7aa761c01b312862e9c1196b, dfce2d4d06de6452998b3c5b2dc33eaa6db2bd37810d04e3d02dc931887cfddd, 01a23f8f59455eb97f55086c21be934e6e5db07e64acb6e63c8d358b763dab4f, 65e1a8e550df1000eb91a7b679cf586efab0f24385b810f50349d50eb80ae806, 5eca1ecbc54d9a7b0e2e5c646578057215a246aeec2132fe7605a078aa43ec,

Attack Name	TYPE	VALUE
<u>Lumma Stealer</u>	SHA256	d0e7a341fe199dbabb5f0798dba0564e9b60e4736a405c46eafc7232cc10dc40, 8a80210b1f6382cdbff2afc0c9a30092fc13687a33f293e36a9dbc0263a45101, a90294b602b51fff7b04e72deeb3e88fb200272321c939f00e13bde1d49ff1a3, 257bcb2bac99fe5e876857ec4511cada759e7f515de629e43cbb0f839575e7fc, 8bfdd127054e1ee93f58148677961929bb9265bb6ba9648f517118c1dfca6504, 78785ab759dd61f4a9fb561faef90234fb0a78696523d1df53312c7a3eff99fe, a4ea760306249b07d5af054b5fc82d5fd9dcab5e5cb6eab3c8e8eb9132ebf882, 3d1d2e2b702d493ddaad5d7deb780ee227eb24438e68b499839a4722e212f8fb, 1be53a1bc4d191e139afb7c053b8f54af43c0338ff1eee40cd1486dfe5b787b1, d0130399fd404226ae5b90897e8e3affe29b7d34081ee1bf11ecb3750ca342c5, d932ee10f02ea5bb60ed867d9687a906f1b8472f01fc5543b06f9ab22059b264, e4d5b043f5c9e0894a5f4a21c93cd7347a609a900da8f56f55a0dd84269e81f1, ce00c5433fb2481534577e90b23e61b164654ad41c5a0f14ba59735ed637e326, 4dc5588ac49fa183824ab585b69a491fd45d1d3b2b01f052adc5062b356e7434, 984a58b77a8657d009b7867d392f320f65bb8cb72b63d9960a90f5a94721f8fb, 43d0cfce7ab2b0c2f6f89f0fa93083f46f290047cef0f75a0ae3a0b8742d84d8, de6c4c3ddb3a3ddbcbea9124f93429bf987dcd8192e0f1b4a826505429b74560, 77460056386f07d96908455241b15091c3edec9fd55fbf6ce7f3a061c7ac5cd, 3f86ca59335214a918870d86a47b21cc77f941dfcb32b7ba97620021621e7444, e63d29cda8af6ad95286c11996f0ac32a70ac24c1c2baa78d22593babd826a41, 82cb239612d74eab70b12a0ca448bd82b3c5b418b8f05213d75ddddbbf0b4a5d, ca47c8710c4ffb4908a42bd986b14cddcca39e30bb0b11ed5ca16fe8922a468b, f0668ce925f36ff7f3359b0ea47e3fa243af13cd6ad9661dfccc9ff79fb4f1cc

