Date of Publication
May 2, 2025

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

APRIL 2025

Table Of Contents

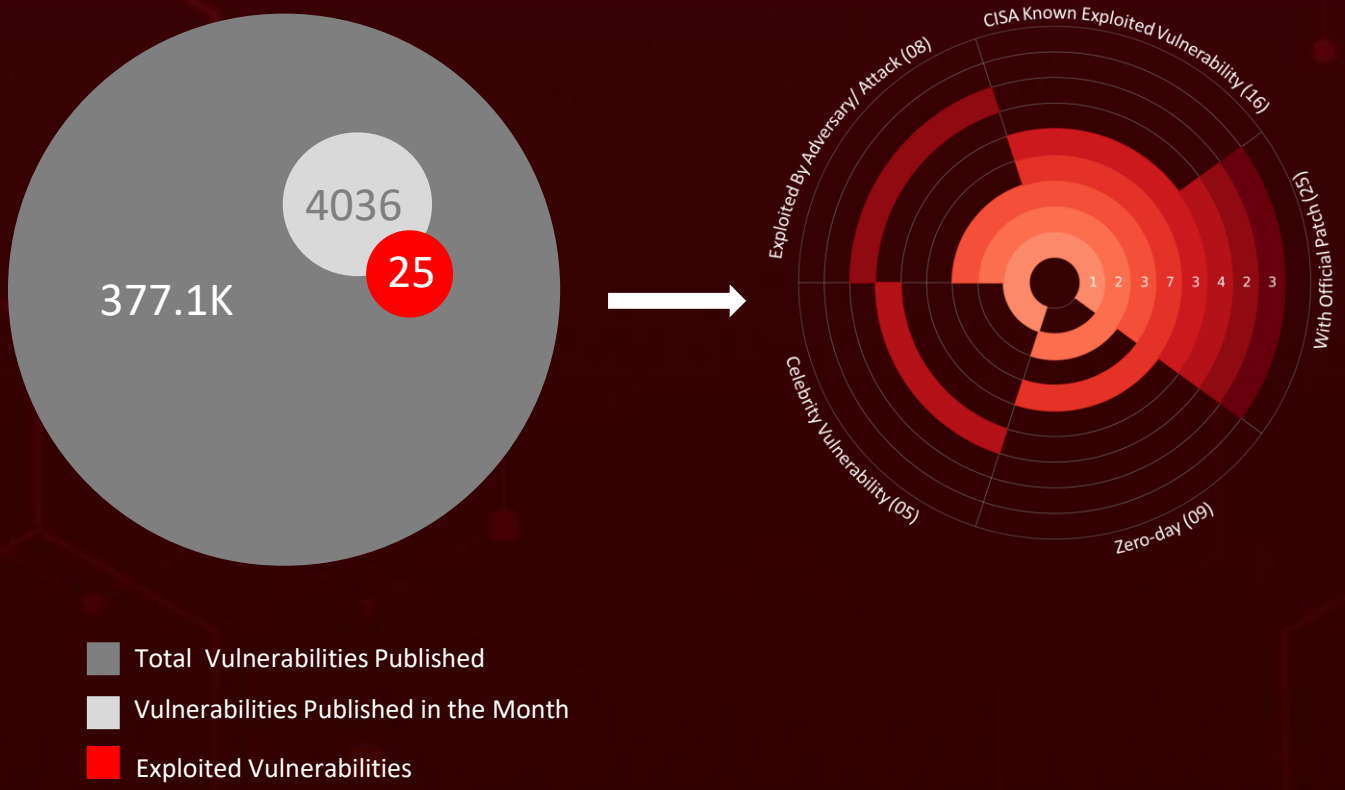
Summary

In **April**, the cybersecurity arena drew significant attention due to the active exploitation of **nine zero-day** vulnerabilities. Among them, Apple patched two zero-day vulnerabilities **(CVE-2025-31200, CVE-2025-31201)** used in targeted attacks. The flaws affect iPhones, Macs, iPads, Apple TVs, and Vision Pro, allowing potential code execution or security bypass.

During this period, ransomware attacks surged, with variants such as **Hellcat**, **PlayBoy Locker**, **DOGE BIG BALLS**, **Interlock**, **CrazyHunter**, **and Cactus** aggressively targeting victims. As ransomware tactics grow more sophisticated, organizations must bolster their defenses by implementing comprehensive backup and disaster recovery strategies. Additionally, training employees to detect and prevent phishing attacks remains essential.

The Lazarus group's "**Operation SyncHole**" targets South Korean industries using exploits and watering hole attacks, deploying malware like ThreatNeedle and SIGNBT. The campaign highlights their evolving tactics to infiltrate supply chains and deepen network access.

Concurrently, eleven threat actors have engaged in various campaigns. The China-linked APT group known as **Earth Alux** is stirring the cyberespionage landscape with nearly undetectable intrusions. This group has set its sights on strategically vital sectors across the Asia-Pacific and Latin American regions. At the same time, the **ToddyCat** APT exploited CVE-2024-11859 in ESET's command-line scanner by using DLL proxying and a custom tool (TCESB) to stealthily load malicious code and manipulate kernel structures. As the cybersecurity landscape evolves, organizations must remain vigilant and proactively address emerging threats.



Insights

In April 2025, a geopolitical cybersecurity landscape unfolds, revealing **Poland, Russia, Turkey, South Korea,** and **Netherlands** as the top-targeted countries.

Highlighted in **April 2025** is a cyber battleground encompassing the **Government, Manufacturing, Technology, Healthcare, Telecommunications** and **Financial** sectors, designating them as the top industries.

HellCat, a 2024 Ransomware-as-a-Service, uses a decentralized model to deliver custom payloads, exfiltrate data, and encrypt systems in a double-extortion scheme targeting high-value sectors.

APT29's classy bait: Masquerading as a wine-tasting invite from a European ministry, the group used **GRAPELOADER** via DLL side-loading to plant the stealthy **WINELOADER** backdoor and establish long-term access.

CVE-2025-24054 lets attackers leak hashes via malicious .library-ms files; exploitation kicked off just days after the patch.

INTERLOCK is a rising ransomware group targeting FreeBSD systems, using double-extortion tactics, social engineering, and an active data leak site to establish itself as a growing threat.

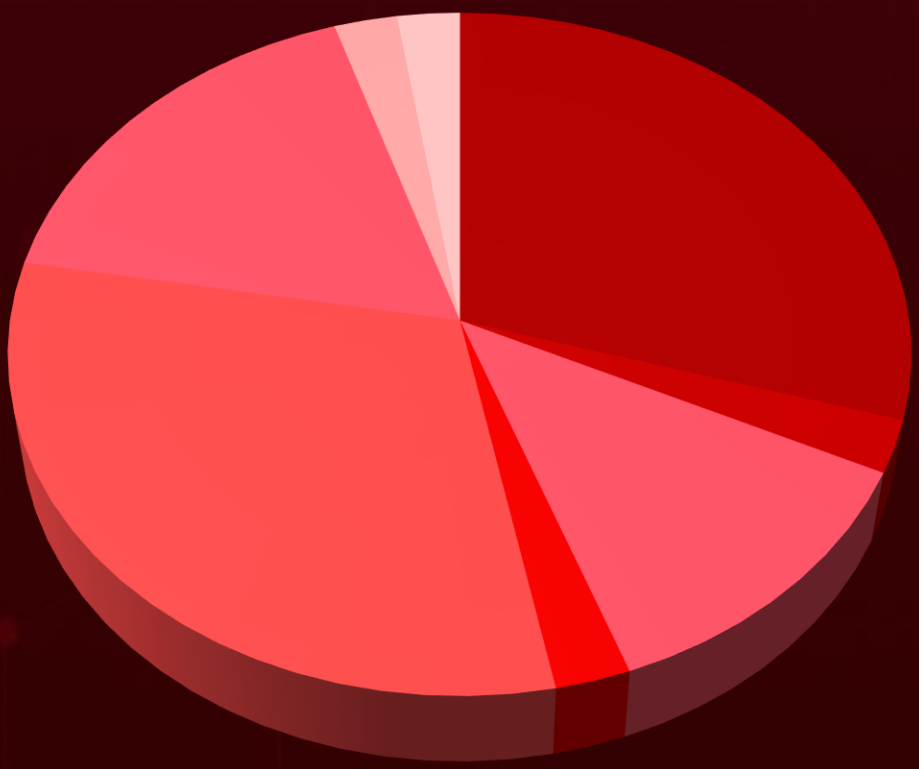
Critical **SAP NetWeaver flaw (CVE-2025-31324)** is being exploited to drop web shells and run malicious code. Attackers can upload harmful files without logging in.

Kimsuky, a North Korean threat actor is targeting South Korea's critical sectors, leveraging old but effective vulnerabilities like CVE-2017-11882 and CVE-2019-0708 (BlueKeep) to breach networks.

ClickFake Interview: Lazarus Group's New Trap for Job Seekers

CVE-2025-32965: Inside the xrpl.js Supply Chain Attack Threatening the XRP Ecosystem

Threat Landscape



Celebrity Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-1974	IngressNightmare	Kubernetes ingress-nginx versions: All versions prior to v1.11.0, v1.11.0 to v1.11.4, and v1.12.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes:ingress-nginx:-:*:*:*:*:*:*:*	-
Kubernetes Unauthenticated Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-653	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution	https://github.com/kubernetes/ingress-nginx/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-1097	IngressNightmare	Kubernetes ingress-nginx versions: All versions prior to v1.11.0, v1.11.0 to v1.11.4, and v1.12.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes:ingress-nginx:-:*:*:*:*:*:*:*	-
Kubernetes Arbitrary Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution	https://github.com/kubernetes/ingress-nginx/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-1098	IngressNightmare	Kubernetes ingress-nginx versions: All versions prior to v1.11.0, v1.11.0 to v1.11.4, and v1.12.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes:ingress-nginx:-:*:*:*:*:*:*:*	-
Kubernetes Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-653	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution	https://github.com/kubernetes/ingress-nginx/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24514	IngressNightmare	Kubernetes ingress-nginx versions: All versions prior to v1.11.0, v1.11.0 to v1.11.4, and v1.12.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kubernetes:ingress-nginx:-:*:*:*:*:*:*:*	-
Kubernetes Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://github.com/kubernetes/ingress-nginx/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-0708	BlueKeep	Windows: 10 - 11 23H2; Windows Server: 2019 – 2022 23H2	Kimsuky
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	MySpy, RandomQuery, KimaLogger
BlueKeep (Microsoft Remote Desktop Services Remote Code Execution Vulnerability)	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1021: Remote Services	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	KEV	PATCH
CVE-2025-31161	CrushFTP Authentication Bypass Vulnerability	CrushFTP	✗	✓	✓
CVE-2025-22457	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✗	✓	✓
CVE-2024-20439	Cisco Smart Licensing Utility Static Credential Vulnerability	Cisco Smart Licensing Utility	✗	✓	✓
CVE-2024-20440	Cisco Smart Licensing Utility Information Disclosure Vulnerability	Cisco Smart Licensing Utility	✗	✗	✓
CVE-2025-29824	Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-30406	Gladinet CentreStack Use of Hard-coded Cryptographic Key Vulnerability	Gladinet CentreStack	✓	✓	✓
CVE-2024-11859	ESET Multiple Products DLL Search Order Hijacking Vulnerability	ESET Multiple Products	✗	✗	✓
CVE-2021-36276	Dell DBUtilDrv2.sys Driver Insufficient Access Control Vulnerability	Dell DBUtilDrv2.sys Driver	✗	✗	✓
CVE-2025-1974	Kubernetes Unauthenticated Remote Code Execution Vulnerability	Kubernetes ingress-nginx	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-1097	Kubernetes Arbitrary Code Execution Vulnerability	Kubernetes	✗	✗	✓
CVE-2025-1098	Kubernetes Code Execution Vulnerability	Kubernetes	✗	✗	✓
CVE-2025-24514	Kubernetes Command Injection Vulnerability	Kubernetes	✗	✗	✓
CVE-2015-2291	Intel Ethernet Diagnostics Driver for Windows Denial-of-Service Vulnerability	Microsoft Windows	✗	✓	✓
CVE-2025-31200	Apple Multiple Products Memory Corruption Vulnerability	Apple Multiple Products	✓	✓	✓
CVE-2025-31201	Apple Multiple Products Arbitrary Read and Write Vulnerability	Apple Multiple Products	✓	✓	✓
CVE-2025-24054	Microsoft Windows NTLM Hash Disclosure Spoofing Vulnerability	Microsoft Windows	✗	✓	✓
CVE-2024-43451	Microsoft Windows NTLMv2 Hash Disclosure Spoofing Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-32433	Erlang/OTP Unauthenticated Remote Code Execution Vulnerability	Erlang/OTP SSH servers	✗	✗	✓
CVE-2019-0708	BlueKeep (Microsoft Remote Desktop Services Remote Code Execution Vulnerability)	Microsoft Remote Desktop Services	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓
CVE-2025-42599	Qualitia Active! Mail Stack Buffer Overflow Vulnerability	Dasan GPON home routers	✓	✓	✓
CVE-2025-32965	xrpl.js Supply Chain Vulnerability	xrpl.js	✗	✗	✓
CVE-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver	✓	✓	✓
CVE-2025-3928	Commvault Web Server Unspecified Vulnerability	Commvault Web Server	✓	✓	✓
CVE-2025-0282	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
GODZILLA	Web Shell	-	Windows	-	Exploiting Vulnerabilities in Exposed Servers
VARGEIT	Backdoor	-	Windows	-	GODZILLA facilitates the delivery
RAILLOAD	Loader	-	Windows	-	VARGEIT deploys via DLL side-loading
MASQLOADER	Loader	-	Windows	-	Side-loaded DLL or shellcode
GolangGhost	Backdoor	-	Windows, macOS	-	Social Engineering
FrostyFerret	Stealer	-	Windows, macOS	-	Social Engineering
TRAILBLAZE	Dropper	CVE-2025-22457	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting vulnerabilities
BRUSHFIRE	Backdoor	CVE-2025-22457	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting vulnerabilities
SPAWNSNARE	Tool	CVE-2025-22457	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting vulnerabilities
SPAWNWAVE	Backdoor	CVE-2025-22457	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting vulnerabilities
SPAWNSLOTH	Backdoor	CVE-2025-22457	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting vulnerabilities

