

Date of Publication
March 3, 2025



HiveForce Labs
MONTHLY
THREAT DIGEST

Vulnerabilities, Attacks, and Actors

FEBRUARY 2025

Table Of Contents

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

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

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

[Celebrity Vulnerabilities](#) 06

[Vulnerabilities Summary](#)..... 08

[Attacks Summary](#)..... 11

[Adversaries Summary](#)..... 14

[Targeted Products](#)..... 15

[Targeted Countries](#)..... 18

[Targeted Industries](#)..... 19

[Top MITRE ATT&CK TTPs](#)..... 20

[Top Indicators of Compromise \(IOCs\)](#)..... 21

[Vulnerabilities Exploited](#)..... 24

[Attacks Executed](#)..... 36

[Adversaries in Action](#)..... 52

[MITRE ATT&CK TTPs](#)..... 58

[Top 5 Takeaways](#)..... 63

[Recommendations](#)..... 64

[Hive Pro Threat Advisories](#)..... 65

[Appendix](#)..... 66

[Indicators of Compromise \(IoCs\)](#)..... 67

[What Next?](#)..... 76

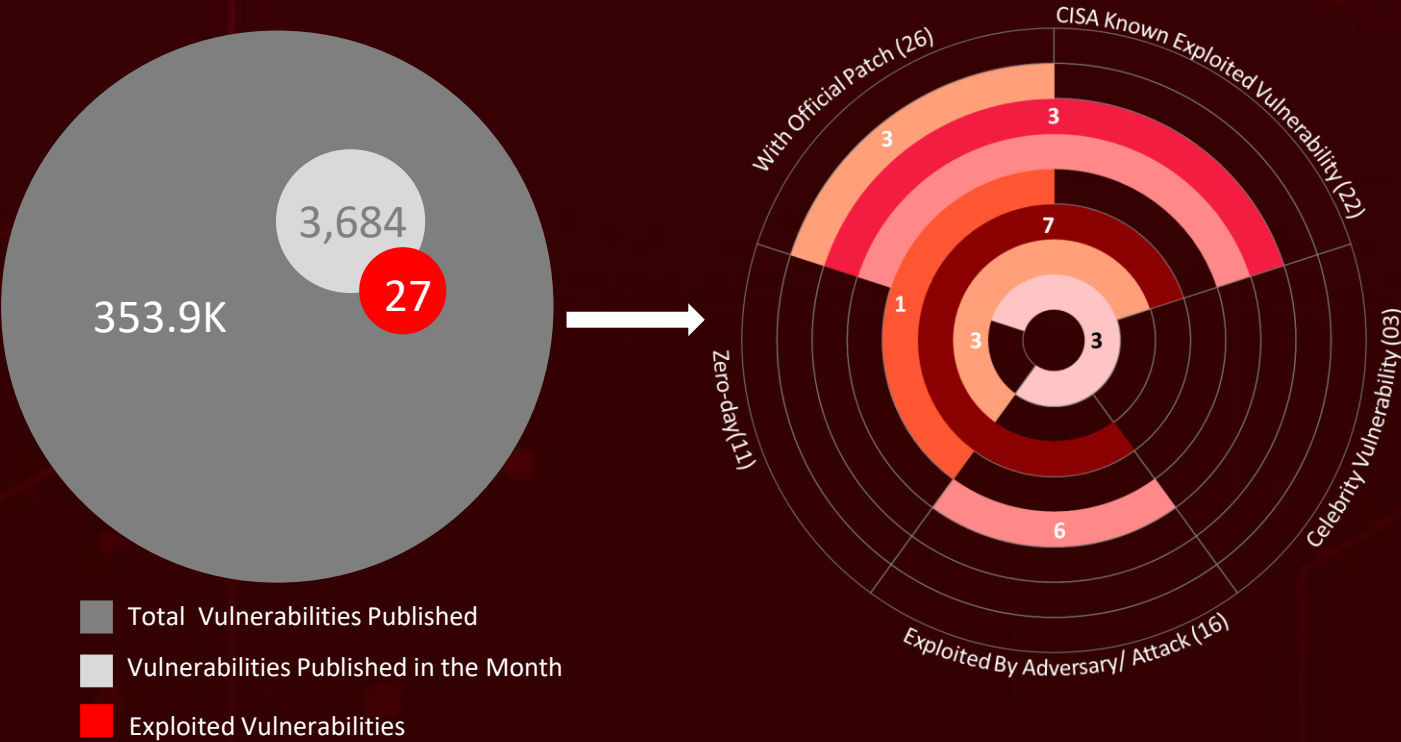
Summary

February saw the cybersecurity world on high alert after the discovery of **eleven** zero-day vulnerabilities. Among them, **CVE-2025-1094**, a critical SQL injection flaw in PostgreSQL’s interactive tool psql, stood out. Meanwhile, the **Silk Typhoon** threat group actively exploited **CVE-2024-12356** and **CVE-2024-12686** for reconnaissance and data exfiltration.

At the same time, ransomware surged, with aggressive variants like **Lynx**, **RA World**, **Vgod**, **NailaoLocker**, and **Ghost** ransomware claiming new victims. As ransomware tactics grow more sophisticated, organizations must bolster defenses with strong backup and disaster recovery strategies.

Meanwhile, North Korean threat actors launched the **Ferret** malware, targeting job seekers and developers through the "**Contagious Interview**" campaign, using fake software installations to compromise systems. A large-scale malware operation, "**StaryDobry**," has been spreading trojanized versions of cracked games such as Garry’s Mod, BeamNG.drive, and Dyson Sphere Program to unsuspecting players, delivering the **XMRig cryptominer**. The **GitVenom** campaign is also on the rise, deploying malware through fake GitHub repositories, aiming at developers and cryptocurrency users.

In parallel, **Salt Typhoon**, a Chinese state-sponsored group, has been infiltrating U.S. telecommunications providers with a stealthy custom tool, **JumbledPath**, to monitor network traffic and extract sensitive data. In many cases, attackers leveraged legitimate credentials to gain access, though one instance likely involved the exploitation of a known **Cisco vulnerability**. As cyber threats escalate, staying vigilant and proactive is more critical than ever. Organizations must continuously adapt to the evolving landscape to defend against emerging risks.



In February 2025, a geopolitical cybersecurity landscape unfolds, revealing **Vietnam, South Korea, Singapore, China, and Thailand** as the top-targeted countries

Highlighted in **February 2025** is a cyber battleground encompassing the **Government, Manufacturing, Technology, Financial Services, and Media** sectors, designating them as the top industries

Zero Trust? Not With These CVE-2025-26465 and CVE-2025-26466
OpenSSH Vulnerabilities Unpatched!

Parallels Desktop Flaw Exposes Mac Users to **Root-Level Attacks** —No Version is Safe Yet!

Microsoft's February Patch Tuesday

Tackles 63 Vulnerabilities Across Key Products, Including **Two** Zero-Days

DragonRan k's Malware Arsenal:

Using Web Shells to Manipulate Search Engine Results

Winnti Strikes Again:

Japan's Corporate Security Shaken by Massive **RevivalStone** Cyber Attack

REF7707 Cyberespionage

Campaign: A Cyber Espionage Masterpiece with Costly Mistakes

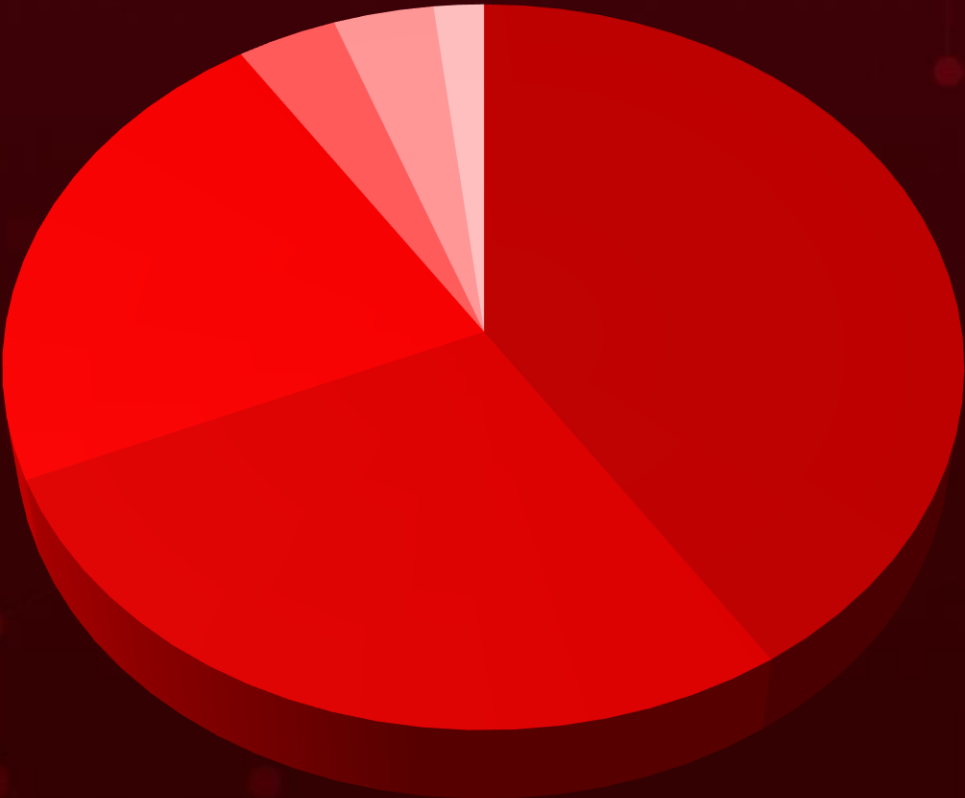
Think Before You Click:

Homoglyph Attacks Using **7-Zip Zero-Day**

Coyote Banking Trojan Strikes Brazil:

Over **70** Financial Apps at Risk!

Threat Landscape





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













Celebrity Vulnerabilities




CVE ID	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-34473</u>		Microsoft Exchange Server	-
	CISA KEY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	Ghost Ransomware
PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	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	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-34523</u>		Microsoft Exchange Server	-
	CISA KEY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	Ghost Ransomware
PROXYSHELL (Microsoft Exchange Server Privilege Escalation Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	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	ZERO-DAY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-31207</u>		Microsoft Exchange Server	-
	CISA KEY		
NAME		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	Ghost Ransomware
PROXYSHELL (Microsoft Exchange Server Security Feature Bypass Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-434	T1190: Exploit Public-Facing Application; T1556: Modify Authentication Process	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207


Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2025-0411	7-Zip Mark-of-the-Web Bypass Vulnerability	7-Zip Version Prior to 24.09			
CVE-2025-24200	Apple iOS and iPadOS Incorrect Authorization Vulnerability	Apple iOS and iPadOS			
CVE-2021-20038	SonicWall SMA 100 Appliances Stack-Based Buffer Overflow Vulnerability	SonicWall SMA			
CVE-2024-53704	SonicWall SonicOS SSLVPN Authentication Bypass Vulnerability	SonicWALL NSv devices, SonicWall SSLVPN			
CVE-2025-21377	NTLM Hash Disclosure Spoofing Vulnerability	Microsoft Windows			
CVE-2025-21391	Windows Storage Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2025-21418	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2025-21194	Microsoft Surface Security Feature Bypass Vulnerability	Microsoft Surface			
CVE-2025-0108	Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability	Palo Alto Networks PAN-OS			
CVE-2025-1094	PostgreSQL psql SQL Injection Vulnerability	PostgreSQL			
CVE-2024-12356	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability	BeyondTrust Privileged Remote Access (PRA)			
CVE-2024-12686	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability	BeyondTrust Privileged Remote Access (PRA)			


CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-0012	Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability	Palo Alto Networks PAN-OS			
CVE-2025-26465	OpenSSH VerifyHostKeyDNS Authentication Bypass Vulnerability	OpenSSH			
CVE-2018-0171	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	Cisco IOS and IOS XE Software			
CVE-2023-20198	Cisco IOS XE Web UI Privilege Escalation Vulnerability	Cisco IOS XE- All versions			
CVE-2023-20273	Cisco IOS XE Web UI Command Injection Vulnerability	Cisco IOS XE- All versions			
CVE-2024-24919	Check Point Security Gateway Information Disclosure Vulnerability	Check Point Security Gateway			
CVE-2025-24989	Microsoft Power Pages Improper Access Control Vulnerability	Microsoft Power Pages			
CVE-2018-13379	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	Fortinet FortiOS			
CVE-2010-2861	Adobe ColdFusion Directory Traversal Vulnerability	Adobe ColdFusion 9.0.1 and earlier			
CVE-2009-3960	Adobe BlazeDS Information Disclosure Vulnerability	Adobe BlazeDS 3.2 and earlier			
CVE-2021-34473	PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server			
CVE-2021-34523	PROXYSHELL (Microsoft Exchange Server Privilege Escalation Vulnerability)	Microsoft Exchange Server			
CVE-2021-31207	PROXYSHELL (Microsoft Exchange Server Security Feature Bypass Vulnerability)	Microsoft Exchange Server			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2019-0604	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint			
CVE-2024-34331	Parallels Desktop Privilege Escalation Vulnerability	Parallels Desktop for Mac			

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Coyote	Banking Trojan	-	-	-	Phishing
SmokeLoader	Loader	CVE-2025-0411	7-Zip		Exploiting Vulnerability
FlexibleFerret	Backdoor	-	-	-	Phishing
FRIENDLYFERRET	Backdoor	-	-	-	Phishing
FROSTYFERRET_UI	Backdoor	-	-	-	Phishing
MULTI_FROSTYFERRET_CMDCODES	Backdoor	-	-	-	Phishing
AsyncRAT	RAT	-	-	-	Phishing
Lynx	Ransomware	-	-	-	-
ValleyRAT	RAT	-	-	-	Social Engineering
PebbleDash	Backdoor	-	-	-	Spear phishing emails
BACKORDER	Loader	-	Windows	-	Trojanized Microsoft Key Management Service (KMS) activation tools and fake Windows Update
DarkCrystal	RAT	-	Windows	-	Deployed by BACKORDER
Kalambur	Backdoor	-	Windows	-	Fake Windows Update

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Abyss Locker	Ransomware	CVE-2021-20038	Windows, Linux, and VMware ESXi		Exploiting vulnerabilities in edge devices
PATHLOADER	Loader	-	Windows and Linux	-	-
FINALDRAFT	RAT	-	Windows and Linux	-	-
GUILoader	Loader	-	Windows and Linux	-	-
Lumma Stealer	Stealer	-	Windows	-	Phishing
RA World	Ransomware	CVE-2024-0012	Palo Alto Networks PAN-OS software		Exploiting vulnerabilities
PlugX	Backdoor	CVE-2024-0012, CVE-2024-24919	Palo Alto Networks PAN-OS, Check Point Security Gateway		Exploiting vulnerabilities
Vgod	Ransomware	-	Windows	-	Exploiting vulnerabilities
XMRig	Cryptominer	-	-	-	Trojanized games
Snake Keylogger	Keylogger	-	Windows	-	Phishing
Winnti RAT	RAT	-	-	-	Deployed by Winnti Loader
Winnti Loader	Loader	-	Windows	-	-
Winnti Rootkit	Rootkit	-	Windows	-	-
NailaoLocker	Ransomware	CVE-2024-24919	Check Point Security Gateway		Exploiting Vulnerabilities
Shadowpad	Backdoor	CVE-2024-24919	Check Point Security Gateway		Exploiting Vulnerabilities

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Ghost	Ransomware	CVE-2018-13379 CVE-2010-2861 CVE-2009-3960 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2019-0604	Fortinet FortiOS, Adobe ColdFusion 9.0.1 and earlier, Adobe BlazeDS 3.2 and earlier, Microsoft Exchange Server, Microsoft SharePoint		Exploiting Vulnerabilities in internet-facing services
FatalRAT	RAT	-	-	-	Phishing
Auto-color	Backdoor	-	Linux	-	-
Quasar RAT	RAT	-	-	-	Phishing
Winos 4.0	Malware framework	-	Microsoft Windows	-	Phishing

Adversaries Summary



ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Kimsuky	Information theft and espionage	North Korea	-	PebbleDash	-
Sandworm	Sabotage and Destruction	Russia	-	BACKORDER, DarkCrystal RAT (aka DcRAT), Kalambur backdoor	Windows
Silk Typhoon	Information theft and espionage	China	CVE-2024-12356 CVE-2024-12686	-	PostgreSQL, BeyondTrust Privileged Remote Access (PRA) and BeyondTrust Remote Support (RS)
Emperor Dragonfly	Espionage and Financial Gain	China	CVE-2024-0012	RA World ransomware (aka RA Group ransomware), PlugX	Palo Alto Networks PAN-OS software
Winnti Group	Information theft and espionage	Iran	-	Winnti RAT (aka DEPLOYLOG), Winnti Loader (also known as PRIVATELOG), Winnti Rootkit	Windows
Salt Typhoon	Information theft and espionage	China	CVE-2018-0171 CVE-2023-20198 CVE-2023-20273	-	Cisco IOS and IOS XE Software



Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	File compression software	7-Zip Version Prior to 24.09
	Proprietary software (operating systems)	Apple iPadOS Version before 17.7.5, Apple iOS and iPadOS Version before 18.3.1
	Hardware security appliances	SonicWall SMA 100 Appliances
	Network security appliances	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
	Operating System	Windows Versions 10 and 11
	Server Operating System	Windows Server 2008, 2012, 2016, 2019, 2022, 23H2 Edition (Server Core installation), 2025
	Enterprise Collaboration and Document Management System	Microsoft SharePoint Server: 2019
		Microsoft SharePoint Server Subscription Edition: All versions
		Microsoft SharePoint Enterprise Server: 2016
	Hardware (Tablet/PC)	Microsoft Surface
	Web-based Productivity Software	Office Online Server: All versions
	Productivity Software	Microsoft Office: 2019
		Microsoft Excel: 2016
	Productivity Software (Mac)	Microsoft Office LTSC: 2021 for Mac - 2024
	Cloud-Based Productivity Software	Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
	Customer Relationship Management (CRM) Software	Microsoft Dynamics 365 Sales customer relationship management (CRM) software
	Low-Code Website Development Platform	Microsoft Power Pages
	Enterprise Messaging and Collaboration Platform	Microsoft Exchange Server

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
	Firewall Operating System	Palo Alto Networks PAN-OS 10.1 versions earlier than 10.1.14-h9 PAN-OS 10.2 versions earlier than 10.2.13-h3 PAN-OS 11.1 versions earlier than 11.1.6-h1 PAN-OS 11.2 versions earlier than 11.2.4-h4 PAN-OS 11.0 (EOL) Palo Alto Networks PAN-OS Versions Prior to 11.2.4-h1, Versions Prior to 11.1.5-h1, Versions Prior to 11.0.6-h1, Versions Prior to 10.2.12-h2
	Relational Database Management System (RDBMS)	PostgreSQL Versions Before 17.3, 16.7, 15.11, 14.16, and 13.19
	Privileged Access Management (PAM) and Remote Access Solution	BeyondTrust Privileged Remote Access (PRA) Versions 24.3.1 and earlier, BeyondTrust Remote Support (RS) Versions 24.3.1 and earlier
	Secure Network Communication Protocol / Open-Source Software	OpenSSH versions 6.8p1 to 9.9p1
	Networking Operating System	Cisco IOS and IOS XE Software
	Network Security Appliances & Security Gateways	Check Point Security Gateway: CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, Quantum Spark Appliances versions: R77.20 (EOL), R77.30 (EOL), R80.10 (EOL), R80.20 (EOL), R80.20.x, R80.20SP (EOL), R80.30 (EOL), R80.30SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, R81.20
	Web Application Development Platform	Adobe ColdFusion 9.0.1 and earlier
	Server-Based Framework for Flash and Flex Applications	Adobe BlazeDS 3.2 and earlier

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
	Network Security Operating System	Fortinet FortiOS
	Desktop Virtualization Software	Parallels Desktop: All versions

