Date of Publication
February 4, 2025

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

January 2025

Table Of Contents

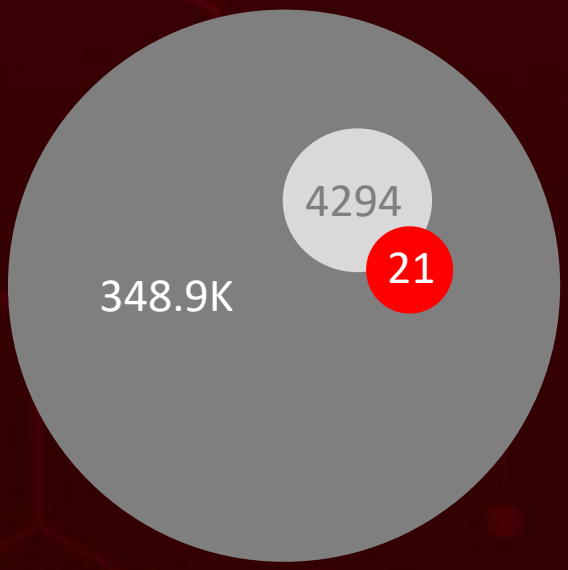
Summary

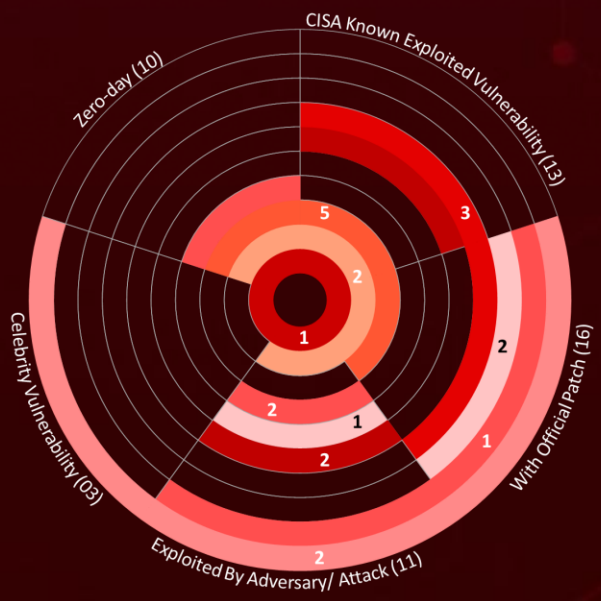
In **January**, the cybersecurity arena drew significant attention due to the active exploitation of **ten zero-day** vulnerabilities. Among them, **CVE-2025-0282** in multiple Ivanti products was exploited by **UNC5337 and CL-UNK-0979** to execute arbitrary code remotely without requiring authentication, with active exploitation detected since December 2024. Fortinet also fixed the critical zero-day flaw **CVE-2024-55591** in FortiOS and FortiProxy, which has been actively exploited by threat actors to compromise Fortinet firewalls and breach enterprise networks.

During this period, ransomware attacks surged, with variants such as **HexaLocker**, **FunkSec**, **and Daixin Team** 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.

FunkSec emerged in late 2024 as a fast-moving ransomware group, blending cybercrime with hacktivism. Using AI-driven tools, they have targeted dozens of victims, demanded low ransoms, and evolved rapidly. Their origins remain unclear, but they are a rising force in AI-powered cyber threats.

Concurrently, **seven** threat actors have engaged in various campaigns. The Russian threat actor **Star Blizzard** has launched a new spear-phishing campaign, using WhatsApp group invitations as lures to compromise accounts, marking a shift in their tactics. At the same time, the **Paper Werewolf** cyberespionage group, active since 2022, has been targeting Russian organizations with phishing emails embedded with malicious macros to deploy **PowerRAT** for unauthorized access and data exfiltration. As the cybersecurity landscape evolves, organizations must remain vigilant and proactively address emerging threats.





Total Vulnerabilities Published

Vulnerabilities Published in the Month

Exploited Vulnerabilities

Insights

In January 2025, a geopolitical cybersecurity landscape unfolds, revealing **Germany, Russia, United States,** and **Egypt** as the top-targeted countries.

Highlighted in **January 2025** is a cyber battleground encompassing the **Government, Technology, Media,** and **Energy** sectors, designating them as the top industries.

Paper Werewolf's Destructive Cyberattacks Shake **Russian Organizations.**

Gayfemboy botnet, a sophisticated Mirai variant, targets a 0-day vulnerability in Four-Faith industrial routers, boasting 15,000+ active nodes and launching DDoS attacks peaking at 100GB traffic.

CVE-2025-0282

Ivanti Zero-day Flaw exploited by threat actors to deploy malwares like DRYHOOK, PHASEJAM and SPAWN ecosystem.