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
PipeMagic	Backdoor	CVE-2025-22457	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting vulnerabilities
GIFTEDCROOK	Infostealer	-	Windows	-	Phishing
Hellcat	Ransomware	-	Windows	-	-
Neptune	Modular RAT	-	Windows	-	Phishing
PlayBoy Locker	Ransomware	-	Windows, NAS, and ESXi	-	Phishing emails or vulnerable Remote Desktop Protocol (RDP) services
ResolverRAT	RAT	-	Windows	-	Phishing
DOGE BIG BALLS	Ransomware	CVE-2015-2291	iQVW32.SYS, iQVW64.SYS	✓	Phishing, Exploiting Vulnerability
GammaSteel	Stealer	-	-	-	Using a malicious LNK file on a USB drive
GRAPELOADER	Loader	-	-	-	Phishing
WINELOADER	Backdoor	-	-	-	Phishing
Interlock	Ransomware	-	Microsoft Windows, Linux	-	Phishing
BerserkStealer	Stealer	-	Microsoft Windows, Linux	-	Phishing
LummaStealer	Stealer	-	Microsoft Windows, Linux	-	Phishing
MySpy	Spyware	CVE-2019-0708 CVE-2017-11882	Windows Server, Microsoft Office	✓	Exploited the RDP vulnerability

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
KimaLogger	Keylogger	CVE-2019-0708 CVE-2017-11882	Windows Server, Microsoft Office		Exploited the RDP vulnerability
Sagerunex	Backdoor	-	Windows	-	Exploiting vulnerabilities in public-facing applications, spear-phishing, or credential abuse
ChromeKatz	Stealer	-	Windows	-	Exploiting vulnerabilities in public-facing applications, spear-phishing, or credential abuse
CredentialKatz	Stealer	-	Windows	-	Exploiting vulnerabilities in public-facing applications, spear-phishing, or credential abuse
ThreatNeedle	Loader	-	-	-	Compromised online media sites
wAgent	Loader	-	-	-	Compromised online media sites
SIGNBT	Backdoor	-	-	-	Compromised online media sites
COPPERHEDGE	Dropper	-	-	-	Compromised online media sites
Agamemnon	Downloader	-	-	-	Compromised online media sites

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
LPEClient	Tool	-	-	-	Compromised online media sites
CrazyHunter	Ransomware	-	-	-	-
LAGTOY	Backdoor	-	Windows	-	Exploiting Internet-Facing Vulnerabilities
Cactus	Ransomware	-	Windows	-	Exploiting Internet-Facing Vulnerabilities
DslogdRAT	RAT	CVE-2025-0282	Ivanti Connect Secure, Policy Secure, and ZTA Gateways		Exploiting Vulnerabilities
Hannibal Stealer	Stealer	-	Windows	-	-

Adversaries Summary

ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Earth Alux	Information Theft and Espionage	China	-	GODZILLA, VARGEIT, RAILLOAD, MASQLOADER	Windows
Lazarus	Information theft and espionage, Sabotage and destruction, Financial crime	North Korea	-	ThreatNeedle, wAgent, SIGNBT, COPPERHEDGE, Agamemnon, LPEClient	Windows, macOS
UNC5221	Information theft and espionage	China	CVE-2025-22457	TRAILBLAZE, BRUSHFIRE, SPAWNSNARE, SPAWNWAVE, SPAWNSLOTH	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ToddyCat	Information Theft and Espionage	China	CVE-2024-11859 CVE-2021-36276	-	Windows
Storm-2460	Financial gain	-	CVE-2025-29824	PipeMagic	Windows
UAC-0226	Information Theft and Espionage	-	-	GIFTEDCROOK	Windows
Shuckworm	Information Theft and Espionage	Russia	-	GammaSteel	-
APT29	Information Theft and Espionage	Russia	-	GRAPELOADER, WINELOADER	Windows

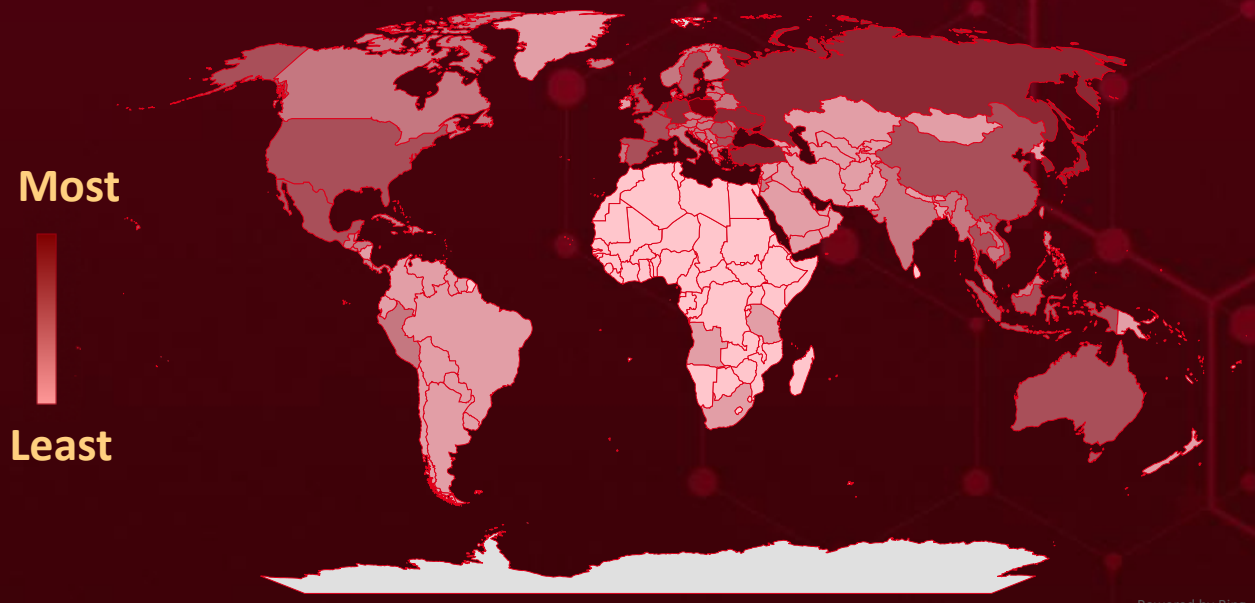
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Kimsuky	Information Theft and Espionage	North Korea	CVE-2019-0708 CVE-2017-11882	MySpy, RandomQuery, KimaLogger	Windows Server, Microsoft Office
Billbug	Information Theft and Espionage	China	-	Sagerunex, ChromeKatz, CredentialKatz	Windows
ToyMaker	Information theft and espionage, Financial crime	-	-	LAGTOY, Cactus ransomware	Windows

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
Microsoft	Mail server	Microsoft Exchange Server
	Server OS	Windows Server: 2008 – 2025
	Operating system	Windows: 10 - 11 24H2
	Productivity software suite	Microsoft Office
	Container Builder	Kubernetes ingress-nginx versions: All versions prior to v1.11.0, v1.11.0 to v1.11.4, and v1.12.0
CrushFTP	Secure file transfer server	CrushFTP versions 10.0.0 through 10.8.3 and 11.0.0 through 11.3.0
CISCO	Management tool	Cisco Smart Licensing Utility versions 2.0.0, 2.1.0, and 2.2.0
Gladinet	EFSS platform	Gladinet CentreStack through 16.1.10296.56315
eset	Endpoint Devices	ESET Multiple Products
DELL	Firmware/utility driver	Dell DBUtilDrv2.sys Driver
intel	Network interface diagnostic tool	iQVW32.SYS: Before 1.3.1.0; iQVW64.SYS: Before 1.3.1.0

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
	Operating System	macOS Prior to Version 15.4.1, iOS and iPadOS Prior to Version 18.4.1, tvOS Prior to Version 18.4.1, visionOS Prior to Version 2.4.1
	Distributed programming platform	All Erlang/OTP SSH servers running versions: OTP-27.3.2 and earlier OTP-26.2.5.10 and earlier OTP-25.3.2.19 and earlier
	Web-based email client	Active! mail 6 BuildInfo: 6.60.05008561 and earlier
	JavaScript library	xrpl.js Versions 4.2.1, 4.2.2, 4.2.3, 4.2.4 and Version 2.14.2
	SAP application platform.	SAP NetWeaver Version 7.50
	Web-based management interface	Commvault Versions 11.36.0 - 11.36.45, 11.32.0 - 11.32.88, 11.28.0 - 11.28.140, 11.20.0 - 11.20.216
	SSL VPN	Ivanti Connect Secure: 22.7R2 through 22.7R2.4
	Network Access Control (NAC)	Ivanti Policy Secure: 22.7R1 through 22.7R1.2
	Zero Trust Access	Ivanti Neurons for ZTA gateways: 22.7R2 through 22.7R2.3

Targeted Countries



Color	Countries
	Poland
	Russia
	Turkey
	South Korea
	Netherlands
	Germany
	Ukraine
	Japan
	Thailand
	Singapore
	Romania
	Belgium
	Sweden
	Bulgaria
	Mexico
	China
	Australia
	France
	Spain
	Indonesia