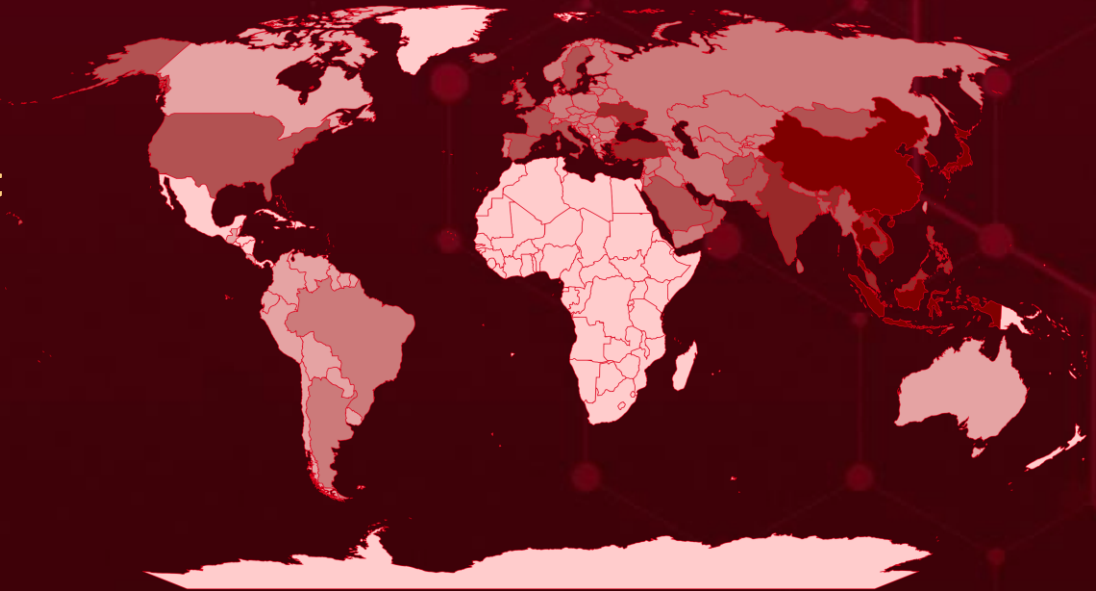


Targeted Countries

Most



Least

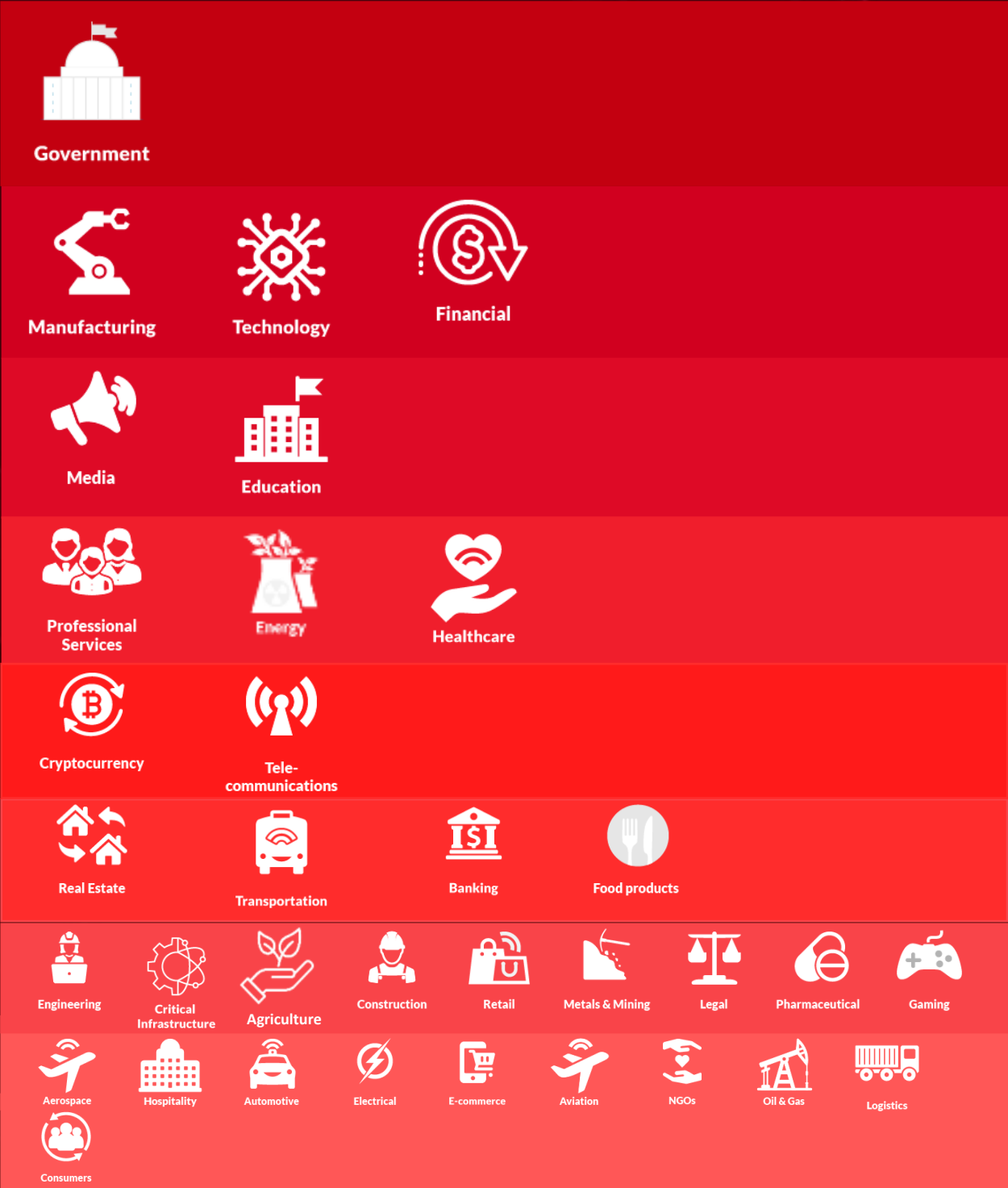


© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin
Powered by Bing

Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
	Japan		United States		Bulgaria		Andorra		Kyrgyzstan
	South Korea		Sweden		Romania		Slovenia		Ecuador
	Singapore		Bangladesh		Azerbaijan		Georgia		Suriname
	China		Oman		Iran		Iraq		Chile
	Thailand		Luxembourg		Albania		Netherlands		French Guiana
	Indonesia		Italy		Bosnia and Herzegovina		Israel		Bolivia
	Vietnam		Ireland		Croatia		Germany		Palestine
	Cambodia		Saudi Arabia		Portugal		Syria		Canada
	Philippines		Timor-Leste		Cyprus		North Macedonia		Paraguay
	Malaysia		Belgium		San Marino		Tajikistan		Colombia
	India		Bahrain		Lithuania		Norway		Peru
	Brunei		Sri Lanka		Slovakia		Brazil		Costa Rica
	Laos		Myanmar		Czech Republic		Greece		Guatemala
	Ukraine		Kuwait		Armenia		Turkmenistan		Dominica
	Turkey		Nepal		Denmark		Holy See		Guyana
	Qatar		North Korea		Taiwan		Austria		Uruguay
	Afghanistan		Maldives		Estonia		Hungary		Australia
	Spain		Mongolia		Jordan		Latvia		Venezuela
	France		United Kingdom		Malta		Uzbekistan		Jamaica
	Pakistan		Serbia		Poland		Lebanon		Barbados
	United Arab Emirates		Kazakhstan		Moldova		Yemen		Curaçao
	Bhutan		Switzerland		Iceland		Liechtenstein		Guadeloupe
					Monaco				Bahamas
					Russia				
					Finland				
					Belarus				
					Montenegro				
					Argentina				

Targeted Industries

Most



Least

TOP 25 MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1036

Masquerading

T1027

Obfuscated Files or Information

T1190

Exploit Public-Facing Application

T1204

User Execution

T1068

Exploitation for Privilege Escalation

T1566

Phishing

T1204.002

Malicious File

T1055

Process Injection

T1547

Boot or Logon Autostart Execution

T1588

Obtain Capabilities

T1071

Application Layer Protocol

T1588.006

Vulnerabilities

T1140

Deobfuscate/Decode Files or Information

T1059.001

PowerShell

T1083

File and Directory Discovery

T1082

System Information Discovery

T1497

Virtualization /Sandbox Evasion

T1560

Archive Collected Data

T1547.001

Registry Run Keys / Startup Folder

T1056

Input Capture

T1021

Remote Services

T1057

Process Discovery

T1056.001

Keylogging

T1555

Credentials from Password Stores



Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>Coyote</u>	SHA256	362af8118f437f9139556c59437544ae1489376dc4118027c24c8d5ce4d84e48, 552d53f473096c55a3937c8512a06863133a97c3478ad6b1535e1976d1e0d45f, 64209e2348e6d503ee518459d0487d636639fa5e5298d28093a5ad41390ef6b0, 67f371a683b2be4c8002f89492cd29d96dceabdbfd36641a27be761ee64605b1, 73ad6be67691b65cee251d098f2541eef3cab2853ad509dac72d8eff5bd85bc0, 839de445f714a32f36670b590eba7fc68b1115b885ac8d689d7b344189521012, bea4f753707eba4088e8a51818d9de8e9ad0138495338402f05c5c7a800695a6, f3c37b1de5983b30b9ae70c525f97727a56d3874533db1a6e3dc1355bfbf37ec, fd0ef425d34b56d0bc08bd93e6ecb11541bd834b9d4d417187373b17055c862e, 330dffe834ebbe4042747bbe00b4575629ba8f2507bccf746763cacf63d655bb, 33cba89eeef139a798b7fa07ff6919dd0c4c6cf4106b659e4e56f15b5809287
<u>AsyncRAT</u>	SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9, 5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8, 6f92b2cdb8b5f68d20dbc7ca23c3a3ec78c4ef1859001940dfa22e38ce459d30, 6d240a48b5e2d1cf761a8b48b146d20729d0a7a3a557e31e75ed4c120ce71aea, c7d4e119149a7150b7101a4bd9ffbf659fba76d058f7bf6cc73c99fb36e8221, 2657fe9b88321d255fc56a81b2df4b0109ab7c525442f31765c94d75c37347aa,

Attack Name	TYPE	VALUE
<u>AsyncRAT</u>	SHA256	124c02ed924e11b06b74e1b8c1290adbb1e50dfa2a7bcf95104c6425a1f82ef5, 3c4df2d02e4b6f4acf7b19238211892db501ee6faa04065dd11b25b56483f9c4, 9a7bc24bd814ab755a8ad67e1aeebc05ff139771928f0eae883daff6f4ae161d, 65d6130ed7d3d822e1b08e7bed8e3adca4188d787d6805935213369c05eb2a99
<u>Lynx</u>	Domain	hxxp[:]//lynxblog[.]net
	Email	martina[.]lestariid1898[@]proton[.]me
	SHA256	571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b, eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc, 80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441, 3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eaed044e, 97c8f54d70e300c7d7e973c4b211da3c64c0f1c95770f663e04e35421dfb2ba0, 468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a
<u>Abyss Locker</u>	SHA256	05b82d46ad331cc16bdc00de5c6332c1ef818df8ceefcd49c726553209b3a0da, 6042a84529958a04a2d46384139da3ef016bf9498e791cd5e34dfece2baa1d2, 3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71, 5fba25759423f9efc92592977f6c9ff77d47a20aa8ec8e9cd17d5cfa786a1852, cd9d88cccd85209966c5a35aba7751b962bcc021a4216d6addfc0c3462ce80da, f9ab649acfe76d6ac088461b471e5d981bdc8b71d940e94c63bc1988a2ed4678, 5f9dfd9557cf3ca96a4c7f190fc598c10f8871b1313112c9aea45dc8443017a2, d48c7f13db60ef615e59773c442485e84acef09343375d0d8a462b285e959baa, d76c74fc7a00a939985ae515991b80afa0524bf0a4feaec3e5e58e52630bd717, 0d9089efe2a28630bc21d8db451ec14dc856c2d40444292c42e7cca218c7029e
	SHA1	59a97f9d7c1d6e10fa41ea9339568fb25ec55e27, 3f90fd241e9422cc447b5ccdc8b7d72507f37e6f, 23873bf2670cf64c2440058130548d4e4da412dd, e44ec82d0d80c754afcd7ed149c263c55d158259,




Attack Name	TYPE	VALUE
<u>Abyss Locker</u>	SHA1	13112e672d807fa7c7f8a383ecfa31e85b880e5a, f24ca204af2237a714e8b41d54043da7bbe5393b, 17d9200843fe0eb224644a61f0d1982fac54d844, 82780c0c1c0e04d994c770a3b3e73727528b0451
	File Path	C:\users\<USER>\appdata\roaming\microsoft\wmi\wmihelper.exe, C:\WINDOWS\system32\config\systemprofile\AppData\Roaming\Microsoft\Wmi\wmihelper.exe, /bin/apache2, C:\Windows\uFmAnlZR.exe, /tmp/e.elf, C:\Users\<USER>\Desktop\e\e.exe, C:\Windows\System32\rclone, C:\Windows\System32\LTSSVC.exe, C:\Windows\System32\filter.txt, C:\Windows\Temp\SophosAV.exe, C:\ProgramData\USOShared\auSophos.exe, C:\ProgramData\USOShared\UpdateSvc.exe, C:\programdata\pr.exe, C:\ProgramData\deploy443.ps1, C:\ProgramData\USOShared\UpdateDrv.sys
	TOR Address	3ev4metjirohtdpshsqlkrqcmxq6zu3d7obrdhglpy5jpbr7whmlfgqd[.]onion
	File Name	wmihelper.xml, wmihelper.key, veeam11.ps1, ped.sys, 3ware.sys
	Host Name	DESKTOP-VM4QKN6, ADMINIS-F69E5L3
	IPv4	139[.]180[.]135[.]191, 67[.]217[.]228[.]101, 64[.]95[.]12[.]57, 64[.]95[.]12[.]70, 149[.]137[.]142[.]15
<u>Ghost Ransomware</u>	MD5	c5d712f82d5d37bb284acd4468ab3533, 34b3009590ec2d361f07cac320671410, d9c019182d88290e5489cdf3b607f982, 29e44e8994197bdb0c2be6fc5dfc15c2, c9e35b5c1dc8856da25965b385a26ec4, d1c5e7b8e937625891707f8b4b594314, ef6a213f59f3fbee2894bd6734bbaed2, ac58a214ce7deb3a578c10b97f93d9c3, c3b8f6d102393b4542e9f951c9435255, 0a5c4ad3ec240fbfd00bdc1d36bd54eb, ff52fdf84448277b1bc121f592f753c5, a2fd181f57548c215ac6891d000ec6b9, 625bd7275e1892eac50a22f8b4a6355d, db38ef2e3d4d8cb785df48f458b35090









Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-0411</u>		7-Zip Version Prior to 24.09	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:7-zip:7-zip:*:*:*:*:*:*	SmokeLoader
7-Zip Mark-of-the-Web Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1059: Command and Scripting Interpreter; T1553.005: Mark-of-the-Web Bypass	https://www.7-zip.org/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-24200</u>		Apple iPadOS Version before 17.7.5, Apple iOS and iPadOS Version before 18.3.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:ipados:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*	-
Apple iOS and iPadOS Incorrect Authorization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1068: Exploitation for Privilege Escalation	https://support.apple.com/en-us/118575




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-20038</u>		SonicWall SMA 200, 210, 400, 410 and 500v appliances firmware 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier versions.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:sonicwall:sma_200_firmware:-:*:*:*:*:*:*	Abyss Locker Ransomware
SonicWall SMA 100 Appliances Stack-Based Buffer Overflow Vulnerability		cpe:2.3:h:sonicwall:sma_200:-:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787 CWE-121	T1574: Hijack Execution Flow, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026
CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<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:*:*:*:*:*:*	-
SonicWall SonicOS SSLVPN Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1556: Modify Authentication Process, T1133: External Remote Services, T1068: Exploitation for Privilege Escalation	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-21377</u>		Windows 10, 11 Windows Server 2008, 2012, 2016, 2019, 2022, 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows :*:*:*:*:*:*:*	-
NTLM Hash Disclosure Spoofing Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1187: Forced Authentication	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21377




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-21391</u>		Windows 10, 11 Windows Server 2016, 2019, 2022, 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows :*:*:*:*:*:*:*	-
Windows Storage Elevation of Privilege Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-59	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21391




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-21418</u>		Windows Server 2008, 2012, 2016, 2019, 2022, 2025 Windows 10, 11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows :*:*:*:*:*:*:*	-
Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21418




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-21194</u>		Microsoft Surface	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:surface:- :*:*:*:*:*:*:	-
Microsoft Surface Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1499: Endpoint Denial of Service, T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21194




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-12356</u>		BeyondTrust Privileged Remote Access (PRA) Versions 24.3.1 and earlier, BeyondTrust Remote Support (RS) Versions 24.3.1 and earlier	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*	-
BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability		cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation, T1133 : External Remote Services	https://www.beyondtrust.com/trust-center/security-advisories/bt24-10




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-0012</u>		Palo Alto Networks PAN-OS Versions Prior to 11.2.4-h1, Versions Prior to 11.1.5-h1, Versions Prior to 11.0.6-h1, Versions Prior to 10.2.12-h2	Emperor Dragonfly
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*	RA World ransomware, PlugX
Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1556: Modify Authentication Process	https://security.paloaltonetworks.com/CVE-2024-0012




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-12686		BeyondTrust Privileged Remote Access (PRA) Versions 24.3.1 and earlier, BeyondTrust Remote Support (RS) Versions 24.3.1 and earlier	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*	-
BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability		cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation, T1133 : External Remote Services	https://www.beyondtrust.com/trust-center/security-advisories/bt24-11




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-26465		OpenSSH versions 6.8p1 to 9.9p1, Red Hat, SUSE, Debian, Fedora, ALT Linux, Ubuntu	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:openssh:openssh:*:*:*:*:*:*:	-
OpenSSH VerifyHostKeyDNS Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-390	T1203: Exploitation for Client Execution T1656: Impersonation	https://security-tracker.debian.org/tracker/CVE-2025-26465




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-20273</u>		Cisco IOS XE- All versions	Salt Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*	-
Cisco IOS XE Web UI Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20 CWE-787	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-24919</u>		Check Point Security Gateway	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:checkpoint:quantum_gateway:*:*:*:*:*.*	NailaoLocker Ransomware, Shadowpad, PlugX
Check Point Security Gateway Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1133: External Remote Services, T1212: Exploitation for Credential Access	https://support.checkpoint.com/results/sk/sk182336

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2010-2861</u>		Adobe ColdFusion 9.0.1 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:coldfusion:*:*:*:*:*:*	Ghost Ransomware
Adobe ColdFusion Directory Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application; T1083: File and Directory Discovery	https://helpx.adobe.com/security/security-bulletin.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2009-3960</u>		Adobe BlazeDS 3.2 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:blazeds:*:*:*:*:*	Ghost Ransomware
Adobe BlazeDS Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1190: Exploit Public-Facing Application; T1005: Data from Local System	https://helpx.adobe.com/security/security-bulletin.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2019-0604</u>		Microsoft SharePoint	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*	Ghost Ransomware
Microsoft SharePoint Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0604

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-34331</u>		Parallels Desktop: All versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:parallels:desktop:19.0:*:*:*:*:*	-
Parallels Desktop Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	MITIGATION LINK
	CWE-269	T1068: Exploitation for Privilege Escalation; T1553: Subvert Trust Controls; T1059: Command and Scripting Interpreter	https://www.parallels.com/products/desktop/download/ https://kb.parallels.com/129860

⚔ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Coyote</u>	The Coyote Banking Trojan is a stealthy and highly capable malware designed to steal sensitive financial data. It can log keystrokes, take screenshots, and deploy phishing overlays to harvest login credentials. Targeting over 70 financial applications and more than 1,000 websites, Coyote operates through a multi-stage attack chain. It typically begins with malicious LNK files, which execute hidden PowerShell commands to initiate infection, ensuring a covert and persistent presence on compromised systems.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Banking Trojan		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>SmokeLoader</u>	SmokeLoader is a versatile malware loader designed to deploy additional threats on infected systems while offering optional modules for information stealing. It frequently obscures its C2 traffic by generating requests to legitimate websites, making detection more challenging. Once installed, SmokeLoader can deliver various payloads, including cryptominers, ransomware, and password stealers. Beyond deploying malware, it may also exfiltrate sensitive data, corrupt files, and disrupt system operations, posing a significant risk to compromised devices.	Exploiting Vulnerability	CVE-2025-0411
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Data Theft, System compromise and Espionage	7-Zip
ASSOCIATED ACTOR			PATCH LINK
-			https://www.7-zip.org/

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FlexibleFerret	FlexibleFerret, part of the macOS Ferret malware family, is a stealthy backdoor designed to evade Apple's XProtect and maintain persistence on infected devices. It disguises itself as a legitimate system process, embedding itself in the User's Library LaunchAgents folder to ensure it runs at startup. The malware communicates with a fraudulent Zoom domain, potentially delivering additional payloads for data theft and remote access.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FRIENDLYFERRET	FRIENDLYFERRET, part of the macOS Ferret malware family, is a stealthy backdoor that disguises itself as a legitimate system file under the name com.apple.secd, alongside a fake ChromeUpdate process. By blending in with macOS system components, it evades detection while maintaining persistent access to compromised devices.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FROSTYFERRET_UI	FROSTYFERRET_UI, part of the macOS Ferret malware family, is a persistence module designed to maintain long-term access to infected systems. Masquerading as a CameraAccess component, it ensures stealthy operation while potentially enabling surveillance capabilities.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MULTI_FROSTYFERRET_CMDCODES	MULTI_FROSTYFERRET_CMDCODE is a stealthy backdoor which is a part of the macOS Ferret malware family.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AsyncRAT	AsyncRAT is a malware known malicious activities since 2019. It can log keystrokes, transfer files, and gain remote desktop control, providing attackers with extensive access to the infected system.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Information Theft, Espionage	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Lynx	Lynx is a fast-evolving Ransomware-as-a-Service (RaaS) operation that uses a ruthless double-extortion tactic encrypting victims’ data while leveraging stolen information for added pressure. Built for multi-platform attacks, it targets Windows, Linux, and ESXi systems, employing advanced encryption and disruptive techniques like shutting down virtual machines. To maximize damage, Lynx not only locks files but also disables critical recovery options, such as shadow copies and volume snapshots, making system restoration nearly impossible.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>ValleyRAT</u>	ValleyRAT, a remote access trojan (RAT) first identified in 2023, has evolved with a sophisticated multi-stage infection process and advanced evasion techniques to maintain long-term access to compromised systems. The malware is spread through fake websites that mimic legitimate sources, including deceptive Google Chrome download pages. ValleyRAT includes features like screenshot capture, process filtering, forced reboots or shutdowns, and Windows event log deletion. In its latest campaign, attackers have escalated their tactics by creating a fraudulent website impersonating a Chinese telecom company.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PebbleDash</u>	PebbleDash is a stealthy backdoor delivered via spear-phishing email attachments, granting attackers remote control over compromised systems. Once installed, it connects to a command-and-control (C&C) server, awaiting instructions to execute various malicious tasks. These include managing processes and files, as well as downloading and uploading data, enabling threat actors to manipulate the system at will. Through PebbleDash, attackers can establish persistent access, posing a significant risk to affected organizations.	spear phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>BACKORDER</u>	The GO-based loader "BACKORDER" operates silently in the background, allowing malicious activities to unfold without detection by Windows Defender. It disables Windows Defender and creates exclusion rules for specific folders, further evading detection.	Trojanized Microsoft Key Management Service (KMS) activation tools and fake Windows Update	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Exfiltration of Data, Malware delivery	Windows
Loader			PATCH LINK
ASSOCIATED ACTOR			
Sandworm			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>DarkCrystal (aka DCRat)</u>	DCrat, also known as Dark Crystal RAT, is a remote access trojan (RAT) first discovered in 2018. This modular malware can be tailored to execute various malicious actions, such as stealing passwords, accessing cryptocurrency wallet information, and hijacking Telegram and Steam accounts.	Deployed by BACKORDER	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Exfiltration of Data, Account Hijacking, System Compromise	Windows
RAT			PATCH LINK
ASSOCIATED ACTOR			
Sandworm			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Kalambur</u>	Kalambur is a C#-based backdoor and downloader crafted to retrieve a repackaged TOR binary within a ZIP file. It subsequently downloads additional malicious tools from what appears to be an attacker-controlled TOR onion site.	Fake Windows Update	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Remote Access, Malware delivery, Exfiltration of Data	Windows
ASSOCIATED ACTOR			PATCH LINK
Sandworm			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Abyss Locker (aka AbyssLocker)</u>	Abyss Locker is a ransomware group that surfaced in 2023 and quickly escalated it cyberattacks through 2024 and into 2025. The group utilizes advanced tactics to breach corporate networks, exfiltrate sensitive data, and encrypt systems, with a particular focus on critical network devices, such as VMware ESXi servers.	Exploiting vulnerabilities in edge devices	CVE-2021-20038
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Exfiltration of Data, Financial Loss, Reputation Damage	Windows, Linux and VMware ESXi
ASSOCIATED ACTOR			PATCH LINK
-			https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PATHLOADER</u>	PATHLOADER is a compact Windows PE file, just 206 kilobytes in size, that downloads and executes encrypted shellcode from an external server. This lightweight executable facilitates the retrieval and execution of malicious code hosted on remote infrastructure.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Malware Delivery, Exfiltration of Data	Windows and Linux
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>FINALDRAFT</u>	FINALDRAFT is a 64-bit malware written in C++ designed for data exfiltration and process injection. It contains additional modules, part of the FINALDRAFT toolkit, which can be injected into targeted processes. The collected data from these modules is then transmitted to the command-and-control (C2) server.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Remote Control, Exfiltration of Data	Windows and Linux
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>GUILOADER</u>	GUIDLOADER is a novel malware loader recently observed in the REF7707 cyber-espionage campaign. It is designed to deploy additional malicious payloads on compromised systems, enabling further exploitation and persistence.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Malware Deployment, System Compromise	Windows and Linux
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Lumma Stealer</u>	Lumma stealer, previously known as LummaC2, is a subscription-based information stealer that has been active since 2022. This malware primarily targets cryptocurrency wallets, browser extensions, and two- factor authentication (2FA) mechanisms. Its main objective is to steal sensitive information from compromised machines, posing a significant threat to users' financial and personal data.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Data theft	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>RA World ransomware</u>	RA World ransomware active since late 2023, has targeted over 20 organizations globally, primarily in manufacturing and healthcare sectors. They employ a multi-extortion strategy, exfiltrating sensitive data before encryption to pressure victims into paying ransoms. Notably, recent attacks have utilized tools associated with Chinese cyber espionage groups, suggesting possible overlaps between espionage and financially motivated activities.	Exploiting vulnerabilities	CVE-2024-0012
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data encryption and Data Exfiltration	Palo Alto Networks PAN-OS software
ASSOCIATED ACTOR			PATCH LINK
Emperor Dragonfly			https://security.paloaltonetworks.com/CVE-2024-0012