Attack Name	TYPE	VALUE
<u>Interlock</u>	SHA256	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaaae3a486aabdc0266e9426f, 4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9, 33dc991e61ba714812aa536821b073e4274951a1e4a9bc68f71a802d034f4fb9, b85586f95412bc69f3dceb0539f27c79c74e318b249554f0eace45f3f073c039, a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642, 0fff8fb05cee8dc4a4f7a8f23fa2d67571f360a3025b6d515f9ef37dfdb4e2ea, e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1, f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e, a68074efeee105c46bd5d86143d183c61bcf1732265f78d9f684fa82715423d3, 2f8a9258c9a5d1dfc93ea99c9990ab728595400a51aa4128f2f7254a98e03fdb, 8940ee45d67adba9c01ef415cb3a71c219799ecba55557e64867b4d8b3a50c54, 6c8efbcef3af80a574cb2aa2224c145bb2e37c2f3d3f091571708288ceb22d5f
<u>Medusa</u>	SHA256	4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6, 657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980, 7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95, 9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669, 736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270, d1e1eb0e0aaedb01df8cc2b98b0119c4aef8c1c2a3930ea0c455f0491e3161eb, c08591a1363993e2fb1fceb28168033fe66c6027531cc051c00fd82e0eb32fc8, fbf6c8f0857d888385f6bc0d46523ebcc1634e06d0e96411fc43a8ae4213d1f3, e871d8936d3b3a98d2b8dc607eadf784e1b3a20c798f3ff217d80257a67917e3, 1d009f5217c2de63ec09f5d459085a2175d5b5d2460da42257cfc52cc323f501,

Attack Name	TYPE	VALUE
<u>Medusa</u>	SHA256	5ff8acd652cc134b84213865aa3f74667c09a331cfa9affd2a2668ce78751516, 7eb39ff9ed4007b4d42dc769c8f0d8199bd8153372a07a175d884a41990839a7, 6d000a159fe10af1b29ddf4e4015931a9e9d0a020aeef0c602d8c5419b5966e6, 1bad2b6e8ab16c5a692b2d05f68f7924a73a5818ddf3a9678ca8caab3568a78e, c9abfc3e4da474e18795f5261f77e60c44e7b3353771281e4304e7506d56fdb4, 3a6d5694eec724726efa3327a50fad3efdc623c08d647b51e51cd578bddda3da, 15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10
<u>Anubis</u>	SHA256	98a76aacbaa0401bac7738ff966d8e1b0fe2d8599a266b111fdc932ce385c8ed
<u>MLTBackdoor</u>	Domains	carrolc[.]com, cwright[.]com, thomphon[.]com
	SHA256	d34e4038c5c80728f9648ba84833f69bc1ccea82e2e8e748b7b7f02fb687b92b, 9e52cc90cff150abe21f0a6440e86e0a99ff383b81061b96def8948e21d0ac66
<u>SPECTRALVIPE</u> <u>R</u>	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
<u>Sinobi</u>	SHA256	1b2a1e41a7f65b8d9008aa631f113cef36577e912c13f223ba8834bbefa4bd14, 676dc8e28c90e64000a998ec257c014cb1152e7a5bdccab3916d8fba401853da, 9432b065c803baa54f1fefac20d97affce212dec2bb9a597fc010064d391fc24, 8bb8c6e72d20e9b07bb55e0b0d168efe99d0088122131ae96d13fa01d3325a17, 82cd0af26bc1e9e3b0bfcfe6c61cf467992367a31d87e6bd7e2efa8e9fecbb25, d4919a7402d7ae02516589fbdfb3cc436749544052843a37b5d36ac4b7385b18
	File Extension	.SINOBI
	Tor Domains	sinobi7yuoppj76qnkwiobwfc2qve2xkv2ckvzyyjbldw7ucpptl62ad[.]onion/login, sinobi57mfegeov2naiufkidlkpze263jtbldokimfjqmk2mye6s4yqd[.]onion/login, sinobibjqytwqxjw24zuerqcjyd3hoow6zia7z6kzvawivamu7nqayd[.]onion/login, sinobicrh73ongfuxajmlyyhalvkhlcgttxkxaxz3gvsgdcbgf76uiqd[.]onion/login, sinobi6ftrg27d6g4sjdt65malds6cfptlnjyw52rskakqjda6uvb7yd[.]onion, sinobi6rlec6f2bgn6rd72xo7hvds4a5ajiu2if4oub2sut7fg3gomqd[.]onion, sinobi6ywgmmvg2gj2yygkb2hxbimaxpqkyk27wti5zjwhfcldhackid[.]onion, sinobi7l3wet3uqn4cagjiessuomv75aw3bvgah4jpp43od7xndb7ka d[.]onion, sinobi7sukclb3ygtorysbtrodgdbnrmgbhov45rwzipubbzhiu5jvqd[.]onion, sinobi23i75c3znmqxxyzqvhnjsar7actgvc4nqeuhgcn5yvz3zqd[.]onion, sinobia6mw6ht2wcdjphessyzpy7ph2y4dyqbd74bgobgju4ybytmk qd[.]onion
<u>INFINITERED</u>	SHA256	8f0158855a656b629ca76ebca565f18bc25563ded34b65d6771632c20edb68ec, 51a57bfc9ed3eb6451c1c289607814d59e1698c666fb97ac5f694c398f23d045