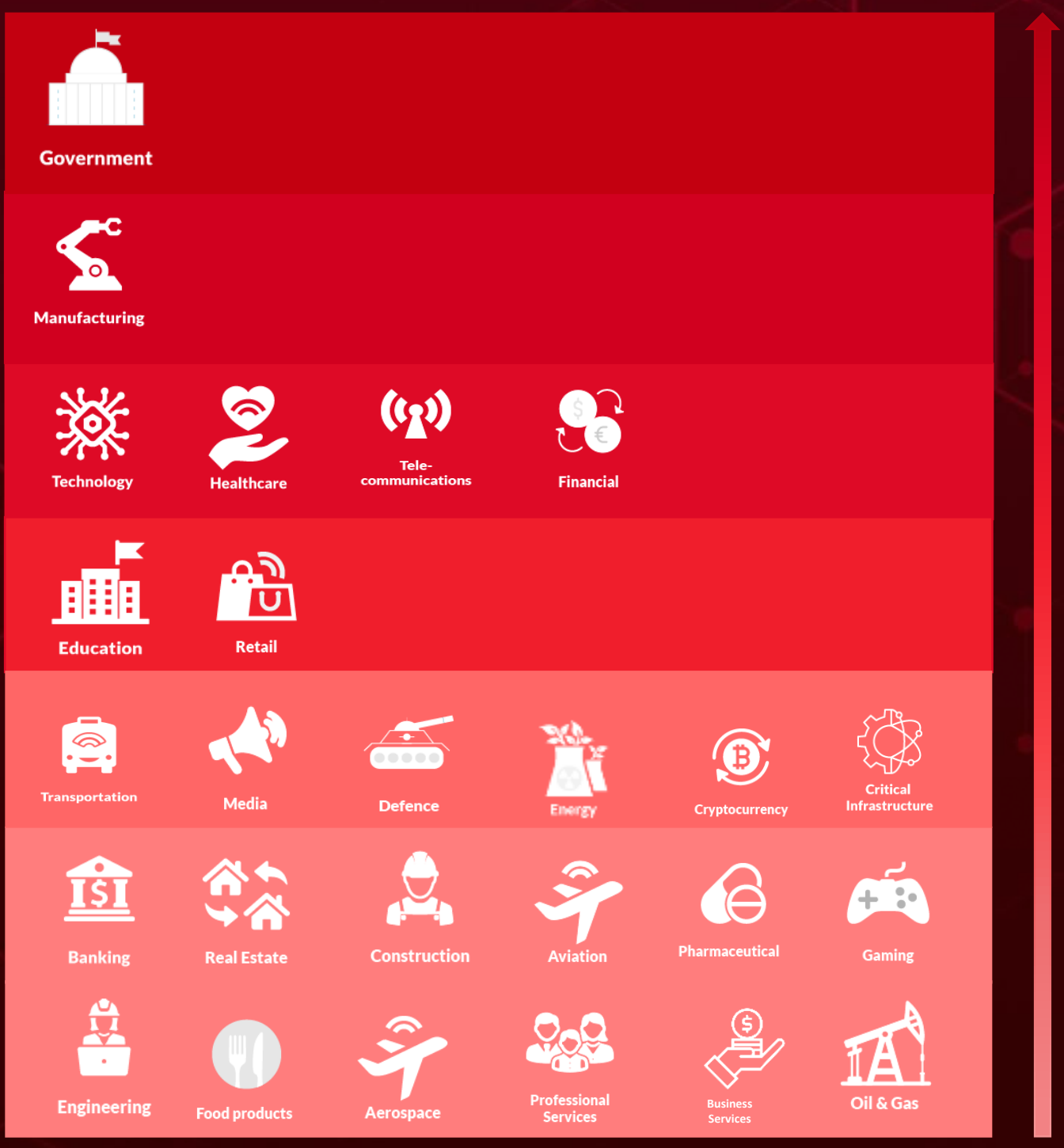
Color	Countries
	Switzerland
	Vietnam
	United Kingdom
	United States
	North Macedonia
	Austria
	Croatia
	El Salvador
	Bahamas
	Estonia
	Philippines
	Finland
	Serbia
	Brunei
	Taiwan
	Albania
	Myanmar
	Greece
	Panama
	Grenada

Color	Countries
	Portugal
	Guatemala
	Saint Lucia
	Haiti
	Slovakia
	Honduras
	Czech Republic
	Hungary
	Timor-Leste
	Iceland
	Dominican Republic
	India
	Andorra
	Belize
	Norway
	Italy
	Peru
	Jamaica
	Antigua and Barbuda
	Cambodia
	Costa Rica

Color	Countries
	Jordan
	Saint Kitts and Nevis
	Laos
	San Marino
	Canada
	Cuba
	Belarus
	Slovenia
	Luxembourg
	Cyprus
	Malaysia
	Denmark
	Malta
	Dominica
	Bosnia and Herzegovina
	Trinidad and Tobago
	Moldova
	Barbados
	Monaco
	Montenegro

Color	Countries
	Liechtenstein
	Lithuania
	Latvia
	United States Virgin Islands
	South Africa
	Puerto Rico
	Holy See
	Greenland
	Hong Kong
	Paraguay
	Azerbaijan
	Samoa
	Angola
	Syria
	Iran
	Guam
	Iraq
	Venezuela
	Israel
	Ecuador
	Kazakhstan
	Kuwait

Targeted Industries



TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1068** Exploitation for Privilege Escalation	**T1566** Phishing	**T1027** Obfuscated Files or Information
T1588 Obtain Capabilities	**T1204** User Execution	**T1588.005** Exploits	**T1588.006** Vulnerabilities	**T1203** Exploitation for Client Execution
T1041 Exfiltration Over C2 Channel	**T1083** File and Directory Discovery	**T1082** System Information Discovery	**T1574** Hijack Execution Flow	**T1140** Deobfuscate/Decode Files or Information
T1057 Process Discovery	**T1059.001** PowerShell	**T1070** Indicator Removal	**T1204.002** Malicious File	**T1566.002** Spearphishing Link
T1078 Valid Accounts	**T1036** Masquerading	**T1105** Ingress Tool Transfer	**T1071** Application Layer Protocol	**T1574.002** DLL Side-Loading

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
GolangGhost	SHA256	0cbbf7b2b15b561d47e927c37f6e9339fe418badf49fa5f6fc5c49f0dc981100, ef9f49f14149bed09ca9f590d33e07f3a749e1971a31cb19a035da8d84f97aa0, 6e186ada6371f5b970b25c78f38511af8d10faaeaed61042271892a327099925, ba81429101a558418c80857781099e299c351b09c8c8ad47df2494634a5332dc, bfac94bfb53b4c0ac346706b06296353462a26fa3bb09fbfc99e3ca090ec127e
FrostyFerret	SHA256	b7b9e7637a42b5db746f1876a2ecb19330403ecb4ec6f5575db4d94df8ec79e8
PipeMagic	SHA256	2712b5f08fff88a78045cf98e6894b521f4b7af3f74aa385584f1f01aa5b6ebe
Hellcat	SHA256	4b2edadc8f90e9fcc976f02a9eda1640cd92c07718c0271842fbd4ca7e2906e2, 53c09e57cea028c0439477cd90bcf8f981067a120a2fb7b86d0f13017727a93a, 5b492a70c2bbded7286528316d402c89ae5514162d2988b17d6434ead5c8c274, 6924479c42b3732e0d57b34714b7210e14655ee1ca570ae4aab1d90c3f6c6428, 93aa8b0f950a7ea7f0cee2ba106efaacf673bb2b504ca0b9e87f9ea41acfb599, b8e71845cc8ccd668a3436d1952a6c57649974bb8399e599dc33afc4c0843be7, dcd7995038ad4839e88e5bb3bf654b4f7c2ad09780a39c9d47596ce717fd4ac2
	MD5	931396d6332709956237cf76ee246b01
	SHA1	b834d9dbe2aed69e0b1545890f0be6f89b2a53c7
	Tor Address	hellcakbszllztlyqbjzwcbdhfrodx55wq77kmftp4bhnhsnn5r3odad[.]onion

Attack Name	TYPE	VALUE
GRAPELOADER	SHA256	d931078b63d94726d4be5dc1a00324275b53b935b77d3eed1712461f0c180164, 24c079b24851a5cc8f61565176bbf1157b9d5559c642e31139ab8d76bbb320f8
WINELOADER	SHA256	adfe0ef4ef181c4b19437100153e9fe7aed119f5049e5489a36692757460b9f8
Interlock	SHA256	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f, 4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9, 33dc991e61ba714812aa536821b073e4274951a1e4a9bc68f71a802d034f4fb9, b85586f95412bc69f3dceb0539f27c79c74e318b249554f0eace45f3f073c039, a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642, 0fff8fb05cee8dc4a4f7a8f23fa2d67571f360a3025b6d515f9ef37dfdb4e2ea, e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1, f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e
MySpy	SHA256	16bb4855a7412ce2bd63b2bcc0de3add1e7ca8c0f22acf8172e760931ef3e7da
KimaLogger	SHA256	68c648a75976911609713dfa33957bf4399cc074b986ec88c85d0ec15e75d640
	MD5	184a4f3f00ca40d10790270a20019bb4
Sagerunex	SHA256	4b430e9e43611aa67263f03fd42207c8ad06267d9b971db876b6e62c19a0805e, 3fb81913c2daf36530c9ae011feebeb5bc61432969598e2dfaa52fc2ce839f20
ChromeKatz	SHA256	2e1c25bf7e2ce2d554fca51291eaeb90c1b7c374410e7656a48af1c0afa34db4, 6efb16aa4fd785f80914e110a4e78d3d430b18cbdd6ebd5e81f904dd58baae61, ea87d504aff24f7daf026008fa1043cb38077eccec9c15bbe24919fc413ec7c7
CredentialKatz	SHA256	e3869a6b82e4cf54cc25c46f2324c4bd2411222fd19054d114e7ebd32ca32cd1, 29d31cfc4746493730cda891cf88c84f4d2e5c630f61b861acc31f4904c5b16d

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-31161</td><td>  </td><td rowspan="2">CrushFTP versions 10.0.0 through 10.8.3 and 11.0.0 through 11.3.0</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:crushftp:crushftp:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">CrushFTP Authentication Bypass Vulnerability</td><td>  </td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td></td><td>CWE-287</td><td>T1556: Modify Authentication Process</td><td>https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update, https://www.crushftp.com/download.html</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-22457</td><td>  </td><td rowspan="2">Ivanti Connect Secure: 22.7R2.5 and prior Pulse Connect Secure (EoS): 9.1R18.9 and prior Ivanti Policy Secure: 22.7R1.3 and prior ZTA Gateways: 22.8R2 and prior</td><td rowspan="2">UNC5221</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*</td><td rowspan="2">TRAILBLAZE, BRUSHFIRE, SPAWNSNARE, SPAWNWAVE, SPAWNSLOTH</td></tr>
<tr><td rowspan="2">Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-121</td><td>T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation</td><td>https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20439	✗	Cisco Smart Licensing Utility versions 2.0.0, 2.1.0, and 2.2.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:smart_license_utility:*:*:*:*:*:*:*:*	-
Cisco Smart Licensing Utility Static Credential Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-912	T1190: Exploit Public-Facing Application; T1212: Exploitation for Credential Access	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20440	✗	Cisco Smart Licensing Utility versions 2.0.0, 2.1.0, and 2.2.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:smart_license_utility:*:*:*:*:*:*:*:*	-
Cisco Smart Licensing Utility Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-532	T1006: File and Directory Discovery; T1082: System Information Discovery	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-29824	✗	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	Storm-2460
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	PipeMagic
Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30406	✗	Gladinet CentreStack through 16.1.10296.56315	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gladinet:centrestack:*:*:*:*:*:*:*:*	-
Gladinet CentreStack Use of Hard-coded Cryptographic Key Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-321	T1552.004 Unsecured Credentials: Private Keys; T1190 : Exploit Public-Facing Application	https://www.centrestack.com/p/gce_latest_release.html

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-11859</td><td>  </td><td rowspan="2">ESET Multiple Products</td><td rowspan="2">ToddyCat</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:eset:multiple_products:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">ESET Multiple Products DLL Search Order Hijacking Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-427</td><td>T1574.001 Hijack Execution Flow: DLL Search Order Hijacking; T1059: Command and Scripting Interpreter</td><td>https://support.eset.com/en/ca8810-dll-search-order-hijacking-vulnerability-in-eset-products-for-windows-fixed</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2021-36276</td><td>  </td><td rowspan="2">Dell DBUtilDrv2.sys Driver</td><td rowspan="2">ToddyCat</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:dell:dbutildrv2.sys_firmware:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Dell DBUtilDrv2.sys Driver Insufficient Access Control Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-285</td><td>T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation</td><td>https://www.dell.com/support/kbdoc/en-us/000190105/dsa-2021-152-dell-client-platform-security-update-for-an-insufficient-access-control-vulnerability-in-the-dell-dbutildrv2-sys-driver</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2015-2291</td><td>  </td><td rowspan="2">iQVW32.SYS: Before 1.3.1.0;
iQVW64.SYS: Before 1.3.1.0</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:intel:ethernet_diagnostics_driver_iqvw32.sys:1.03.0.7:*:*:*:*:*:*:*
cpe:2.3:a:intel:ethernet_diagnostics_driver_iqvw64.sys:1.03.0.7:*:*:*:*:*:*:*
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:*</td><td rowspan="2">DOGE BIG BALLS Ransomware</td></tr>
<tr><td>Intel Ethernet Diagnostics Driver for Windows Denial-of-Service Vulnerability</td><td>  </td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-20</td><td>T1059: Command and Scripting Interpreter;
T1068: Exploitation for Privilege Escalation;
T1499: Endpoint Denial of Service</td><td>https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-31200</td><td>  </td><td rowspan="2">macOS Prior to Version 15.4.1, iOS and iPadOS Prior to Version 18.4.1, tvOS Prior to Version 18.4.1, visionOS Prior to Version 2.4.1</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:*:*
cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:*:*
cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Apple Multiple Products Memory Corruption Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-787</td><td>T1059: Command and Scripting Interpreter;
T1566: Phishing</td><td>https://support.apple.com/en-us/108382 , https://support.apple.com/en-us/118575 , https://support.apple.com/en-us/108414 , https://support.apple.com/en-us/118481</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-31201		macOS Prior to Version 15.4.1, iOS and iPadOS Prior to Version 18.4.1, tvOS Prior to Version 18.4.1, visionOS Prior to Version 2.4.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:*:* cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*:*	-
Apple Multiple Products Arbitrary Read and Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation; T1203: Exploitation for Client Execution	https://support.apple.com/en-us/108382 , https://support.apple.com/en-us/118575 , https://support.apple.com/en-us/108414 , https://support.apple.com/en-us/118481