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PlugX</u>	PlugX, a backdoor linked to China-based espionage groups like Mustang Panda, enables remote access, data exfiltration, and command execution. Recent attacks show its use alongside RA World ransomware, indicating a shift toward financially motivated cybercrimes.	Exploiting vulnerabilities	CVE-2024-0012, CVE-2024-24919
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data collection and Espionage	Palo Alto Networks PAN-OS, Check Point Security Gateway
ASSOCIATED ACTOR			PATCH LINK
Emperor Dragonfly			https://security.paloaltonetworks.com/CVE-2024-0012 , https://support.checkpoint.com/results/sk/sk182336

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Vgod Ransomware</u>	Vgod is a newly identified ransomware variant that targets Windows systems, encrypting files and appending the ".Vgod" extension. This malware employs a double extortion tactic encrypting files while stealing sensitive data leaving victims with the grim choice of paying a ransom or risking a data leak.	Exploiting vulnerabilities	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data encryption and Data Exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>XMRig</u>	XMRig is an open-source cryptocurrency mining software primarily used for mining Monero (XMR). While it has legitimate uses, cybercriminals often deploy it in cryptojacking attacks, secretly using victims' computing resources to mine cryptocurrency.	Trojanized games	-
TYPE		IMPACT	AFFECTED PRODUCTS
Cryptominer		Resource drain, Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Snake Keylogger</u> <u>(aka 404 Keylogger)</u>	Snake Keylogger is a stealthy malware that captures keystrokes, credentials, and other sensitive data from infected systems. Recent variants have evolved to evade detection, making it a persistent cybersecurity threat. It's actively targeting Windows users across China, Turkey, Indonesia, Taiwan, and Spain. This persistent malware has already triggered over 280 million blocked infection attempts, underscoring its widespread impact.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	Windows
Keylogger			PATCH LINK
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Winnti RAT</u> <u>(aka DEPLOYLOG)</u>	Winnti RAT is a remote access Trojan used by the Winnti Group to maintain persistence and execute commands on compromised systems. It enables data exfiltration, credential theft, and lateral movement within networks. The malware is often deployed via ERP vulnerabilities or supply chain attacks, posing risks to intellectual property.	Winnti Loader	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Data Theft and Data Exfiltration	-
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Winnti Loader (aka PRIVATELOG)	Winnti Loader is a stealthy malware loader designed to execute second-stage payloads while evading detection. It uses obfuscation techniques such as encrypted logs and DLL sideloading to deploy additional malware, including backdoors and keyloggers. The loader is frequently used in targeted attacks against critical industries.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Malware Deployment	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Winnti Rootkit	Winnti Rootkit is an advanced persistence tool that allows attackers to hide malicious activities and maintain long-term access to infected systems. It operates at the kernel level, intercepting system calls and bypassing security mechanisms. This rootkit is primarily used in espionage campaigns targeting high-value corporate and government networks.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Rootkit		Stealthy access and Persistence	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>NailaoLocker Ransomware</u>	NailaoLocker is a ransomware distributed by the Green Nailao threat cluster, primarily targeting European healthcare organizations via ShadowPad and PlugX backdoors. It uses AES-256-CTR encryption, appending a ".locked" extension to encrypted files, and demands ransom via a Proton email address.	Exploiting Vulnerabilities	CVE-2024-24919
		IMPACT	AFFECTED PRODUCTS
TYPE		Data encryption	Check Point Security Gateway
Ransomware			PATCH LINK
ASSOCIATED ACTOR			https://support.checkpoint.com/results/sk/sk182336
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>ShadowPad</u>	ShadowPad is a modular backdoor malware linked to Chinese state-sponsored threat groups, used for espionage and cybercrime. It provides remote access, keylogging, data exfiltration, and the ability to deploy additional payloads like ransomware. Initially discovered in supply chain attacks, it remains a persistent threat to critical industries worldwide.	Exploiting Vulnerabilities	CVE-2024-24919
		IMPACT	AFFECTED PRODUCTS
TYPE		Remote access and Data exfiltration	Check Point Security Gateway
Backdoor			PATCH LINK
ASSOCIATED ACTOR			https://support.checkpoint.com/results/sk/sk182336
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Ghost Ransomware</u>	<p>Ghost ransomware surfaced in early 2021, rapidly gaining attention for targeting exposed internet services by exploiting known security vulnerabilities. The group behind it, suspected to be based in China, frequently modified their ransomware payloads, changed file extensions for encrypted files, altered ransom note texts, and used various email addresses to avoid identification.</p>	Exploiting Vulnerabilities in internet-facing services	CVE-2018-13379 CVE-2010-2861 CVE-2009-3960 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2019-0604
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Financial Losses, Operational Disruption, Reputational Damage	Fortinet FortiOS, Adobe ColdFusion 9.0.1 and earlier, Adobe BlazeDS 3.2 and earlier, Microsoft Exchange Server, Microsoft SharePoint
ASSOCIATED ACTOR			PATCH LINK https://www.fortiguard.com/psirt/FG-IR-18-384 https://helpx.adobe.com/coldfusion/kb/coldfusion-security-hot-fix-bulletin.html 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0604
-			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
FatalRAT	FatalRAT, a remote access Trojan (RAT), enables persistent access for attackers. They exploit legitimate Chinese cloud services, such as myqcloud CDN and Youdao Cloud Notes, to conceal their infrastructure and avoid detection. Through a multi-stage payload delivery, they silently deploy malware, bypassing security defenses. FatalRAT provides attackers with full control over compromised systems, allowing keystroke logging, data theft, and remote command execution.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Persistent Access, Data Theft, Bypassing Security Defenses	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
-			


NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Auto-color	A new Linux malware strain, Auto-color, is named after the filename it adopts upon installation. Auto-color provides attackers with complete remote control over compromised systems. The malware integrates seamlessly into the system, resisting deletion. If the user lacks root privileges, it halts installation to avoid detection. However, when executed with elevated privileges, it installs a malicious library that mimics a legitimate system library to remain undetected.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Remote Control, Persistent Presence	Linux
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
-			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Quasar RAT</u>	Quasar RAT is a .NET-based malware family employed by various threat actors. Fully functional and open-source, it is frequently packed to complicate source code analysis.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Remote Control and Surveillance, System Disruption	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
-			


NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Winos 4.0</u>	Winos4.0 malware steals sensitive data, which can be used for subsequent attacks. A secondary attack chain has been discovered, deploying an online module capable of capturing screenshots from WeChat and online banking platforms.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft, Compromise of Sensitive Platforms	Microsoft Windows
Malware framework			PATCH LINK
ASSOCIATED ACTOR			-
-			


Adversaries in Action


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Kimsuky (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394, Sparkling Pisces, Springtail)</u>	North Korea	Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks and Ministry of Unification, Sejong Institute and Korea Institute for Defense Analyses, Business, Cryptocurrency	South Korea, United States, Japan, Russia, Vietnam and European nations
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	-	PebbleDash	-


TTPs


TA0043: Reconnaissance; TA0011: Command and Control; TA0010: Exfiltration; TA0005: Defense Evasion; TA0004: Privilege Escalation; TA0003: Persistence; TA0002: Execution; TA0001: Initial Access; T1620: Reflective Code Loading; T1592: Gather Victim Host Information; T1590: Gather Victim Network Information; T1590.005: IP Addresses; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1218.005: Mshta; T1217: Browser Information Discovery; T1204: User Execution; T1204.002: Malicious File; T1140: Deobfuscate/Decode Files or Information; T1132: Data Encoding; T1112: Modify Registry; T1102: Web Service; T1090: Proxy; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1056: Input Capture; T1056.001: Keylogging; T1055: Process Injection; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1036: Masquerading; T1036.007: Double File Extension; T1027: Obfuscated Files or Information; T1027.010: Command Obfuscation; T1021: Remote Services

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRY
 <p><u>Sandworm (aka Sandworm Team, Iron Viking, CTG-7263, Voodoo Bear, Quedagh, TEMP.Noble, ATK 14, BE2, UAC-0082, UAC-0113, UAC-0125, FROZENBARENTS, IRIDIUM, Seashell Blizzard, APT 44)</u></p>	Russia	Critical Infrastructure, Government	Ukraine
	MOTIVE		
	Sabotage and Destruction		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	BACKORDER, DarkCrystal RAT (aka DcRAT), Kalambur backdoor	Windows
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1569: System Services; T1569.002: Service Execution; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1070: Indicator Removal; T1070.004: File Deletion; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1056: Input Capture; T1056.001: Keylogging; T1082: System Information Discovery; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1021.004: SSH; T1113: Screen Capture; T1005: Data from Local System; T1090: Proxy; T1090.003: Multi-hop Proxy; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel; T1036: Masquerading			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
<div></div> <div><u>Silk Typhoon (aka Hafnium, Red Dev 13, ATK233, G0125)</u></div>	China	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACK S/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-12356 CVE-2024-12686	-	-
TTPs			
TA0043: Reconnaissance, TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, T1588: Obtain Capabilities, T1588.006: Vulnerabilities, T1588.005: Exploits, T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1133: External Remote Services			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Emperor Dragonfly (aka Bronze Starlight, DEV-0401, Cinnamon Tempest, SLIME34, SLIME34)</u></p>	China	Government banks, think tanks, embassies, legal entities	Europe, Asia
	MOTIVE		
	Espionage and Financial Gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-0012	RA World ransomware (aka RA Group ransomware), PlugX	Palo Alto Networks PAN-OS software
TTPs			
TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0007: Discovery, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, TA0006: Credential Access, TA0009: Collection, T1083: File and Directory Discovery, T1490: Inhibit System: Recovery, T1552: Unsecured Credentials, T1560: Archive Collected Data, T1573: Encrypted Channel, T1496: Resource Hijacking, T1203: Exploitation for Client Execution, T1055.001: Dynamic-link Library Injection, T1055: Process Injection, T1105: Ingress Tool Transfer, T1555: Credentials from Password Stores, T1027: Obfuscated Files or Information, T1036: Masquerading, T1486: Data Encrypted for Impact			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Winnti Group (aka APT 41, Blackfly, Wicked Panda)</u></p>	Iran	Manufacturing, Materials, Energy	Japan
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	Winnti RAT (aka DEPLOYLOG), Winnti Loader (also known as PRIVATELOG), Winnti Rootkit	Windows
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, T1190: Exploit Public-Facing Application, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell, T1505: Server Software: Component, T1505.003: Web Shell, T1574: Hijack Execution Flow, T1574.001: DLL Search Order Hijacking, T1547: Boot or Logon Autostart Execution, T1547.006: Kernel Modules and Extensions, T1543: Create or Modify System Process, T1543.003: Windows Service, T1078: Valid Accounts, T1078.002: Domain Accounts, T1014: Rootkit: T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1070: Indicator Removal, T1070.004: File Deletion, T1016: System Network Configuration Discovery, T1018: Remote System Discovery, T1201: Password Policy Discovery, T1069: Permission Groups Discovery, T1135: Network Share Discovery, T1007: System Service Discovery, T1049: System Network Connections Discovery, T1033: System Owner/User Discovery, T1082: System Information Discovery, T1120: Peripheral Device Discovery, T1021: Remote Services, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares, T1560: Archive Collected Data, T1560.001: Archive via Utility, T1588.004: Digital Certificates			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Salt Typhoon (aka GhostEmperor, UNC2286, FamousSparrow, Earth Estries, RedMike)</u></p>	China	Telecommunication	United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2018-0171 CVE-2023-20198 CVE-2023-20273	-	-
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0010: Exfiltration, TA0011: Command and Control, T1588: Obtain Capabilities, T1588.006: Vulnerabilities, T1555: Credentials from Password Stores, T1555.003: Credentials from Web Browsers, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1600: Weaken Encryption, T1027: Obfuscated Files or Information, T1556: Modify Authentication Process, T1016: System Network Configuration Discovery, T1222: File and Directory Permissions Modification, T1190: Exploit Public-Facing Application, T1021: Remote Services, T1021.004: SSH, T1068: Exploitation for Privilege Escalation, T1584: Compromise Infrastructure, T1105: Ingress Tool Transfer			