Attack Name	TYPE	VALUE
<u>INFINITERED</u>	Session ID prefix	xc32038474a
	GUID delimiter	b49e334d-9c01-463e-9bc5-00a6920fb66e
<u>DarkKomet</u>	SHA256	287cf ee849fb039c74d55222db58512d597381c3c30fbd2f1bb1a2500e9a7129
<u>Lumma</u>	SHA256	f0668ce925f36ff7f3359b0ea47e3fa243af13cd6ad9661dfccc9ff79fb4f1cc
<u>Vidar</u>	SHA256	0e90c63363265f75f8637c1a3e9ec277a1ea1a8436dd7561fff59cfb722c6612
<u>Potemkin</u>	SHA256	2abe5dd3a057fdef935722e50e9251c272d29fd26113187b853a1f9a9cb89d9b, 79f7b67ce8b39070f3e1c2b90fce0ce84134782a7dedcccc1edac197ee9e089b
<u>RMMProject</u>	SHA256	3b7ae925e2d64522b4f69b56285b05aeca8c5aab5ab46a9c02c4fafb69d881ce
<u>BabaDeda Loader</u>	SHA256	0098b2c38a69132bfde02d329d6c1c6e2b529d32d7b775a2ac78a369c0d10853, 062f019515bff366fcbf49cca3f776c21e2beb81c043a45eea81044a9391fd97
<u>Edgecution</u>	SHA256	a08d8e63b0cd3638fb40b8e6da546e26da69439597565827f9cec87915f78568, 3d1158884fb339b3328bd330fcc27598e1f1c94bcac39e75d1a272afa4deee1a
<u>Gaslight</u>	SHA256	6328567511d88fdc2ae0939c5ef17b7a63d2a833881900de018a4f12f4982525
<u>TinyRCT</u>	SHA256	4e1f8888d020decd09799ec946f1bf677cac6612b24582ddb4d8ede425d8384
<u>Prinz Eugen</u>	Domains	g-captchafestung[.]sbs, festung-e[.]duckdns[.]org
	URLs	hxxps[:]//212[.]80[.]7[.]74/serverscan[.]ps1, hxxps[:]//212[.]80[.]7[.]74/stager/mini, hxxps[:]//212[.]80[.]7[.]74/stager/ps1, hxxp[:]//stndrdbnk[.]cc

Attack Name	TYPE	VALUE
<u>Prinz Eugen</u>	Email	prinzeugen[.]mail2tor[.]co, standardbankcc[.]cock[.]li
	TOR Address	prinzfkbjiazbrur4mjje6mntjc4vydx3iatkkzycufoylqcoo4y7pqd[.]onion, 6cudc5cqa2bjpwdhcwm2lj6dbqejjjqzeo6ipwvmbazr6cgu7vfk3dad[.]onion, prinzkpn6d3itrgcytmsmlcpt5mgwn3ihpck2hsed5cezlbtti3wkliid[.]onion
	Bitcoin Address	bc1q2ztpcvqdaptej6uu2ywt9mrlatx6envu34rf0v
	Tox ID	496187425B2944D73FBB17CAF3F9FD569B9ED3A08A497A8314CB4F27A51E65081ACEE1E22F21

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

July 01, 2026 • 9:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com