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24054	✗	Windows Server 2008 – 2025 Windows 10 – 11 24H2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows NTLM Hash Disclosure Spoofing Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1566: Phishing; T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24054

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43451	✗	Windows Server 2008 – 2025 Windows 10 -11 24H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows NTLMv2 Hash Disclosure Spoofing Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1566: Phishing; T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32433	✗ ZERO-DAY	All Erlang/OTP SSH servers running versions: OTP-27.3.2 and earlier OTP-26.2.5.10 and earlier OTP-25.3.2.19 and earlier	-
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:erlang:otp:*:*:*:*:*:*:*:*	-
Erlang/OTP Unauthenticated Remote Code Execution Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINKS**
	CWE-306	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation; T1210: Exploitation of Remote Services	https://github.com/erlang/otp/releases, https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11882	✗ ZERO-DAY	Microsoft Office	Kimsuky
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:office:-:*:*:*:*:*:*:*:*	MySpy, RandomQuery, KimaLogger
Microsoft Office Memory Corruption Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-119	T1059: Command and Scripting Interpreter; T1005: Data from Local System	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-42599	✗	Active! mail 6 BuildInfo: 6.60.05008561 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:qualitia:active_mail:*:*:*:*:*:*:*:*	-
Qualitia Active! Mail Stack Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1574: Hijack Execution Flow	https://jvn.jp/en/jp/JVN22348866/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32965	✗	xrpl.js Versions 4.2.1, 4.2.2, 4.2.3, 4.2.4 and Version 2.14.2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:xrpl.js:xrpl.js:*:*:*:*:*:*:*:*	-
xrpl.js Supply Chain Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1059: Command and Scripting Interpreter; T1059.007: JavaScript ;T1195: Supply Chain Compromise	https://github.com/XRPLF/xrpl.js/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-31324	✗	SAP NetWeaver Version 7.50	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sap:sap_netweaver:7.50.*.*.*.*.*.*.*	-
SAP NetWeaver Unrestricted File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1505.003: Server Software Component: Web Shell	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-3928	✗	Commvault Versions 11.36.0 - 11.36.45, 11.32.0 - 11.32.88, 11.28.0 - 11.28.140, 11.20.0 - 11.20.216	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:commvault:commvault:*:*:*:*:*:*:*:*	-
Commvault Web Server Unspecified Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1059: Command and Scripting Interpreter; T1505.003: Server Software Component: Web Shell	https://documentation.commvault.com/11.20/download_software.html

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-0282</td><td>✗</td><td rowspan="2">Ivanti Connect Secure: 22.7R2 through 22.7R2.4
Ivanti Policy Secure: 22.7R1 through 22.7R1.2
Ivanti Neurons for ZTA gateways: 22.7R2 through 22.7R2.3</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✓</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*
cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*:*:*</td><td rowspan="2">DslogdRAT</td></tr>
<tr><td rowspan="3">Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-121</td><td>T1059: Command and Scripting Interpreter; T1210: Exploitation of Remote Services</td><td>https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283</td></tr>
</table>

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GODZILLA	GODZILLA is a web shell that delivers first-stage backdoors, operating entirely in memory to evade traditional disk-based detection methods. It uses AES encryption for secure communication, making detection even more challenging.	Exploiting Vulnerabilities in Exposed Servers	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Evasion of Detection, Increased Risk of Further Attacks	Windows
Web Shell			
ASSOCIATED ACTOR			**PATCH LINK**
Earth Alux			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
VARGEIT	VARGEIT is a primary backdoor executed via shellcode injection using a debugger script. It enables attackers to collect system and drive information, gather data on running processes, and interact with the Windows Defender Firewall. VARGEIT also allows for directory management, including creating, setting, searching, and deleting directories, as well as reading from and writing to files. Additionally, it can execute command lines and inject miscellaneous tools into controlled instances of mspaint or conhost.	GODZILLA facilitates the delivery	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Tool Injection into Controlled Processes, Unauthorized Directory Management	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Earth Alux			-

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
RAILLOAD	RAILLOAD is a loader component with a base64-encoded configuration. Its decryption process involves first decoding the base64 string, followed by AES-128 CBC mode decryption. In some variants, RAILLOAD includes execution guardrails to control its operation.	VARGEIT deploys via DLL side-loading	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Increased Attack Surface, Evasion of Detection	Windows
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
Earth Alux			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MASQLOADER	MASQLOADER is a loader that, in recent versions, incorporates an anti-API hooking technique. It achieves this by overwriting the code section of ntdll.dll in memory with the original code from the file, effectively removing any API hooks inserted by security and monitoring tools. This method enables MASQLOADER and the injected payload to evade detection by circumventing monitoring tools that rely on intercepted API calls.	Side-loaded DLL or shellcode	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Bypasses Security Measures, Enabling Further Exploitation	Windows
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
Earth Alux			-

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
GolangGhost	GolangGhost is an interpreted Go backdoor crafted for remote control and data exfiltration, specifically targeting Windows and macOS systems. It features the ability to steal data from Chrome browsers and, once the victim is registered with the command-and-control (C2) server, it can execute a range of commands.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Remote Control, Chrome Browser Data Theft	Windows, macOS
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus Group			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FrostyFerret	FrostyFerret is designed to steal the user's system password and uses the same icon as Chrome to disguise itself.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Password Theft	Windows, macOS
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus Group			-

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
TRAILBLAZE	TRAILBLAZE is a minimal, in-memory-only dropper written in raw C, utilizing syscalls to ensure it remains compact enough to fit within a shell script as Base64.	Exploiting vulnerabilities	CVE-2025-22457
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		Evasion of Detection, System Compromise	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5221			https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
BRUSHFIRE	BRUSHFIRE is a passive backdoor written in C that hooks into the SSL_read function. It first executes the original SSL_read, checks if the returned data starts with a specific string, and if so, XOR decrypts and runs the contained shellcode. If the shellcode returns a value, the backdoor sends it back using SSL_write.	Exploiting vulnerabilities	CVE-2025-22457
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Exfiltration, Remote Access	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5221			https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457

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
SPAWNSNARE	SPAWNSNARE is a C-based utility designed for Linux that extracts the uncompressed Linux kernel image and encrypts it using AES without requiring any command-line tools.	Exploiting vulnerabilities	CVE-2025-22457
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Tool		Exposure of sensitive system information	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5221			https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SPAWNWAVE	SPAWNWAVE is an advanced version of SPAWNANT that incorporates features from other malware in the SPAWN ecosystem. It shares similarities with the publicly reported SPAWNCHIMERA and RESURGE malware families.	Exploiting vulnerabilities	CVE-2025-22457
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5221			https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457

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
SPAWNSLOTH	SPAWNSLOTH is a log tampering tool injected into the dslogserver process. It disables logging and prevents log forwarding to an external syslog server while the SPAWNSNAIL backdoor is active.	Exploiting vulnerabilities	CVE-2025-22457
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Log Tampering, Increased Persistence	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5221			https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PipeMagic	PipeMagic is a sophisticated backdoor Trojan malware distributed via fake ChatGPT applications developed in Rust, targeting entities globally since 2022. The malware uses encrypted communication through named pipes and grants attackers remote access, enabling further infections like ransomware or data theft	Exploiting vulnerabilities	CVE-2025-29824
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Remote Control, Data Exfiltration and Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Storm-2460			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824

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
GIFTEDCROOK	GIFTEDCROOK is a custom malware developed in C/C++ used in the UAC-0226 cyber-espionage campaign. It extracts sensitive data from browsers like Chrome, Edge, and Firefox, including credentials and cookies. The stolen data is exfiltrated via PowerShell commands to a Telegram bot, enabling covert communication.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
UAC-0226			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Hellcat	HellCat is a Ransomware-as-a-Service (RaaS) operation that emerged in 2024, leveraging a decentralized affiliate model to deliver customized payloads and infrastructure. It gains access through phishing or exploiting vulnerabilities, then exfiltrates data and encrypts systems in a double-extortion scheme.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Exfiltration, Financial Loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Neptune	Neptune RAT is a deceptive and dangerous malware posing as a remote access tool, spreading through platforms like GitHub and Telegram. Beneath the surface, it functions as a versatile tool for cybercriminals capable of stealing credentials, intercepting cryptocurrency transactions, monitoring user activity, and severely compromising system integrity.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Modular RAT		Data theft and Financial gain	Windows
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
PlayBoy Locker	PlayBoy Locker is a sophisticated ransomware strain operated by a group active since September 2024. Offered as a service, it provides threat actors with customizable ransomware payloads, a web-based management dashboard, and dark web-based customer support. Written in C++, the malware employs a hybrid encryption scheme that combines the HC-128 stream cipher with the Curve25519 elliptic curve algorithm to lock files. Once inside a network, it performs LDAP scans to discover other machines, attempts lateral movement by replicating itself, and terminates active processes to maximize impact. Infected files are appended with the ".PLBOY" extension, and victims receive a ransom note titled INSTRUCTIONS.txt containing payment and communication details.	phishing emails or vulnerable Remote Desktop Protocol (RDP) services	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		System Compromise, Encrypt Data	Windows, NAS, and ESXi
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ResolverRAT	ResolverRAT is a stealthy remote access trojan recently uncovered, notable for its sophisticated use of in-memory execution and runtime resolution techniques. ResolverRAT is built to evade both static and behavioral detection mechanisms. It operates entirely in memory, using strong encryption and compression to remain hidden from traditional security tools. Its capabilities include chunked data exfiltration where large files are broken into smaller pieces to mimic normal network activity and parallel command processing, allowing it to execute multiple tasks simultaneously without system instability.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft	Windows
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
DOGE BIG BALLS	DOGE BIG BALLS is a customized and rebranded variant of the Fog ransomware. Designed to do more than just encrypt files, this strain aims to confuse, intimidate, and mislead its victims. A single click initiates a stealthy PowerShell script that checks for administrative privileges before downloading and executing multiple malicious payloads. It encrypts files with a ".flocked" extension, deletes shadow copies, logs its activity, and drops a ransom note that leads victims to a Tor site. There, they're asked to pay $1,000 in Monero and, oddly, to list their top five work achievements. The malware also gathers detailed system information and adds a disturbing twist by including real personal details of an individual.	Phishing, Exploiting Vulnerability	CVE-2015-2291
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data, System Compromise	iQVW32.SYS, iQVW64.SYS
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GammaSteel	GammaSteel is an information-stealing malware designed to exfiltrate sensitive data from compromised networks. It is delivered via a stealthy PowerShell-based attack chain, allowing it to operate with minimal visibility and evade traditional detection methods. Once deployed, GammaSteel silently harvests data, targeting system information, credentials, and other valuable assets, before transmitting them to attacker-controlled servers.	Using a malicious LNK file on a USB drive	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Shuckworm			-

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
GRAPELOADER	GRAPELOADER is a recently identified initial-stage tool designed for host fingerprinting, establishing persistence, and delivering follow-on payloads. GRAPELOADER consistently features a shared code structure, obfuscation techniques, and string decryption methods. Upon execution, it gathers basic system information such as the host name and username and transmits this data to a Command and Control (C2) server. The tool then remains active, awaiting instructions or the delivery of next-stage shellcode, positioning it as a versatile component in multi-stage attack chains.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Loads WINELOADER	-
ASSOCIATED ACTOR			**PATCH LINK**
APT29			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
WINELOADER	A newer variant of the WINELOADER backdoor has emerged, embedded within a 64-bit trojanized DLL named vmtools.dll. While the file claims to export 964 functions, only one of them is used as the true entry point for malicious activity. Notably, the Export Directory reveals RVA duplicity each pair of exported functions shares the same Relative Virtual Address indicating that the DLL actually contains just 482 unique exports. This deceptive export structure, paired with the backdoor's stealthy execution, suggests a deliberate effort to evade static analysis and blend in with legitimate system components.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
APT29			-