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1592: Gather Victim Host Information	
	T1590: Gather Victim Network Information	T1590.005: IP Addresses
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1588: Obtain Capabilities	T1588.004: Digital Certificates
		T1588.005: Exploits
		T1588.006: Vulnerabilities
	T1584: Compromise Infrastructure	
	T1586: Compromise Accounts	T1586.002: Email Accounts
TA0001: Initial Access	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1091: Replication Through Removable Media	
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1566: Phishing	T1566.001: Spear-phishing Attachment
		T1566.002: Spear-phishing Link
TA0002: Execution	T1047: Windows Management Instrumentation	
	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
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1106: Native API	
	T1204: User Execution	T1204.002: Malicious File
	T1569: System Services	T1569.002: Service Execution
	T1129: Shared Modules	
TA0003: Persistence	T1203: Exploitation for Client Execution	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1505: Server Software Component	T1505.003: Web Shell
	T1098: Account Manipulation	
	T1133: External Remote Services	
	T1136: Create Account	T1136.001: Local Account
		T1136.002: Domain Account
	T1542: Pre-OS Boot	T1542.003: Bootkit
	T1543: Create or Modify System Process	T1543.003: Windows Service

Tactic	Technique	Sub-technique
TA0003: Persistence	T1556: Modify Authentication Process	
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.006: Kernel Modules and Extensions
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
TA0004: Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1098: Account Manipulation	
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1543: Create or Modify System Process	T1543.003: Windows Service
		T1548.002: Bypass User Account Control
	T1548: Abuse Elevation Control Mechanism	T1548.004: Elevated Execution with Prompt
		T1055.001: Dynamic-link Library Injection
		T1055.002: Portable Executable Injection
	T1055: Process Injection	T1055.012: Process Hollowing
		T1547.001: Registry Run Keys / Startup Folder
		T1547.006: Kernel Modules and Extensions
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
TA0005: Defense Evasion	T1014: Rootkit	
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.010: Command Obfuscation
	T1036: Masquerading	T1036.003: Rename System Utilities
		T1036.005: Match Legitimate Name or Location
		T1036.007: Double File Extension
		T1036.008: Masquerade File Type
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
		T1055.002: Portable Executable Injection
		T1055.012: Process Hollowing
	T1070: Indicator Removal	T1070.004: File Deletion
	T1078: Valid Accounts	T1078.002: Domain Accounts

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1112: Modify Registry	
	T1140: Deobfuscate/Decode Files or Information	
	T1202: Indirect Command Execution	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.005: Mshta
		T1218.010: Regsvr32
		T1218.011: Rundll32
	T1542: Pre-OS Boot	T1542.003: Bootkit
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1222: File and Directory Permissions Modification	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.012: Disable or Modify Linux Audit System
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
		T1548.004: Elevated Execution with Prompt
	T1556: Modify Authentication Process	
	T1600: Weaken Encryption	
	T1620: Reflective Code Loading	
	T1553: Subvert Trust Controls	T1553.002: Code Signing
		T1553.005: Mark-of-the-Web Bypass
	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
		T1574.002: DLL Side-Loading
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
	T1656: Impersonation	
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.002: Security Account Manager
	T1040: Network Sniffing	
	T1212: Exploitation for Credential Access	
	T1556: Modify Authentication Process	
	T1056: Input Capture	T1056.001: Keylogging
		T1056.004: Credential API Hooking
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers

Tactic	Technique	Sub-technique
TA0007: Discovery	T1007: System Service Discovery	
	T1010: Application Window Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1040: Network Sniffing	
	T1046: Network Service Discovery	
	T1049: System Network Connections Discovery	
	T1057: Process Discovery	
	T1069: Permission Groups Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1120: Peripheral Device Discovery	
	T1135: Network Share Discovery	
	T1201: Password Policy Discovery	
	T1217: Browser Information Discovery	
	T1614: System Location Discovery	T1614.001: System Language Discovery
	T1087: Account Discovery	T1087.002: Domain Account
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1518: Software Discovery	T1518.001: Security Software Discovery
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
	T1091: Replication Through Removable Media	
	T1563: Remote Service Session Hijacking	
	T1570: Lateral Tool Transfer	
TA0009: Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1056: Input Capture	T1056.001: Keylogging
		T1056.004: Credential API Hooking
	T1005: Data from Local System	
	T1025: Data from Removable Media	
	T1039: Data from Network Shared Drive	
	T1074: Data Staged	
	T1113: Screen Capture	
	T1114: Email Collection	
	T1115: Clipboard Data	
	T1213: Data from Information Repositories	
	T1530: Data from Cloud Storage	

Tactic	Technique	Sub-technique
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.003: Multi-hop Proxy
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1095: Non-Application Layer Protocol	
	T1102: Web Service	
	T1105: Ingress Tool Transfer	
	T1219: Remote Access Software	
	T1571: Non-Standard Port	
	T1573: Encrypted Channel	
TA0010: Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
	T1041: Exfiltration Over C2 Channel	
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1496: Resource Hijacking	
	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	

Top 5 Takeaways

#1

In **February**, there were **eleven zero-day** vulnerabilities, with the **One Celebrity Vulnerability** dubbed **PROXYSHELL** taking center stage. Meanwhile, **CVE-2024-34331** in Parallels Desktop allows **root escalation**, remains **unpatched** in all known versions, and has public exploits users must stay vigilant.

#2

Nation-state cyber threats surged in **February**, with **Silk Typhoon** exploiting **BeyondTrust** flaws, **Salt Typhoon** breaching **U.S. telecom networks**, and **North Korea's Ferret** malware targeting job seekers and developers through fake software.

#3

Cyberattacks hit **169 countries** in February, with **Vietnam, South Korea, Singapore, China, and Thailand** facing the brunt of the threats. From espionage-driven nation-state campaigns to financially motivated cybercrime, no region was immune as adversaries expanded their reach globally.

#4

The **Government, Manufacturing, Technology, Financial Services, and Media** sectors were prime targets, with ransomware, data theft, and espionage campaigns wreaking havoc. As attackers refine their tactics, organizations in these industries must stay ahead with proactive security measures.

#5

Ransomware is evolving. Double extortion, backup destruction, and rapid zero-day exploits make recovery impossible. **RaaS** enables anyone to launch attacks, while threats like **Lynx, RA World, and Ghost** ransomware spread fast. Patch, secure backups, and enforce zero-trust before it's too late.

Recommendations

Security Teams

















This digest can be used as a guide to help security teams prioritize the **27 significant vulnerabilities** and block the indicators related to the **6 active threat actors**, **33 active malware**, and **172 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 **27 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).

Hive Pro Threat Advisories (FEBRUARY 2025)

MONDAY		TUESDAY		WEDNESDAY		THURSDAY		FRIDAY		SATURDAY		SUNDAY	
										1		2	
	3		4		5		6		7		8		9
													
	10		11		12		13		14		15		16
													
	17		18		19		20		21		22		23
													
	24		25		26		27		28		29		
													

Click on any of the icons to get directed to the advisory

	Red Vulnerability Report		Amber Attack Report
	Amber Vulnerability Report		Red Actor Report
	Green Vulnerability Report		Amber Actor Report
	Red Attack Report		

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>Coyote</u>	SHA256	362af8118f437f9139556c59437544ae1489376dc4118027c24c8d5ce4d84e48, 552d53f473096c55a3937c8512a06863133a97c3478ad6b1535e1976d1e0d45f, 64209e2348e6d503ee518459d0487d636639fa5e5298d28093a5ad41390ef6b0, 67f371a683b2be4c8002f89492cd29d96dceabdbfd36641a27be761ee64605b1, 73ad6be67691b65cee251d098f2541eef3cab2853ad509dac72d8eff5bd85bc0, 839de445f714a32f36670b590eba7fc68b1115b885ac8d689d7b344189521012, bea4f753707eba4088e8a51818d9de8e9ad0138495338402f05c5c7a800695a6, f3c37b1de5983b30b9ae70c525f97727a56d3874533db1a6e3dc1355bfbf37ec, fd0ef425d34b56d0bc08bd93e6ecb11541bd834b9d4d417187373b17055c862e, 330dffe834ebbe4042747bbe00b4575629ba8f2507bccf746763cacf63d655bb, 33cba89eeeaf139a798b7fa07ff6919dd0c4c6cf4106b659e4e56f15b5809287
<u>SmokeLoader</u>	SHA256	554d9ddd6fd1ccb15d7686c8badb8653323c71884c7f20efb19b56324ff34fc1, 62eb856a5f646c2883a3982f15c3eb877641f9e69783383ce8a73c688eccd543, 5c7d582ba61ac95fb0d330ecc05feeb4853ac1de1f5a6fd12df6491dd0b7ea34, 2e33c2010f95cbda8bf0817f1b5c69b51c860c536064182b67261f695f54e1d5, 888f68917f9250a0936fd66ea46b6c510d0f6a0ca351ee62774dd14268fe5420
<u>FlexibleFerret</u>	SHA1	388ac48764927fa353328104d5a32ad825af51ce, 1a28013e4343fddf13e5c721f91970e942073b88, 3e16c6489bac4ac2d76c555eb1c263cd7e92c9a5, 76e3cb7be778f22d207623ce1907c1659f2c8215, b0caf49884d68f72d2a62aa32d5edf0e79fd9de1, bd73a1c03c24a8cdd744d8a513ae8d2ddfa2de5f, ccac0f0ba463c414b26ba67b5a3ddaabdef6d371, d8245cdf6f51216f29a71f25e70de827186bdf71, b071fbd9c42ff660e3f240e1921533e40f0067eb, ee7a557347a10f74696dc19512ccc5fcfca77bc5