Critical Mitel MiCollab

Flaws enabling authentication bypass and unauthorized file access. These vulnerabilities can be chained for advanced attacks, risking system compromise.

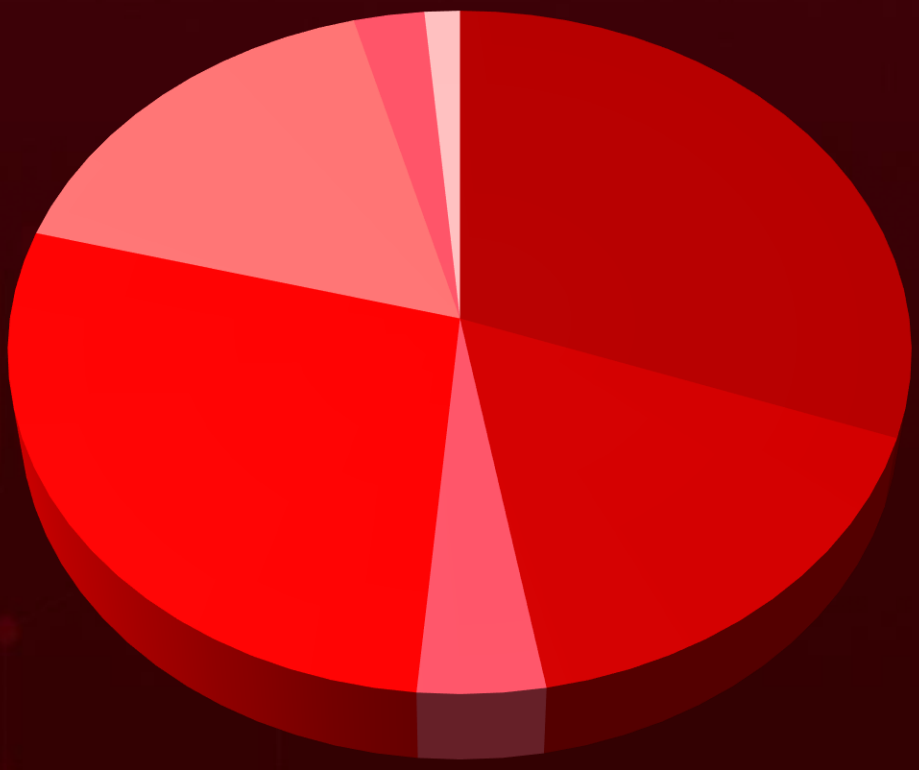
SonicWall fixed the critical **CVE-2025-23006** flaw in its SMA 1000 Series, allowing remote attackers to execute arbitrary commands.

Aquabotv3 new Mirai variant making waves with DDoS-as-a-service, exploiting vulnerabilities in Mitel SIP phones.

Silent Lynx APT targeted Kyrgyzstan's National Bank and Ministry of Finance with phishing campaigns, using malicious payloads and Telegram bots for espionage.

CVE-2024-55591, a **zero-day** vulnerability in FortiOS and FortiProxy, is being exploited by attackers to bypass authentication and escalate privilege.

Threat Landscape



- Malware Attacks
- Injection Attacks
- Denial-of-Service Attacks
- Social Engineering
- Eavesdropping Attacks
- Password Attacks
- Supply Chain Attacks

Celebrity Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-49112	LDAPBleed	Windows: 10 - 11 24H2 Windows Server: 2008 – 2025	-
	ZERO-DAY		
	✕	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Unknown Infostealer malware
Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	✕		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-49113	LDAPNightmare	Windows: 10 - 11 24H2 Windows Server: 2008 – 2025	-
	ZERO-DAY		
	✕	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Unknown Infostealer malware
Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability	✕		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1498: Network Denial of Service	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49113

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*	EAGERBEE backdoor
Microsoft Exchange Server Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application; T1078: Valid Accounts	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855

Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-49112	LDAPBleed	Microsoft Windows	✗	✗	✓
CVE-2024-49113	LDAPNightmare	Microsoft Windows	✗	✗	✓
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	✓	✓	✓
CVE-2024-41713	Mitel MiCollab Path Traversal Vulnerability	MiCollab Version	✗	✓	✓
CVE-2024-55550	Mitel MiCollab Path Traversal Vulnerability	MiCollab Version	✗	✓	✓
CVE-2024-35286	Mitel MiCollab SQL Injection Vulnerability	MiCollab Version	✗	✗	✓
CVE-2024-12856	Four-Faith OS Command Injection Vulnerability	Four-Faith F3x24 and F3x36	✓	✗	✗
CVE-2025-0282	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	✓	✓
CVE-2025-0283	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✗	✗	✓
CVE-2024-43405	ProjectDiscovery Nuclei Remote Code Execution Vulnerability	ProjectDiscovery Nuclei	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2024-55591	Fortinet FortiOS Authorization Bypass Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2025-21333	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability	Windows Hyper-V	✓	✓	✓
CVE-2025-21334	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability	Windows Hyper-V	✓	✓	✓
CVE-2025-21335	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability	Windows Hyper-V	✓	✓	✓
CVE-2025-23006	SonicWall SMA1000 Pre-Authentication Deserialization of Untrusted Data Vulnerability	SonicWall SMA1000	✓	✓	✓
CVE-2025-24085	Apple Multiple Products Use After Free Vulnerability	Apple Multiple Products	✓	✓	✓
CVE-2024-40891	Zyxel CPE Telnet Command Injection Vulnerability	Zyxel CPE Telnet	✓	✗	✗
CVE-2024-41710	Mitel SIP Phones Command Injection Vulnerability	Mitel SIP Phones	✗	✗	✓
CVE-2018-10562	Dasan GPON Routers Command Injection Vulnerability	Dasan GPON home routers	✗	✓	✓
CVE-2018-10561	Dasan GPON Routers Authentication Bypass Vulnerability	Dasan GPON home routers	✗	✓	✓
CVE-2023-26801	lb-link bl-lte300_firmware Command Injection Vulnerability	lb-link bl-lte300_firmware	✗	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Quasar	RAT	-	Windows	-	Masqueraded as Malicious npm package
NonEuclid	RAT	-	-	-	-
PowerRAT	RAT	-	Windows	-	Phishing emails
PowerTaskel	Hack Tool	-	Windows	-	Phishing emails
QwakMyAgent	Hack Tool	-	Windows	-	Phishing emails
EAGERBEE	Backdoor	CVE-2021-26855	Microsoft Exchange Server	✓	Exploiting Vulnerabilities
Gayfemboy	Botnet	CVE-2024-12856	Four-Faith F3x24 and F3x36	✓	Exploiting Vulnerabilities
DRYHOOK	Stealer	CVE-2025-0282 CVE-2025-0283	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting Vulnerabilities
PHASEJAM	Dropper	CVE-2025-0282 CVE-2025-0283	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting Vulnerabilities
SPAWNANT	Dropper	CVE-2025-0282 CVE-2025-0283	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting Vulnerabilities
SPAWNMOLE	Web Shell	CVE-2025-0282 CVE-2025-0283	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting Vulnerabilities
SPAWNSNAIL	Backdoor	CVE-2025-0282 CVE-2025-0283	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting Vulnerabilities
SPAWNSLOTH	Dropper	CVE-2025-0282 CVE-2025-0283	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	✓	Exploiting Vulnerabilities

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Sliver	Framework	-	Windows	-	Spear-phishing
HexaLocker	Ransomware	-	-	-	-
Skuld	Stealer	-	-	-	-
Resocks	Toolkit	-	Windows	-	Spear-phishing
SlowStepper	Backdoor	-	-	-	Trojanized VPN installers
Lumma	Stealer	-	-	-	using fake CAPTCHAs
TorNet	Backdoor	-	-	-	PureCrypter drops the TorNet backdoor
PureCrypter	Loader	-	-	-	Social Engineering
Mirai	Botnet	CVE-2024-40891	Zyxel CPE series devices	No	Exploiting Vulnerabilities
FunkSec	Ransomware	-	-	-	-
Aquabotv3	Botnet	CVE-2024-41710 CVE-2018-17532 CVE-2023-26801 CVE-2022-31137 CVE-2018-10562 CVE-2018-10561	Mitel SIP Phones, Teltonika RUT9XX, lb-link bl-lte300_firmware Roxy Wi, Dasan GPON home routers	✓	Exploiting Vulnerabilities
Daixin Team	Ransomware	-	-	-	Exploit VPN vulnerabilities, Phishing, and weak authentication