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
Interlock	INTERLOCK is a rising ransomware group gaining attention for its technical sophistication, including malware compiled in C/C++ for both Windows and Linux systems. While the Windows variant is most commonly observed, what truly sets INTERLOCK apart is its rare and deliberate focus on FreeBSD environments an unusual target in the ransomware ecosystem. The group employs polished double-extortion tactics and operates a data leak site called “Worldwide Secrets Blog,” where stolen data is published and victims are invited to negotiate ransom terms. Once launched, these fake installers execute a PowerShell backdoor, enabling the deployment of additional tools and ultimately delivering the ransomware payload.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		System Compromise, Encrypt Data, Data Theft	Microsoft Windows, Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BerserkStealer	BerserkStealer is a credential-stealing malware designed to harvest sensitive information that can be used to facilitate lateral movement across compromised networks. It has been observed packed with the Interlock group’s custom packer, a technique also used to obfuscate other malware families linked to the group.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft	Microsoft Windows, Linux
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
LummaStealer	Lumma Stealer, also known as LummaC2 Stealer, is an information-stealing malware written in C that has been available as Malware-as-a-Service (MaaS) on Russian-speaking forums since at least August 2022. It primarily targets cryptocurrency wallets and two-factor authentication (2FA) browser extensions, stealing sensitive data from the victim's machine.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data Theft	Microsoft Windows, Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MySpy	MySpy, a mobile surveillance app often labeled as "stalkerware" for its ability to covertly track phone activity and location, has been involved in a data breach exposing user information. In a recent campaign, the Kimsuky group employed MySpy to gather system information.	Exploited the RDP vulnerability	CVE-2019-0708 CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Spyware		Privacy Invasion, Data Theft	Windows Server, Microsoft Office
ASSOCIATED ACTOR			**PATCH LINKS**
Kimsuky			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708, https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

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
RandomQuery	RandomQuery is a malware strain primarily designed for file enumeration and data exfiltration. Some variants offer expanded capabilities, including keylogging and deployment of additional specialized payloads.	Exploited the RDP vulnerability	CVE-2019-0708 CVE-2017-11882
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Credential Theft, Enabling Further Attacks	Windows Server, Microsoft Office
Keylogger			
ASSOCIATED ACTOR			**PATCH LINKS**
Kimsuky			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708, https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
KimaLogger	KimaLogger is a stealthy keylogger used to monitor user activity, capture credentials, and exfiltrate sensitive data to attacker-controlled C2 servers.	Exploited the RDP vulnerability	CVE-2019-0708 CVE-2017-11882
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Credential Theft, Data Exfiltration	Windows Server, Microsoft Office
Keylogger			
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708, https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

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
Sagerunex	Sagerunex backdoor variants employ obfuscation to evade detection and use both traditional C2 infrastructure and legitimate platforms like Dropbox, Twitter, and Zimbra for stealthy communication and data exfiltration.	Exploiting vulnerabilities in public-facing applications, spear-phishing, or credential abuse.	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Exfiltration, Persistence and Control	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Billbug			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ChromeKatz	ChromeKatz stealer is capable of extracting both stored credentials and cookies from the Chrome browser.	Exploiting vulnerabilities in public-facing applications, spear-phishing, or credential abuse.	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Credential Theft, Session Hijacking	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Billbug			-

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
CredentialKatz	CredentialKatz is a stealer designed to extract credentials stored in the Chrome browser.	Exploiting vulnerabilities in public-facing applications, spear-phishing, or credential abuse.	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Credential Theft, Privacy Violation	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Billbug			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ThreatNeedle	The ThreatNeedle variant, a hallmark backdoor of Lazarus, was discovered running as a subprocess of Cross EX, a legitimate Korean software. It employed advanced encryption, generating Curve25519 key pairs for ChaCha20-encrypted communications with the C2. ThreatNeedle facilitated stealthy data exfiltration and persistence via system services like IKEEXT or SSP registration.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Stealthy Persistence, Facilitation of Further Malware Deployment	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

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
wAgent	wAgent, a malicious loader documented in 2020, was disguised as liblzma.dll and executed via the command line. It can receive data in both form-data and JSON formats, depending on the C2 server it successfully connects to.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Covert Execution, Facilitation of Further Malware Deployment	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SIGNBT	The latest version of SIGNBT has limited remote control capabilities, focusing primarily on executing additional payloads. The C2 server is hardcoded, without relying on configuration files. The malware receives an RSA public key from the C2, encrypts a randomly generated AES key, and uses it to encrypt all traffic.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Covert Communication, Potential for Lateral Movement	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

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
COPPERHEDGE	COPPERHEDGE, a dropper and variant of Manuscrypt, was used in the DeathNote cluster attacks. The latest version retrieves C2 configuration data from Alternate Data Streams (ADS) and communicates with the C2 via HTTP, using three to four randomly named parameters per request. Lazarus primarily deployed COPPERHEDGE for internal reconnaissance during the operation.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		Internal Reconnaissance, Facilitation of Further Malware Deployment	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Agamemnon	The Agamemnon downloader is designed to fetch and execute additional payloads from its C2 server. It processes commands by parsing parameters delimited by ";;" received from the C2.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Payload Delivery, Command Execution	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LPEClient	LPEClient is a tool used for victim profiling and payload delivery, previously observed in attacks targeting defense contractors and the cryptocurrency sector.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Tool		Payload Delivery, Targeted Operations	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

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
CrazyHunter	CrazyHunter is a Go-based ransomware first observed in January 2025, built on the open-source Prince encryptor. Notably, around 80% of the toolkit used in its attack chain consists of repurposed open-source tools—a strategic choice that lowers development costs and complicates attribution.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial Loss, Data Exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LAGTOY	LAGTOY is a custom backdoor designed to extract credentials from targeted enterprises. It enables the creation of reverse shells and the execution of commands on compromised endpoints. LAGTOY employs a time-based logic to determine whether to execute commands or remain dormant for a specified duration.	Exploiting Internet-Facing Vulnerabilities	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Remote Command Execution, Targeted Exploitation	Windows
ASSOCIATED ACTOR			**PATCH LINK**
ToyMaker			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cactus	Cactus employed various remote administration tools, such as eHorus, RMS, and AnyDesk, across different endpoints to sustain long-term access. They conducted extensive network reconnaissance, deployed remote management tools, executed a ransomware payload, exfiltrated sensitive data, and deleted shadow volume copies to hinder data recovery.	Exploiting Internet-Facing Vulnerabilities	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Exfiltration, Financial Loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
ToyMaker			-

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
DslogdRAT	DslogdRAT is a new RAT targeting Japanese organizations, installed via a zero-day Ivanti Connect Secure vulnerability (CVE-2025-0282). It deploys with a web shell, enabling command execution and communication with a C2 server.	Exploiting Vulnerabilities	CVE-2025-0282
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System compromise and data exfiltration	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
-			https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Hannibal Stealer	Hannibal Stealer is a data-stealing malware that extracts credentials, cryptocurrency wallet information, and other sensitive data from infected systems. It targets various applications and also hijacks clipboards for cryptocurrency transactions.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Data theft	Windows
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.

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Earth Alux	China	Government, Technology, Logistics, Manufacturing, Telecommunications, IT Services, Retail	Asia-Pacific (APAC) and Latin American
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	GODZILLA, VARGEIT, RAILLOAD, MASQLOADER	Windows

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1083: File and Directory Discovery; T1055: Process Injection; T1480: Execution Guardrails; T1588: Obtain Capabilities; T1588.002: Tool; T1588.006: Vulnerabilities; T1211: Exploitation for Defense Evasion; T1564: Hide Artifacts; T1070: Indicator Removal; T1070.004: File Deletion; T1070.009: Clear Persistence; T1057: Process Discovery; T1570: Lateral Tool Transfer; T1543: Create or Modify System Process; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1005: Data from Local System; T1001: Data Obfuscation; T1041: Exfiltration Over C2 Channel; T1588.005: Exploits; T1070.006: Timestomp; T1053: Scheduled Task/Job; T1027: Obfuscated Files or Information; T1505.003: Web Shell; T1082: System Information Discovery; T1036: Masquerading; T1135: Network Share Discovery; T1105: Ingress Tool Transfer; T1518.001: Security Software Discovery

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 Lazarus Group (aka UNC2970, Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor, Citrine Sleet, Gleaming Pisces)	North Korea	Cryptocurrency, centralized finance (CeFi), Software, IT, Financial, Semiconductor Manufacturing, and Telecommunications Industries	Worldwide
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	-	ThreatNeedle, wAgent, SIGNBT, COPPERHEDGE, Agamemnon, LPEClient	Windows, macOS

TTPs

TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; T1584: Compromise Infrastructure; T1584.001: Domains; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1189: Drive-by Compromise; T1068: Exploitation for Privilege Escalation; T1583: Acquire Infrastructure; T1583.001: Domains; T1036: Masquerading; T1608: Stage Capabilities; T1608.004: Drive-by Target; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1543.003: Windows Service; T1574: Hijack Execution Flow; T1574.001: DLL; T1547: Boot or Logon Autostart Execution; T1547.005: Security Support Provider; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1573.001: Symmetric Cryptography; T1105: Ingress Tool Transfer; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1027.009: Embedded Payloads; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1570: Lateral Tool Transfer; T1564: Hide Artifacts; T1564.004: NTFS File Attributes; T1082: System Information Discovery; T1083: File and Directory: Discovery; T1057: Process Discovery; T1049: System Network Connections Discovery; T1016: System Network Configuration Discovery; T1087: Account Discovery; T1087.001: Local Account; T1087.002: Domain Account; T1569: System Services; T1569.002: Service Execution; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1135: Network Share Discovery; T1007: System Service Discovery

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UNC5221 (aka UTA0178, Red Dev 61)</td><td>China</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-22457</td><td>TRAILBLAZE, BRUSHFIRE, SPAWNSNARE, SPAWNWAVE, SPAWNSLOTH</td><td>Ivanti Connect Secure, Policy Secure, and ZTA Gateways</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0003: Persistence; TA0011: Command and Control; T1068: Exploitation for Privilege Escalation; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1588.005: Exploits; T1588.006: Vulnerabilities; T1070.004: File Deletion; T1070: Indicator Removal; T1027: Obfuscated Files or Information; T1204: User Execution; T1059: Command and Scripting Interpreter</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 ToddyCat	China	-	Worldwide
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2024-11859 CVE-2021-36276	-	Windows
TTPs			
TA0042: Resource Development; TA0005: Defense Evasion; T1588: Obtain Capabilities; T1574: Hijack Execution Flow; TA0007: Discovery; TA0003: Persistence; T1036: Masquerading; T1059: Command and Scripting Interpreter; TA0002: Execution; TA0011: Command and Control; TA0004: Privilege Escalation; T1068: Exploitation for Privilege Escalation; T1588.005: Exploits; T1027: Obfuscated Files or Information; T1574.001: DLL Search Order Hijacking; T1211: Exploitation for Defense Evasion; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1588.006: Vulnerabilities; T1082: System Information Discovery; T1083: File and Directory Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Storm-2460	-	-	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
	CVE-2025-29824	PipeMagic	Windows
TTPs			
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0011: Command and Control; T1055: Process Injection; T1059: Command and Scripting Interpreter; T1555: Credentials from Password Stores; T1071: Application Layer Protocol; T1562: Impair Defenses; T1486: Data Encrypted for Impact; T1082: System Information Discovery; T1547: Boot or Logon Autostart Execution; T1005: Data from Local System; T1588.006: Vulnerabilities; T1588.005: Exploits; T1588: Obtain Capabilities			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UAC-0226</td><td>-</td><td rowspan="2">Military, Law Enforcement Agencies, Government</td><td rowspan="2">Ukraine</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft and Espionage</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TARGETED CVE</td><td>-</td><td>GIFTEDCROOK</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0006: Credential Access; TA0005: Defense Evasion; T1059: Command and Scripting Interpreter; T1140: Deobfuscate/Decode Files or Information; TA0010: Exfiltration; TA0009: Collection; T1566.001: Spearphishing Attachment; T1027: Obfuscated Files or Information; TA0002: Execution; TA0011: Command and Control; T1059.001: PowerShell; TA0007: Discovery; TA0003: Persistence; T1204: User Execution; T1082: System Information Discovery; T1555: Credentials from Password Stores; T1204.002: Malicious File; T1539: Steal Web Session Cookie ; T1041: Exfiltration Over C2 Channel; T1567.002: Exfiltration to Cloud Storage; T1567: Exfiltration Over Web Service; T1555.003: Credentials from Web Browsers; T1566: Phishing</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Shuckworm (aka Primitive Bear, Winterflounder, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Gamaredon, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard)</td><td>Russia</td><td rowspan="2">Military</td><td rowspan="2">Ukraine</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td rowspan="2">ASSOCIATED ATTACKS/RANSOMWARE</td><td rowspan="2">AFFECTED PRODUCTS</td></tr>
<tr><td>TARGETED CVEs</td></tr>
<tr><td>-</td><td>GammaSteel</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0007: Discovery; TA0005: Defense Evasion; TA0010: Exfiltration; TA0011: Command and Control; T1091: Replication Through Removable Media; T1567: Exfiltration Over Web Service; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1059.001: PowerShell; T1132: Data Encoding; T1132.001: Standard Encoding; T1001: Data Obfuscation; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1547.009: Shortcut Modification; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1027: Obfuscated Files or Information; T1033: System Owner/User Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 APT29 (aka Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo, Blue Kitsune, G0016, Midnight Blizzard, SeaDuke, TA421, UAC-0029, UNC3524, Cranefly , TEMP.Monkeys, Blue Dev 5, NobleBaron, Solar Phoenix, Earth Koshchei)	Russia	Embassies, Government, and Diplomatic entities	Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	GRAPELOADER, WINELOADER	Windows