Attack Name	TYPE	VALUE
<u>FlexibleFerret</u>	SHA256	3c4becde20e618efb209f97581e9ab6bf00cbd63f51f4ebd5677e352c57e992a, bd2aa5805b76f272b43a595b3d73e29d0fc4647e15e87950b8f904ea26dcf053
<u>FRIENDLYFERRET</u> <u>I</u>	SHA1	17e3906f6c4c97b6f5d10e0e0e7f2a2e2c97ca54, 2e51218985afcaa18eadc5775e6b374c78e2d85f, 7e07765bf8ee2d0b2233039623016d6dfb610a6d, de3f83af6897a124d1e85a65818a80570b33c47c
<u>FrostyFerret_UI</u>	SHA1	7da429f6d2cdd8a63b3930074797b990c02dc108, 7e07765bf8ee2d0b2233039623016d6dfb610a6d, 828a323b92b24caa5f5e3eff438db4556d15f215, 831cdcde47b4edbe27524085a6706fbfb9526cef, 8667078a88dae5471f50473a332f6c80b583d3de, dba1454fbea1dd917712fbece9d6725244119f83, e876ba6e23e09206f358dbd3a3642a7fd311bb22
<u>MULTI_FROSTY_FERRET_CMDC</u> <u>ODES</u>	SHA1	203f7cfbf22b30408591e6148f5978350676268b, a25dff88aeaaaf9f956446151a9d786495e2c546, aa172bdccb8c14f53c059c8433c539049b6c2cdd
<u>AsyncRAT</u>	SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9, 5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8, 6f92b2cdb8b5f68d20dbc7ca23c3a3ec78c4ef1859001940dfa22e38ce459d30, 6d240a48b5e2d1cf761a8b48b146d20729d0a7a3a557e31e75ed4c120ce71aea, c7d4e119149a7150b7101a4bd9fffbf659fba76d058f7bf6cc73c99fb36e8221, 2657fe9b88321d255fc56a81b2df4b0109ab7c525442f31765c94d75c37347aa, 124c02ed924e11b06b74e1b8c1290adbb1e50dfa2a7bcf95104c6425a1f82ef5, 3c4df2d02e4b6f4acf7b19238211892db501ee6faa04065dd11b25b56483f9c4, 9a7bc24bd814ab755a8ad67e1aeabc05ff139771928f0eae883daff6f4ae161d, 65d6130ed7d3d822e1b08e7bed8e3adca4188d787d6805935213369c05eb2a99, 90245116af6f781c72ad78b8d160fa0c0b9d95bd033c83137c75fc60236dd2d5

Attack Name	TYPE	VALUE
<u>AsyncRAT</u>	IPv4	138[.]68[.]81[.]155
<u>Lynx</u>	Domain	hxxp[:]//lynxblog[.]net
	Email	martina[.]lestariid1898[@]proton[.]me
	SHA256	571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b, eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc, 80908a51e403efd47b1d3689c3fb9447d3fb962d691d856b8b97581eefc0c441, 3e68e5742f998c5ba34c2130b2d89ca2a6c048feb6474bc81ff000e1eae d044e, 97c8f54d70e300c7d7e973c4b211da3c64c0f1c95770f663e04e35421dfb2ba0, 468e3c2cb5b0bbc3004bbf5272f4ece5c979625f7623e6d71af5dc0929b89d6a
<u>ValleyRAT</u>	SHA256	968b976167b453c15097667b8f4fa9e311b6c7fc5a648293b4abd75d80b15562, 6ed466a2a6eeb83d1ff32ba44180352cf0a9ccc72b47e5bd55c1750157c8dc4c
<u>BACKORDER</u>	SHA256	48450c0a00b9d1ecce930eadbac27c3c80db73360bc099d3098c08567a59cd d3, 22c79153e0519f13b575f4bfc65a5280ff93e054099f9356a842ce3266e40c3 d, a42de97a466868efbfc4aa1ef08bfdb3cc5916d1accd59cfffff1a896d569412, 8cfa4f10944fc575420533b6b9bbcabbf3ae57fe60c6622883439dbb1aa6036 9, 8a4df53283a363c4dd67e2bda7a430af2766a59f8a2faf341da98987fe8d7cb d, 70c91ffdc866920a634b31bf4a070fb3c3f947fc9de22b783d6f47a097fec2d8, 0e58d38fd2df86eeb4a556030a0996c04bd63e09e669b34d3bbc10558edf31 a6, 5bff08a6aa7a7541c0b7b1660fd944cec55fa82df6285166f4da7a48b81f776e , 4b9e32327067a84d356acb8494dc05851dbf06ade961789a982a5505b9e06 1e3
<u>DarkCrystal</u>	SHA256	039c8dd066efa3dd7ac653689bfa07b2089ce4d8473c907547231c6dd2b136 ec, 0e58d38fd2df86eeb4a556030a0996c04bd63e09e669b34d3bbc10558edf31 a6, 1a1ffcbab9bff4a033a26e8b9a08039955ac14ac5ce1f8fb22ff481109d781a7, 2de08a0924e3091b51b4451c694570c11969fb694a493e7f4d89290ae5600c 2c, 4b0038de82868c7196969e91a4f7e94d0fa2b5efa7a905463afc01bfca4b822 1, 7c0da4e314a550a66182f13832309f7732f93be4a31d97faa6b9a0b311b463f f,

Attack Name	TYPE	VALUE
<u>DarkCrystal</u>	SHA256	a00beaa5228a153810b65151785596bebe2f09f77851c92989f620e37c60c935, b45712acbadcd17cb35b8f8540ecc468b73cac9e31b91c8d6a84af90f10f29f8, cd7c36a2f4797b9ca6e87ab44cb6c8b4da496cff29ed5bf727f0699917bae69a, 4b2e4466d1becfa40a3c65de41e5b4d2aa23324e321f727f3ba20943fd6de9e5, 553f7f32c40626cbddd6435994aff8fc46862ef2ed8f705f2ad92f76e8a3af12, d774b1d0f5bdb26e68e63dc93ba81a1cdf076524e29b4260b67542c06fbfe55c, 70cad07a082780caa130290fcb1fd049d207777b587db6a5ee9ecf15659419f, C5853083d4788a967548bee6cc81d998b0d709a240090cfed4ab530ece8b436e
<u>Kalambur</u>	SHA256	aadd85e88c0ebb0a3af63d241648c0670599c3365ff7e5620eb8d06902fdde83, 7d92b10859cd9897d59247eb2ca6fb8ec52d8ce23a43ef99ff9d9de4605ca12b, d13f0641fd98df4edcf839f0d498b6b6b29fbb8f0134a6dae3d9eb577d771589, dd7a9d8d8f550a8091c79f2fb6a7b558062e66af852a612a1885c3d122f2591b
<u>Abyss Locker</u>	SHA256	05b82d46ad331cc16bdc00de5c6332c1ef818df8ceefcd49c726553209b3a0da, 6042a84529958a04a2d46384139da3ef016bf9498e791cd5e34dfecec2baa1d2, 3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71, 5fba25759423f9efc92592977f6c9ff77d47a20aa8ec8e9cd17d5cfa786a1852, cd9d88cccd85209966c5a35aba7751b962bcc021a4216d6addfc0c3462ce80da, f9ab649acfe76d6ac088461b471e5d981bdc8b71d940e94c63bc1988a2ed4678, 5f9dfd9557cf3ca96a4c7f190fc598c10f8871b1313112c9aea45dc8443017a2, d48c7f13db60ef615e59773c442485e84acef09343375d0d8a462b285e959baa, d76c74fc7a00a939985ae515991b80afa0524bf0a4feaec3e5e58e52630bd717, 0d9089efe2a28630bc21d8db451ec14dc856c2d40444292c42e7cca218c7029e
	SHA1	59a97f9d7c1d6e10fa41ea9339568fb25ec55e27, 3f90fd241e9422cc447b5ccdc87d72507f37e6f, 23873bf2670cf64c2440058130548d4e4da412dd, e44ec82d0d80c754afcd7ed149c263c55d158259,

Attack Name	TYPE	VALUE
<u>Abyss Locker</u>	SHA1	13112e672d807fa7c7f8a383ecfa31e85b880e5a, f24ca204af2237a714e8b41d54043da7bbe5393b, 17d9200843fe0eb224644a61f0d1982fac54d844, 82780c0c1c0e04d994c770a3b3e73727528b0451
	File Path	C:\users\<USER>\appdata\roaming\microsoft\wmi\wmihelper.exe, C:\WINDOWS\system32\config\systemprofile\AppData\Roaming\Microsoft\Wmi\wmihelper.exe, /bin/apache2, C:\Windows\uFmAnlZR.exe, /tmp/e.elf, C:\Users\<USER>\Desktop\e\e.exe, C:\Windows\System32\rclone, C:\Windows\System32\LTSSVC.exe, C:\Windows\System32\filter.txt, C:\Windows\Temp\SophosAV.exe, C:\ProgramData\USOShared\auSophos.exe, C:\ProgramData\USOShared\UpdateSvc.exe, C:\programdata\pr.exe, C:\ProgramData\deploy443.ps1, C:\ProgramData\USOShared\UpdateDrv.sys
	TOR Address	3ev4metjirohtdpshsqlkrqcmxq6zu3d7obrdhglpy5jpbr7whmlfgqd[.]onion
	File Name	wmihelper.xml, wmihelper.key, veeam11.ps1, ped.sys, 3ware.sys
	Host Name	DESKTOP-VM4QKN6, ADMINIS-F69E5L3
	IPv4	139[.]180[.]135[.]191, 67[.]217[.]228[.]101, 64[.]95[.]12[.]57, 64[.]95[.]12[.]70, 149[.]137[.]142[.]15
<u>PATHLOADER</u>	SHA256	9a11d6fcf76583f7f70ff55297fb550fed774b61f35ee2edd95cf6f959853bcf
<u>FINALDRAFT</u>	SHA256	83406905710e52f6af35b4b3c27549a12c28a628c492429d3a411fdb2d28cc8c, 39e85de1b1121dc38a33eca97c41dbd9210124162c6d669d28480c833e059530, 83406905710e52f6af35b4b3c27549a12c28a628c492429d3a411fdb2d28cc8c, f45661ea4959a944ca2917454d1314546cc0c88537479e00550eef05bed5b1b9
<u>GUILOADER</u>	SHA256	17b2c6723c11348ab438891bc52d0b29f38fc435c6ba091d4464f9f2a1b926e0, 20508edac0ca872b7977d1d2b04425aaa999ecf0b8d362c0400abb58bd686f92,