TTPs
TA0007: Discovery; TA0005: Defense Evasion; TA0010: Exfiltration; TA0002: Execution; TA0003: Persistence; TA0001: Initial Access; TA0009: Collection; TA0011: Command and Control; T1566: Phishing; T1204: User Execution; T1204.001: Malicious Link; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1005: Data from Local System; T1566.002: Spearphishing Link; T1059.001: PowerShell; T1059: Command and Scripting Interpreter; T1218: System Binary Proxy Execution; T1016: System Network Configuration Discovery; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1041: Exfiltration Over C2 Channel; T1027.009: Embedded Payloads; T1070.001: Clear Windows Event Logs; T1070: Indicator Removal; T1573.001: Symmetric Cryptography; T1573: Encrypted Channel; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1082: System Information Discovery; T1656: Impersonation

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 

Kimsuky (aka Velvet Chollima, Larva-24005, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394, Sparkling Pisces, Springtail)</td><td>North Korea</td><td rowspan="3">Software Companies, Energy, Finance</td><td rowspan="3">South Korea, Japan, United States, China, Germany, Singapore, South Africa, Netherlands, Mexico, Vietnam, Belgium, United Kingdom, Canada, Thailand, and Poland</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2019-0708
CVE-2017-11882</td><td>MySpy, RandomQuery, KimaLogger</td><td>Windows Server, Microsoft Office</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1059: Command and Scripting Interpreter; T1566: Phishing; T1566.001: Spearphishing Attachment; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1082: System Information Discovery; T1056: Input Capture; T1056.001: Keylogging; T1133: External Remote Services; T1190: Exploit Public-Facing Application; T1204: User Execution; T1560: Archive Collected: Data; T1567: Exfiltration Over Web Service; T1595: Active Scanning; T1595.002: Vulnerability Scanning; T1039: Data from Network Shared Drive</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 Billbug (aka Lotus Blossom, Lotus Panda, Spring Dragon, Dragonfish, Thrip, Bronze Elgin, CTG-8171, ATK 1, ATK 78, RADIUM, Raspberry Typhoon, Red Salamander)	China	Government, Aviation, Telecommunications, and Construction	Southeast Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Sagerunex, ChromeKatz, CredentialKatz	Windows

TTPs
TA0043: Reconnaissance;TA0010: Exfiltration; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; T1078.001: Default Accounts; T1078: Valid Accounts; T1566.001: Spearphishing Attachment; T1566: Phishing; T1134.002:Create Process with Token; T1027: Obfuscated Files or Information; T1134: Access Token Manipulation; T1082: System Information Discovery; T1021: Remote Services; T1071.001: Web Protocols; T1555: Credentials from Password Stores; T1041: Exfiltration Over C2 Channel; T1560.001: Archive via Utility; T1560: Archive Collected Data; T1555.003: Credentials from Web Browsers; T1071: Application Layer Protocol; T1573: Encrypted Channel; T1090: Proxy; T1090.002: External Proxy; T1018: Remote System Discovery; T1021.004: SSH; T1204: User Execution; T1140: Deobfuscate/Decode Files or Information; T1070.006: Timestomp; T1070: Indicator Removal; T1204.002: Malicious File; T1547.001: Registry Run Keys / Startup Folder; T1547: Boot or Logon Autostart Execution; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
ToyMaker</td><td>-</td><td rowspan="2">Critical infrastructure</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Financial crime</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>LAGTOY, Cactus ransomware</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0010: Exfiltration; TA0040: Impact; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; T1190: Exploit Public-Facing Application; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1082: System Information Discovery; T1590: Gather Victim Network Information; T1136: Create Account; T1003: OS Credential Dumping; T1560: Archive Collected Data; T1048: Exfiltration Over Alternative Protocol; T1543: Create or Modify System Process; T1018: Remote System Discovery; T1070: Indicator Removal; T1070.007: Clear Network Connection History and Configurations; T1070.009: Clear Persistence; T1608.001: Upload Malware; T1070.003: Clear Command History; T1608: Stage Capabilities; T1218.007: Msiexec; T1218: System Binary Proxy Execution; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1021.004: SSH; T1021: Remote Services; T1222: File and Directory Permissions Modification; T1222.001: Windows File and Directory Permissions Modification; T1059.003: Windows Command Shell; T1098: Account Manipulation; T1490: Inhibit System Recovery</td></tr>
</table>

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1091: Replication Through Removable Media	
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	
	T1195: Supply Chain Compromise	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
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
	T1106: Native API	
	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	T1098: Account Manipulation	
	T1133: External Remote Services	
	T1136: Create Account	
	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1546: Event Triggered Execution	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1078: Valid Accounts	T1078.001: Default Accounts
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1547.005: Security Support Provider
		T1547.009: Shortcut Modification
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading

Tactic	Technique	Sub-technique
TA0004: Privilege Escalation	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1068: Exploitation for Privilege Escalation	
	T1098: Account Manipulation	
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1548: Abuse Elevation Control Mechanism	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1078: Valid Accounts	T1078.001: Default Accounts
TA0005: Defense Evasion	T1027: Obfuscated Files or Information	T1027.002: Software Packing
		T1027.007: Dynamic API Resolution
		T1027.009: Embedded Payloads
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
	T1055: Process Injection	T1055.002: Portable Executable Injection
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.003: Clear Command History
		T1070.004: File Deletion
		T1070.006: Timestomp
		T1070.007: Clear Network Connection History and Configurations
		T1070.009: Clear Persistence
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
		T1134.002: Create Process with Token
	T1140: Deobfuscate/Decode Files or Information	
	T1211: Exploitation for Defense Evasion	
	T1218: System Binary Proxy Execution	T1218.005: Mshta
		T1218.011: Rundll32
	T1222: File and Directory Permissions Modification	T1222.001: Windows File and Directory Permissions Modification
	T1480: Execution Guardrails	
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
	T1553: Subvert Trust Controls	T1553.005: Mark-of-the-Web Bypass
	T1556: Modify Authentication Process	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1564: Hide Artifacts	T1564.004: NTFS File Attributes

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL Search Order Hijacking
	T1620: Reflective Code Loading	
	T1656: Impersonation	
	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
TA0006: Credential Access	T1003: OS Credential Dumping	
	T1056: Input Capture	T1056.001: Keylogging
	T1110: Brute Force	
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
		T1552.004: Private Keys
	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
	T1558: Steal or Forge Kerberos Tickets	
	T1606: Forge Web Credentials	T1606.001: Web Cookies
	T1557: Adversary-in-the-Middle	T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay
TA0007: Discovery	T1007: System Service Discovery	
	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1040: Network Sniffing	
	T1049: System Network Connections Discovery	
	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	T1087.002: Domain Account
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1526: Cloud Service Discovery	
	T1614: System Location Discovery	
TA0008: Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.004: SSH
	T1210: Exploitation of Remote Services	
	T1570: Lateral Tool Transfer	
TA0009: Collection	T1005: Data from Local System	
	T1039: Data from Network Shared Drive	
	T1113: Screen Capture	
	T1115: Clipboard Data	
	T1119: Automated Collection	

Tactic	Technique	Sub-technique
TA0009: Collection	T1005: Data from Local System	
	T1039: Data from Network Shared Drive	
	T1113: Screen Capture	
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1123: Audio Capture	
	T1125: Video Capture	
	T1185: Browser Session Hijacking	
	T1557: Adversary-in-the-Middle	
	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	T1001: Data Obfuscation	
	T1008: Fallback Channels	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.002: External Proxy
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1205: Traffic Signaling	
	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	
	T1496: Resource Hijacking	
	T1499: Endpoint Denial of Service	T1499.004: Application or System Exploitation
	T1529: System Shutdown/Reboot	
	T1531: Account Access Removal	
TA0042: Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1584: Compromise Infrastructure	T1584.001: Domains
		T1584.003: Virtual Private Server
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1587: Develop Capabilities	T1587.001: Malware
		T1587.004: Exploits

Tactic	Technique	Sub-technique
TA0042: Resource Development	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.005: Exploits
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.004: Drive-by Target
TA0043: Reconnaissance	T1590: Gather Victim Network Information	
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
	T1596: Search Open Technical Databases	T1596.002: WHOIS
	T1598: Phishing for Information	T1598.002: Spearphishing Attachment
		T1598.003: Spearphishing Link

Top 5 Takeaways

#1 In **April**, there were nine zero-day vulnerabilities with 'Two Celebrity Vulnerabilities' taking center stage. These featured flaws such as **IngressNightmare, BlueKeep**. Meanwhile, a critical flaw, CVE-2025-30406, in CentreStack has been exploited since March, allowing remote code execution via a hard-coded key.

#2 Ransomware is on the rise, with relentless variants like **Hellcat, PlayBoy Locker, DOGE BIG BALLS, Interlock, CrazyHunter, and Cactus** claiming new victims. As attacks grow more sophisticated, organizations must act fast strengthening defenses, securing backups, and refining disaster recovery plans to stay ahead of the threat.

#3 Cyberattacks hit **164** countries in April, with **Poland, Russia, Turkey, South Korea, and Netherlands,** 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, Healthcare, Telecommunications and Financial** 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 A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These include the **GolangGhost, PipeMagic, WINELOADER, LummaStealer, MySpy, and DslogdRAT.**

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **25 significant vulnerabilities** and block the indicators related to the **11 active threat actors, 41 active malware,** and **219 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 **25 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
GODZILLA	SHA256	245fdb5e35b6f51b26d4cf3999a40dde13987240f9bf565fe03a1f6adb9da9b2
VARGEIT	SHA256	28517bff286ade02b81da52f9fcddcb9764023ae7035bc593d081fdd2a8c85d9, 43e5c3d6182ab6d9d71b5892c5087b4ef4b3093126bcdf4ebcef0b15e04e0c03, 4be6f5e76ea02ae348b26fc32a0dabe009d05b701e53270cf40ca50fa76197b0, a14e226a50c12e637e8b280ad688e5637db752c72d0f8b2bac5f2d3d487e1c21, a9804fa05845707f094fe91668a5c3792f2441d371816b46fbe636953fc5787d, b8e1a46146c09ef54b802a6989b485ef5982a86228a24ec0839ec5af7b42e648, b9fefe3946d0c9e000262a10b184090da45925f24b7dfc9d25abe63bc55ca7ed, d692c85da91bb5e5724f520ca392b68eee144a3719a7441c779c8ce73d3b25dc
RAILLOAD	SHA256	00a41c8272d405ba85ae9d0e435e3030033e8a032f3d762367d0a57d41524f3a, 0d3ec88b0bfa5530e45dec75dfbea7ae683bdea91105b5f90a787beaabd1ef27, 0f6fe5d0ee754d581d4a8d989e83272b121d0125bd3c77e57a6b14db23f425ab, 13e0aef0ab6d218e68c5c5b6008872eb73104f161c902511aec3df5bce89136e, 16509adf92b1ac3097452affd8dda640936c8a40272592b978db3698487df5fa, 19bcca292814942f2fe8d142a679cc6a97fa6cbf77a0c98873146e918013bb5c, 1c8c14251710fbdef994d9ccf1d3507cf0ef5cd6c7d3495af2adfe7f97cc0dc2, 1c93ba375016bcb41b915b78eb4ab023ecf456e240823a1d6d2b5297b3523956, 281fc3aff361f202a41f4aff84a5f61e5728fd8ea0c1219a8bca540a959a4ee2, 2971a53769745c107a89eeb5f48e3b3e9680d371bf06b028c7769c961e6f9e55, 3129bfad321be526f231c64aac10d7d8f416dc14cab11c1bbc57252c75823959,

Attack Name	TYPE	VALUE
RAILLOAD	SHA256	3b7c29489c1feaafc587eac0ffcca79964259c9687d86a5cce5ea70261f7439b, 3f0157cfb493df1cd051cc87364c7bdbe3719927335b76b7c567b369ab47b3be, 41410a8aa4a4fcd811ef67ba023e263f4cd6667039b01547d23a3eb758d97b96, 442446fbc012847a12448398b619837614498bb611968e64166f0e9040c311db, 455510fe663775e09a2d0bbfdc4c8ec2e26665e10f9599b05dc59ea460f06ac8, 47ea0392ec123e3949b9ae2638b9078cd5efd4da942e38f149ccfb74d8e70123, 529e691a9d60b8ae0c64de82402e76c112df3bc27be5f2e94ee58252a67804a1, 52c8eacbcc8906036894a3a11cb4181d454c3a4f685500a799263cdcf6c6d88e, 5502735d81accb96c58300d1e21765b8b53a4749aad68e513b2558ed79f83cc4, 5518b542afd9d456ee8dea4dec3e0e8a98a42982b33f8f629d3d8edeca0dbf4d, 55b4e3814a349c9de4c99237f62d42787a6fef64b809db9cf52cfe0602cac01e, 5872da9dfd5ed3c0b9e0a05466a56c6ac6966012b5b3e14ac43a1225ba5e6bb2, 5aaca0994795ba7da0f10cd393ac32cc1e78c9afd4e9d09bbbe430f168c0eebe, 5d358bcd0acb999fdec332f0a2d1fe51952542f0836b9618ab18f253597d244c, 5dcd5cb720a40692b7e49540a42f1d12e831aaab369d9fe31a66b0433b825264, 62d71b61af750ad3b763d98504a174a1949a359a4cb4f6ce2795b7b3240919eb, 67dddc4ce777df1baa19acb1c3535eb01a54f24516a85312bafe4cba11d74483, 681e9aab60b1c64dacbc7c8574d294333b9cd4494ec683b0c780866c3e1e7d40, 762525805afe6a0891275ebc2ae1f067e9aad8f310afc0b1ad800cc980ed8b55, 7654e7f7076f07e76ae478c1df65f1711918ad4f36c45f520cc46cdcb1128cc2, 7ad44f7e1f78ee83f20da498584ec7138c2514580ddfe62698be7587ae2678e1, 83968575244ab2e44a5b94423bb1cacd10bb293ddcbbddbc2fc117f9335b6e78,

Attack Name	TYPE	VALUE
RAILLOAD	SHA256	846be29c140850fd9524339acd67eac4b84bc59ed056544356d199226452ea88, 85f9bac9eefb5fbc1e51508ce12cda10a69d8bde82952891081b19d6833297ab, 86e2d56761fb4dc16c7b0cd8da241c9899af851f5df751ffc67a2d68062e71f4, 86f5f088cf997766e52860b57506ba0923454a63bee39e4e3de2fb98c4fee240, 8c89362d4bed8bd2f0fbffc450bca4e7666fc7a3e88ec56a5dd149593fd697ec, 91034c01e800b116095eecdb073a5262852fc2c788f9fcd09259d6c09ce88ac6, 9366ece5ff9082145184adb2e91053d5e0d68d4d9f9a9f054aad68b8e7368443, 9b5e6c2f287ea7931bb27f63111ef0035265bc27751f01bd6c7f3dd3395bbaf5, 9d9f40c6c2dc14118452f7f1b56346e60a8681fb83300e4292576e635b37f9c8, 9f94bb59bfc32958a15cd8e225f270802bd9e14929e5d0f4f488842710a361ea, a042157e7460f6c28c984a1c1f3803521a556c67e26411854e497685ef436325, a79679d8f9551810504ff316465fb289d1ac64dc52bcaabd70267217d33d603c, a845cb84ea11f0fa7a982407705e892f58d7cb407eadc5329416464cccdd6a23, ab6145f1ea6c8a682bea289cef06c0f27fa076b8f88a89a2631167541fc835e9, ac70d98af57d9e3da9ee485a4ab1badbb28e89d15c4ef2df521423881a147e43, afd83d598843f93f7cad02bbe8467da2f257b5344600090034bb795844f05bdc, b0a42d1c5a07bbe317a034e204c0eb64ae5d99e3dfbfbd9b3b098caea4b19f96, b32dd5d549bcf4b674b4e7cf5481064b38ea614c666b158afedc7084b715c1fa, b92452a6c2cd13193a6df88278c31c85008acf448655c18389c84b353026d15e, ba0105c8fa99b8f3a82c32d20e94031f22e277286b738db529e763955df248dc, bd0dbf799e98137238ae38f134c7af82d7ff673c0a418044add022021d98a27, be01089ad2c2e7af32677ec0a7a9a541dee1cb149639d60fb7b7e9b641d2ccdb,

Attack Name	TYPE	VALUE
RAILLOAD	SHA256	c0d1deb30fd3507455dae99aabf1cc23638b2bcf1908099e08081ee2691a24b0, c56c88ce8e45a9caa043f1f4831442f09bae6f1a083910f772afc1e27be3b606, c6a28c9cac9c4b5ef57998bdc7a7f430fff7c9ac819fef278f8350751b6edaab, cd385806117ebe1504af4669671b4c0a252faec873e1402aaebeb413fdd58556, d31eb16688d1b36652e87d43ad5755d139eedd74b500ddcee97a5545d8d1fe7b, d34947e11879598b85d9baa703cb96a83d7c3ccb53868ab86ff9a2f37dc91459, d83a837910305567acfd49d2d416fc4b113f080e31730c9b0abefa4b01192a40, ded42e37f05950374496824ce3f4d540a45e97be35ed6d7ddcfcf12a7b2cd46f, dfbb857e6383789545c719c99d878a678a0aeae2a6a1c8f44e87b7aa478fc354, e03062caa13400df3d60efb1aa2b0f19dcf65fefc38d4bc9931c0918b5dc4865, e299b865cdb0fdd9605e3c5e9d00fb473c77af4ed213775d594cc0fe91b8dd3a, e3465c996e149b218d95a4b109e6e3ff268e8d63aafa73d4855750b33c66a33c, e6141757775ce9747b12f21cc7f8411e5ab4916649f38738f4e93b2ca7cc274a, ee8385313e03890c6862f70c94f2c5a3e9cd09764fcac4488fabc5ce9613228a, f0cd90b42969706d1a78e75608aded6d5ac8610f36cab8f8be7160c5cbf485a5, f92493bf2b46873feee38ea2dac69ff830637983d569b64ee87e75f7fe08de88, fd1720b11ddd7ae226889deca9a6532df676a4991f0209c0a3d6d7be52276dcf, Fd3637392404c3ed169a4999f6a05274715109f9fa028be9ad9ce7853d983d54
MASQLOADER	SHA256	8b0023248bc037631b26694f34d7bc8163e2d5f5919fe61f3dbc1354f87d6792
GolangGhost	SHA256	0cbbf7b2b15b561d47e927c37f6e9339fe418badf49fa5f6fc5c49f0dc981100, ef9f49f14149bed09ca9f590d33e07f3a749e1971a31cb19a035da8d84f97aa0, 6e186ada6371f5b970b25c78f38511af8d10faaeaed61042271892a327099925, ba81429101a558418c80857781099e299c351b09c8c8ad47df2494634a5332dc, bfac94bfb53b4c0ac346706b06296353462a26fa3bb09fbfc99e3ca090ec127e
FrostyFerret	SHA256	b7b9e7637a42b5db746f1876a2ecb19330403ecb4ec6f5575db4d94df8ec79e8

Attack Name	TYPE	VALUE
TRAILBLAZE	MD5	4628a501088c31f53b5c9ddf6788e835
	File Path	/tmp/.i
BRUSHFIRE	File Path	/tmp/.r
	MD5	e5192258c27e712c7acf80303e68980b
SPAWNSNARE	MD5	6e01ef1367ea81994578526b3bd331d6
	File Path	/bin/dsmain
SPAWNWAVE	MD5	ce2b6a554ae46b5eb7d79ca5e7f440da
	File Path	/lib/libdsupgrade.so
SPAWNSLOTH	File Path	/tmp/.liblogblock.so
	MD5	10659b392e7f5b30b375b94cae4fdca0
PipeMagic	SHA256	2712b5f08fff88a78045cf98e6894b521f4b7af3f74aa385584f1f01aa5b6ebe
GIFTEDCROOK	SHA256	8427dc6e7da4c163d20c7f188232cf3f83c78ddb6fcad04cec84b33e0f9bdfc0, 7ca3f2505e1778e6de3927571ba49d27b36447e6c28a60161d55fd2254966bce, 2930ad9be3fec3ede8f49cecd33505132200d9c0ce67221d0b786739f42db18a, 530185fac69e756fb62f23e21e7c0b0828a964b91bbf40f1d04fc2136c1b6dd1, ff1be55fb5bb3b37d2e54adfbe7f4fbba4caa049fad665c8619cf0666090748a, d7a66fd37e282d4722d53d31f7ba8ecdabc2e5f6910ba15290393d9a2f371997
Hellcat	SHA256	4b2edadc8f90e9fcc976f02a9eda1640cd92c07718c0271842fbd4ca7e2906e2, 53c09e57cea028c0439477cd90bcf8f981067a120a2fb7b86d0f13017727a93a, 5b492a70c2bbded7286528316d402c89ae5514162d2988b17d6434ead5c8c274, 6924479c42b3732e0d57b34714b7210e14655ee1ca570ae4aab1d90c3f6c6428, 93aa8b0f950a7ea7f0cee2ba106efaacf673bb2b504ca0b9e87f9ea41acfb599, b8e71845cc8ccd668a3436d1952a6c57649974bb8399e599dc33afc4c0843be7, dcd7995038ad4839e88e5bb3bf654b4f7c2ad09780a39c9d47596ce717fd4ac2
	MD5	931396d6332709956237cf76ee246b01
	SHA1	b834d9dbe2aed69e0b1545890f0be6f89b2a53c7
	Tor Address	hellcakbszllztlyqbjzwcbdhfrodx55wq77kmftp4bhnhsnn5r3odad[.]onion

Attack Name	TYPE	VALUE
Neptune	SHA256	8df1065d03a97cc214e2d78cf9264a73e00012b972f4b35a85c090855d71c3a5, e8c8f74ae15e7d809d9013bdfa2a10dd54e00d4ea5ff4ed6cd4a163b80d2d318, add3e9a1c6654d1ec9b7fd0ffea6bdcd0eb7b3e4afa70c6776835cc238e8f179, 9a35113e1d9412701d85b5af01b4ad2b1e584c6e0963e439053808b29b4da90a, 684d2d50dd42e7ba4e9bd595e9b6f77eb850185556c71db4eda6f78478a5e6fb, 9ca70da0ea94b3bea68c9a3259ec60192c5be1ae7630a08924053168bbf41335, 1bbd4262c8821a0290fe40a8e374c6e5fa2084331670ede42e995d3d5902efcd, 20c31ac326b5c6076f9b1497f98b14a0acd36ff562dfa2076589a47a41d0e078, 6d02eb3349046034cf05e25e28ef173c01d9e0ea1f4d96530defe9e2a3d5e8a0, cd2b320433843d4d694ae8185c7ef07a90d7dce6d05a38ac4481ad2eab9bcfe5, 630b1879c2e09b2f49dd703a951fb3786ede36b79c5f00b813e6cb99462bf07c
PlayBoy Locker	SHA256	3030a048f05146b85c458bcabe97968e5efdd81b224b96c30c83b74365839e7b, a9e1bd8f9cbeeec64da558027f380195f7ed572f03830a890dd0494e64d98556, a9e1bd8f9cbeeec64da558027f380195f7ed572f03830a890dd0494e64d98556
	File Name	INSTRUCTIONS.txt
	TOR Address	vlofmq2u3f5amxmnblvxaghy73aedwta74fyceywr6eeguw3cn6h6uad[.]onion
ResolverRAT	SHA256	80625a787c04188be1992cfa457b11a166e19ff27e5ab499b58e8a7b7d44f2b9
DOGE BIG BALLS	SHA256	3d2cbef9be0c48c61a18f0e1dc78501ddabfd7a7663b21c4fcc9c39d48708e91, f08b5316f6bc009d0cb41d4ce0086e615bf130b667cb2cdceecad07fda24fc49, 8e209e4f7f10ca6def27eabf31ecc0dbb809643feaecb8e52c2f194daa0511aa,