Attack Name	TYPE	VALUE
<u>GUILOADER</u>	SHA256	41a3a518cc8abad677bb2723e05e2f052509a6f33ea75f32bd6603c96b721081, d9fc1cab72d857b1e4852d414862ed8eab1d42960c1fd643985d352c148a6461, f29779049f1fc2d45e43d866a845c45dc9aed6c2d9bbf99a8b1bdacf ac2d52f2, 33f3a8ef2c5fbd45030385b634e40eaa264acbaeb7be851cbf04b62 bbe575e75, 41141e3bdde2a7aebf329ec546745149144eff584b7fe878da7a2ad 8391017b9, 49e383ab6d092ba40e12a255e37ba7997f26239f82bebcd28efaa42 8254d30e1, 5e3dbfd543909ff09e343339e4e64f78c874641b4fe9d68367c4d10 24fe79249, 7cd14d3e564a68434e3b705db41bddeb51dbb7d5425fd901c5ec90 4dbb7b6af0, 842d6ddb7b26fdb1656235293ebf77c683608f8f312ed917074b30f bd5e8b43d, f90420847e1f2378ac8c52463038724533a9183f02ce9ad025a6a10f d4327f12
<u>Lumma Stealer</u>	SHA256	e15c6ecb32402f981c06f3d8c48f7e3a5a36d0810aa8c2fb8da0be053b95a8e2
	URL	hxxps[:]//80[.]76[.]51[.]231/Kompass-4[.]1[.]2[.]exe,
<u>RA World (aka RA Group ransomware)</u>	SHA256	2707612939677e8ea4709ecb4f45953d4a136a9934b6d0c256917383cdaef813, 38a26fffbab5297e4229897654d2f67c6ee52b316c7ac4d4a1493d187b49ec25
<u>PlugX</u>	Domain	police[.]tracksyscloud[.]com, caco[.]blueskyanalytics[.]net
	IPv4	154[.]223[.]18[.]123, 23[.]227[.]203[.]181
	SHA256	8615cc8487833522ffd014c0f0661b3d1bed7a4cb51138b1ee172173002192be, b6e88396594070a92cbf1c313858392b052703944162de64ce3ad494996bd177, 583941ca6e1a2e007f5f0e2e112054e44b18687894ac173d0e93e035cea25e83, e3bae2e2b757a76db92ab017328d1459b181f8d98e04b691b62ff65d1e1be280, 60b3a42b96b98868cae2c8f87d6ed74a57a64b284917e8e0f6c248c691d51797, eb9e557fac3dd50cc46a544975235ebfce6b592e90437d967c9afba234a33f13, 16b62c9dc6060a19a5b64491b7242ace1c707dbe531b843c854fcc1dc39febbe,

Attack Name	TYPE	VALUE
<u>PlugX</u>	SHA256	5dd7813fa8aad22bd6c80811c8c7300f114a8e7897a2bd46343a06884d774914, 70cd979cc17a89856c2a6acccb32964c01c208cb232cbd9e782d2baab00c36e4
<u>Vgod</u>	SHA256	241c3b02a8e7d5a2b9c99574c28200df2a0f8c8bd7ba4d262e6aa8ed1211ba1f
<u>XMRig</u>	SHA256	e60ef7de4d1e27944469ce534b113b6d49ddd266febba5fc8d02e77a3b6d5b08
<u>Snake Keylogger</u>	MD5	f8410bcd14256d6d355d7076a78c074f, f8410bcd14256d6d355d7076a78c074f
	SHA256	7e9b9833268dae6e33c83b582ec7fb353f0dc6514f869e3228f0effa161da00f
<u>Winnti Loader (also known as PRIVATELOG)</u>	SHA256	169d35bdb36c2bfc3bbf64392de1b05d56553172a13cae43a43acbe2aa18587, b9d4ec771a79f53a330b29ed17f719dac81a4bfe11caf0eac0efacd19d14d090, 4608a63c039975fb8f3ffd221ec6877078542def44767f50447db1d514eb0779, 1e53559e6be1f941df1a1508bba5bb9763aedba23f946294ce5d92646877b40c
<u>Winnti Rootkit</u>	SHA256	e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596, c649e75483dd0883de2fef001a44263a272c6b49a8d1c9ea7c00c044495200ad, 569c1d9b2822c17e64214421409c5649eafc5df9abd88d40a5554f57f32588e8
<u>NailaoLocker</u>	SHA256	7a0503da293da51a95aab0b1aa0970c8f82f04cb5149abe98fef934ba991064e, 2b069dcde43b874441f66d8888dcf6c24b451d648c8c265dfffb81c7dffafd667, 27b313243daf145c9105f5372e01f1cea74c62697195c1a21c660be5f7ee788c, a2e937d0b9d5afa5b638cd511807e0fcb44ec81b354e2cf0c406f19e5564e54e
<u>Shadowpad</u>	URL	hxxps[:]//dscry[.]chtq[.]net
	IPv4	193[.]56[.]255[.]214, 158[.]247[.]199[.]185, 104[.]238[.]135[.]232, 139[.]84[.]137[.]63, 141[.]164[.]35[.]65, 176[.]222[.]55[.]131, 193[.]56[.]255[.]214, 37[.]120[.]239[.]33, 45[.]76[.]209[.]205, 45[.]77[.]153[.]108, 45[.]77[.]170[.]188, 47[.]242[.]0[.]122, 52[.]194[.]253[.]134,

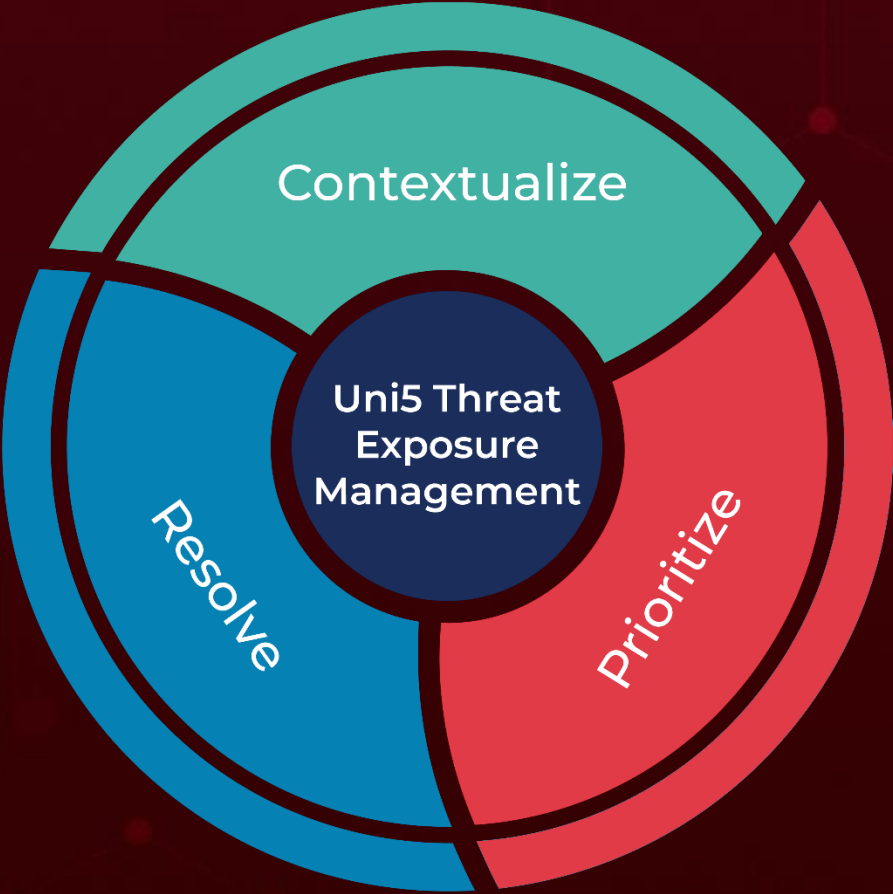
Attack Name	TYPE	VALUE
<u>Shadowpad</u>	IPv4	64[.]176[.]226[.]182, 64[.]176[.]59[.]232, 64[.]176[.]65[.]49, 8[.]210[.]30[.]189, 8[.]218[.]244[.]117
	SHA256	c5f8a256d0969e253633160b9728b6c2bc044f536e92af178a05a59 8aaa09c1f, 0a749474b5f4a8537e50ea5b60d8c94f5c688fe414cd400c3397adc a4315a509, a2bb321d41b2300e80f9400950fa2125470d5b3927933ab4d6397f 0cbf81532a, 697e6454d9be19f0bd60aeffa0238498a91d1ea5a23112f7c8f981af d2fedb23
<u>Ghost Ransomware</u>	MD5	c5d712f82d5d37bb284acd4468ab3533, 34b3009590ec2d361f07cac320671410, d9c019182d88290e5489cdf3b607f982, 29e44e8994197bdb0c2be6fc5dfc15c2, c9e35b5c1dc8856da25965b385a26ec4, d1c5e7b8e937625891707f8b4b594314, ef6a213f59f3fbee2894bd6734bbaed2, ac58a214ce7deb3a578c10b97f93d9c3, c3b8f6d102393b4542e9f951c9435255, 0a5c4ad3ec240fbfd00bdc1d36bd54eb, ff52fdf84448277b1bc121f592f753c5, a2fd181f57548c215ac6891d000ec6b9, 625bd7275e1892eac50a22f8b4a6355d, db38ef2e3d4d8cb785df48f458b35090
<u>FatalRAT</u>	MD5	2477e031f776539c8118b8e0e6663b0, 02d8c59e5e8a85a81ee75ce517609739, 05c528a2b8bb20aad901c733d146d595, 15962f79997a308ab3072c10e573e97c, 17278c3f4e8bf56d9c1054f67f19b82c, 172ee543d8a083177fc1832257f6d57d, 1fe3885dea6be2e1572d8c61e3910d19, 249f568f8b8709591e7afd934ebea299, 266bb19f9ceb1a4ccbf45577bbeaac1a, 3c583e01eddd0ea6fe59a89aea4503b4, 3ec20285d88906336bd4119a74d977a0, 43156787489e6aa3a853346cded3e67b, 46630065be23c229adff5e0ae5ca1f48, 577e1a301e91440b920f24e7f6603d45, 5be46b50cac057500ea3424be69bf73a, 60a92d76e96aaa0ec79b5081ddcc8a24, 60dbc3ef17a50ea7726bdb94e96a1614, 635f3617050e4c442f2cbd7f147c4dcf, 675a113cdbcce171e1ff172834b5f740, 68a27f7ccbfa7d3b958fad078d37e299,

Attack Name	TYPE	VALUE
<u>FatalRAT</u>	MD5	73e49ddf4251924c66e3445a06250b10, 787f2819d905d3fe684460143e01825c, 7ac3ebac032c4afd09e18709d19358ed, 8f67a7220d36d5c233fc70d6ecf1ee33, 9b4d46177f24ca0a4881f0c7c83f5ef8, 9c3f469a5b54fb2ec29ac7831780ed6d, 9d34d83e4671aaf23ff3e61cb9daa115, a935ef1151d45c7860bfe799424bea4b, bcec6b78adb3cf966fab9025dacb0f05, d0d3efcff97ef59fe269c6ed5ebb06c9, ebc0809580940e384207aa1704e5cc8e, eca08239da3acaf0d389886a9b91612a, ed6837f0e351aff09db3c8ee93fbcf06, fb8dc76a0cb0a5d32e787a1bb21f92d2, feb49021233524bd64eb6ce37359c425
<u>Auto-color</u>	SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3 072d4c43, 65a84f6a9b4ccddcdae812ab8783938e3f4c12cfba670131b1a8039 5710c6fb4, 83d50fcf97b0c1ec3de25b11684ca8db6f159c212f7ff50c92083ec5f bd3a633, a1b09720edcab4d396a53ec568fe6f4ab2851ad00c954255bf1a0c0 4a9d53d0a, bace40f886aac1bab03bf26f2f463ac418616bacc956ed97045b7c30 72f02d6b, e1c86a578e8d0b272e2df2d6dd9033c842c7ab5b09cda72c588e04 10dc3048f7, 85a77f08fd66aeabc887cb7d4eb8362259afa9c3699a70e3b81efac9 042bb255, bf503b5eb456f74187a17bb8c08bcc9b3d91a7f0f6fd50110540b05 1510d1ca
<u>Winos 4.0</u>	SHA256	f519802d1abc6f364b519e6c9a108edfb688d42d438167c1524387c fbdf066ef, 8b1b9a789136ca3abe25938204845c351aaf0c97c0708ade8d4d8ba 4ded95ba7

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 free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON
March 3, 2025 • 3:00 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com