Attack Name	TYPE	VALUE
DOGE BIG BALLS	SHA256	805b2f5cab2a4ba6088e6b6f91d6f1f0671c61092b571358969d69ff8c184c30, 30a6688899c22a3ce4c1b977fae762e3f7342d776e1aa2c90835e785d42f60c1,ecfed78315f942fe0e6762acd73ef7f30c34620615ef5e71f899e1d069dabd9e, 2c38a56beec1f7c8b919a1a2d9f9497358e763a1c8d9d71aa8a0e4ef062d3ec2, 4ad9216a0a6ac84a7b0b5593b0fc97e27de9cdfeb84ab7e5339ae5a4102100c0, 8d843c757aea85087a95794f93071bfacb7c4db06f33520308f39b97cf88cabb
MySpy	SHA256	16bb4855a7412ce2bd63b2bcc0de3add1e7ca8c0f22acf8172e760931ef3e7da
KimaLogger	SHA256	68c648a75976911609713dfa33957bf4399cc074b986ec88c85d0ec15e75d640
	MD5	184a4f3f00ca40d10790270a20019bb4
Sagerunex	SHA256	4b430e9e43611aa67263f03fd42207c8ad06267d9b971db876b6e62c19a0805e, 3fb81913c2daf36530c9ae011feebeb5bc61432969598e2dfaa52fc2ce839f20
ChromeKatz	SHA256	2e1c25bf7e2ce2d554fca51291eaeb90c1b7c374410e7656a48af1c0afa34db4, 6efb16aa4fd785f80914e110a4e78d3d430b18cbdd6ebd5e81f904dd58baae61, ea87d504aff24f7daf026008fa1043cb38077eccec9c15bbe24919fc413ec7c7
CredentialKatz	SHA256	e3869a6b82e4cf54cc25c46f2324c4bd2411222fd19054d114e7ebd32ca32cd1, 29d31cfc4746493730cda891cf88c84f4d2e5c630f61b861acc31f4904c5b16d
ThreatNeedle	SHA256	94868d8db5a22df0b841d282d5d408d00179224ec7031386fbd80f0473f486b3
	MD5	f1bcb4c5aa35220757d09fc5feea193b
wAgent	SHA256	922a2ffdbfbbc3998ff38111d20c6ed88bba0e09de7f0f66a28b06c0ee51f69c
	MD5	dc0e17879d66ea9409cdf679bfea388c

Attack Name	TYPE	VALUE
SIGNBT	SHA256	507929bd787b09db862543f203e6f9faa23409af534891bbbf145296c1697eed, 4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74, 507066f487ea037bde2e91158a63113585776fe0c13cfa7fe6252ae58e89a59a, 04bc903a0f44c31e976a2a090d8b846d68c3d87122293f8ce0c2d20a1978e37e
COPPERHEDGE	SHA256	23ac99fb8de813172bb641baefff59fd8b84f1b39b362d7fd11736b5667bee56
	MD5	2d47ef0089010d9b699cd1bbbc66f10a
Agamemnon	SHA256	1174fd03271f80f5e2a6435c72bdd0272a6e3a37049f6190abf125b216a83471, 9c906c2f3bfb24883a8784a92515e6337e1767314816d5d9738f9ec182beaf44, e13888eed2466efaae729f16fc8e348fbabea8d7acd6db4e062f6c0930128f8f, c92c158d7c37fea795114fa6491fe5f145ad2f8c08776b18ae79db811e8e36a3, 17f1c3dc3ad9e0e87e6a131bd93d12c074b443f365eea2e720b9d9939f9ce22e, 75bf8feeac2b5b1690feab45155a6b97419d6d1b0d36083daccb061dc5dbdea8
CrazyHunter	Email	payment[.]attack-tw1337[@]proton[.]me
	TOR Address	7i6sfmfvmqfaabjksckwrttu3nsbopl3xev2vbxbkghsivs5lqp4yeqd[.]onion
	SHA1	318a601a5d758dd870c38b8c4792a2c3405e6c28, 0937377d1ef1d47a04f1e55d929fe79c313d7640, 79c3fd97d33e114f8681c565f983cd8b8f9d8d93, b6737248f7baed88177658598002df5433155450, bed4229e774f136e1898fad9d37bd96e9156369e
	SHA256	f72c03d37db77e8c6959b293ce81d009bf1c85f7d3bdaa4f873d3241833c146b
LAGTOY	SHA256	fdf977f0c20e7f42dd620db42d20c561208f85684d3c9efd12499a3549be3826
Cactus	IPv4	206[.]188[.]196[.]20, 51[.]81[.]42[.]234, 178[.]175[.]134[.]52, 162[.]33[.]177[.]56, 64[.]52[.]80[.]252,

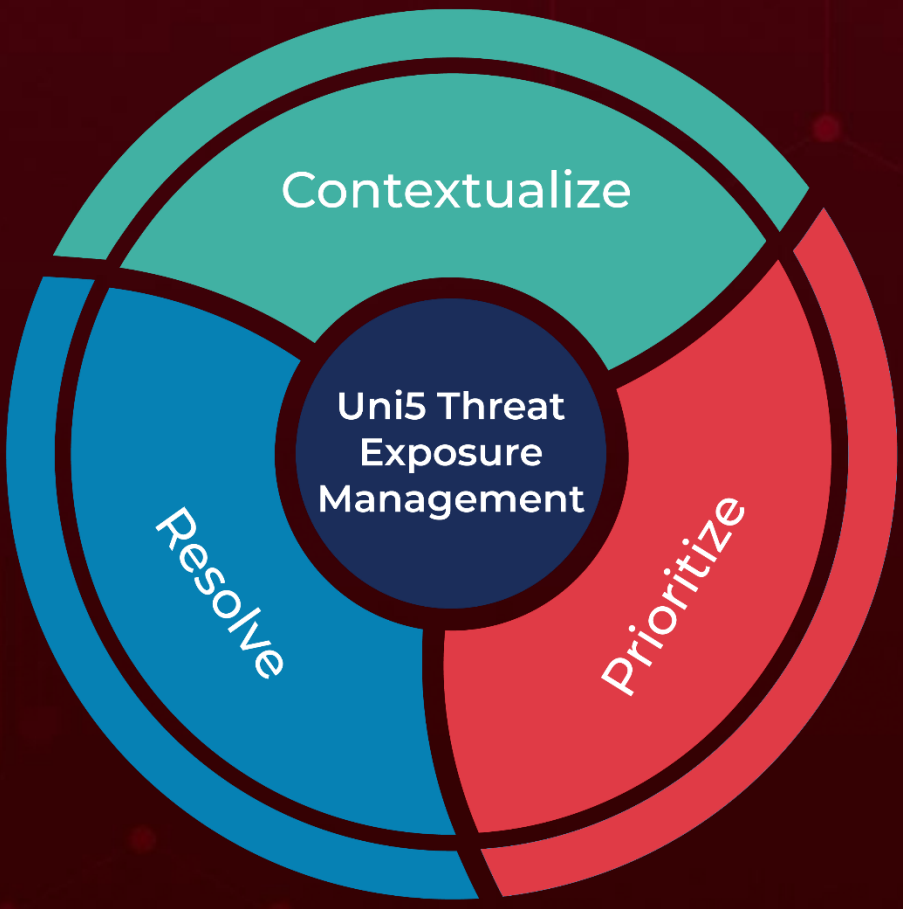
Attack Name	TYPE	VALUE
Cactus	IPv4	162[.]33[.]178[.]196, 103[.]199[.]16[.]92
	SHA256	670586ea97fcd63f4375a976cc5ddaede00f2e4e5651ede2fa8b61b929563d31, d3d0bd2f72d0e23650ef47ff3c5297c1a201270a71fee78e8badfa816d455e13, 55a4e88be5f80260e3366b6adc1c2d1c6b0673105b509371ff7f3525d2f1c3ec, 696b05ad1f8b81195b58414e04d3793919900807d1f06d22cd8384abc69e8fd8, 3334a247c7b28dcb284d823f8d150240916de03b8f84a70435d0d9433bd55263, b9ca2460ecb3e3fed011b1b7f119b58c755c78af752f6acc0a7173ea6caa20e1, 46ff4366713bfcad09086dfd6f309897f1f4b7df854335651b4734d15f324e2e, d94efdfa16d6de2aee2384e62a29ce559bcbf37910ef7aa524a35df12e248c24, 2b89a710d29598c840696c34d9443d825265e8a03fa55610ff253b450969fb88, 5b7d784ca76f53acc95b418d04b9f3f608b5bc6e6d1c51a4f8725c9d9186e24e, 77bbd39c8a1b9093c9ad8e5d94265e5d95f8ca275d4eea2218d560cba6dfd838, 1000cd4b74290bcecbe1be07146dad30a46f264bfeb0b8ceb00c83a6ff1e70d9, 871b245bd87dbb3ed064e9e42522dcb7dee8d80b9463f8ee4bcf9da184dd5e87, e330ec98280560fc0b434e408e2075bb84c3106e5a9fe4aed121d048ca96fa8a, 8f50df60a73e4f849d71d3a93d1f0cbbdb16e1165dbae0ce61b27d4de85092fa, de9f7cdb07454c8b2b7598895f8f25151e59ae8d5c18db463e2ce1e8accc79bc, 58ea56177cf0e8a863d6e9f11570a3e61239e21e1d0b5667537b7223d4131c42, d7da599c59de7fa5a42044665f8e6eeef7b313a2733886a24a8732e8689f4df4, 3373cac62071e1ea2f2e50d349258cfefe4aca5a8fa8f3644fd1c1bec36fa47b, 378bec795d652d3941510969c1db6a42fab4d493704fbd52121a48d2ba459d0d, 0aa62974c2fb1acd200a78adf85f7bc5444869f6b3a40f619e17991e6a5fd460, 0f99e9767ac4b8950c2e6be2e33b5fe06fb400c65cb9af9d9e2b334d4dd73e33, a82c5abfc976b78a19020e690992a803fae267080d1e3fb30dff552a0ddf73b1, 7adee0f8f400d72b70d34b9bd90b3559c71d7f0f5b2695b5ed70e733e76d9e46,

Attack Name	TYPE	VALUE
GRAPELOADER	SHA256	d931078b63d94726d4be5dc1a00324275b53b935b77d3eed1712461f0c180164, 24c079b24851a5cc8f61565176bbf1157b9d5559c642e31139ab8d76bbb320f8
WINELOADER	SHA256	adfe0ef4ef181c4b19437100153e9fe7aed119f5049e5489a3669275746 0b9f8
Interlock	SHA256	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f, 4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9, 33dc991e61ba714812aa536821b073e4274951a1e4a9bc68f71a802d034f4fb9, b85586f95412bc69f3dceb0539f27c79c74e318b249554f0eace45f3f073c039, a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642, 0fff8fb05cee8dc4a4f7a8f23fa2d67571f360a3025b6d515f9ef37dfdb4e2ea, e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1, f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e
BerserkStealer	SHA256	eb1cdf3118271d754cf0a1777652f83c3d11dc1f9a2b51e81e37602c43b47692, a5623b6a6f289bb328e4007385bdb1659407a9e825990a0faaef3625a2e782cf
LummaStealer	SHA256	4672fe8b37b71be834825a2477d956e0f76f7d2016c194f1538139d21703fd6e
DslogdRAT	SHA256	1dd64c00f061425d484dd67b359ad99df533aa430632c55fa7e7617b55dab6a8
Hannibal Stealer	SHA256	f69330c83662ef3dd691f730cc05d9c4439666ef363531417901a86e7c4d31c8

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

May 2, 2025 . 10:00 AM

More at www.hivepro.com