Adversaries Summary

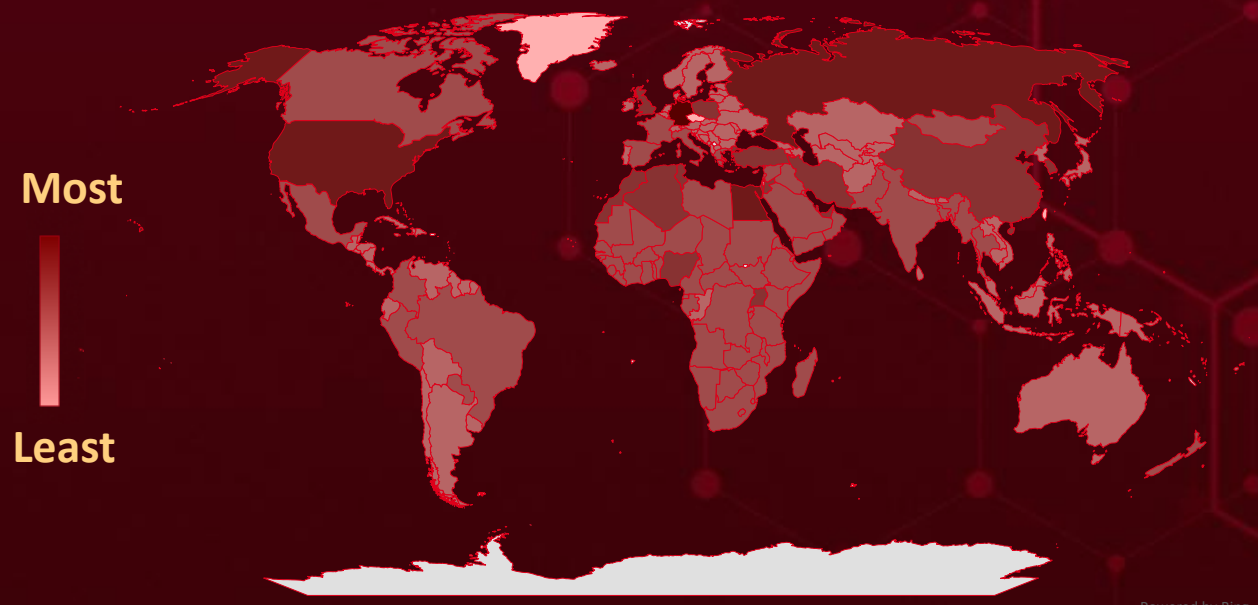
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
Paper Werewolf	Espionage and Destruction	-	-	PowerRAT, PowerTaskel and QwakMyAgent	Windows
UNC5337	Espionage	China	CVE-2025-0282, CVE-2025-0283	DRYHOOK, PHASEJAM, SPAWNANT, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
Star Blizzard	Information theft and espionage	Russia	-	-	-
Silent Lynx APT	Information theft and espionage	Iran	-	Resocks Toolkit	Windows
STAC5143	Information theft and espionage	Iran	-	Unknown Ransomware	Windows
STAC5777	Information theft and espionage	-	-	Unknown Ransomware	Windows
PlushDaemon	Information theft and espionage	China	-	SlowStepper Backdoor	-

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
Mitel Powering connections	Unified Communications	MiCollab Version 9.8 SP1 FP2 (9.8.1.201) and earlier
	Endpoint Device	Mitel SIP Phones
Four-Faith	Operating system	Four-Faith F3x24 and F3x36
Microsoft	Mail server	Microsoft Exchange Server
	Server OS	Windows Server: 2008 – 2025
	Operating system	Windows: 10 - 11 24H2
ProjectDiscovery	Vulnerability Scanner	Nuclei prior to version 3.3.2
ivanti	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

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
SONICWALL	Secure Remote Access (SRA) Appliance	SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) Version 12.4.3-02804 and earlier
FORTINET	Operating System	FortiOS Versions 7.0.0 through 7.0.16,
	Web Proxy	FortiProxy Versions 7.2.0 through 7.2.12, FortiProxy Versions 7.0.0 through 7.0.19
	Operating System	Apple visionOS Version affected before 2.3, tvOS Version affected before 18.3, macOS Version affected before 15.3, watchOS Version affected before 11.3, iOS and iPadOS Version affected before 18.3
ZYXEL NETWORKS	Endpoint Device	Zyxel CPE Series
DASAN DNS Dasan Network Solutions	Router	Dasan GPON home routers
LB-LINK	Router	lb-link bl-lte300_firmware

Targeted Countries



Color	Countries	Color	Countries	Color	Countries	Color	Countries	Color	Countries
	Germany		Bangladesh		Seychelles		Sao Tome & Principe		Lesotho
	Russia		New Zealand		Botswana		Kuwait		Liberia
	United States		Cyprus		South Africa		Senegal		Libya
	Egypt		Singapore		Ghana		Cabo Verde		Rwanda
	Poland		Djibouti		Sudan		Sierra Leone		Gambia
	Morocco		Canada		Greece		Cameroon		Haiti
	China		DR Congo		Togo		Somalia		Uruguay
	South Korea		Pakistan		Guinea		Zimbabwe		Tajikistan
	Turkey		Benin		Mongolia		Colombia		Laos
	United Arab Emirates		Saudi Arabia		Guinea-Bissau		Madagascar		Samoa
	Algeria		Equatorial Guinea		Mozambique		Spain		Latvia
	Nigeria		South Sudan		India		Malawi		Sri Lanka
	Iran		Eritrea		Namibia		Syria		Czech Republic (Czechia)
	Qatar		Congo		Brazil		Mali		Bhutan
	Israel		Eswatini		Niger		Thailand		Denmark
	Tunisia		Myanmar		Iraq		Mauritania		Kyrgyzstan
	Jordan		Ethiopia		Oman		Comoros		Bosnia and Herzegovina
	Uganda		Central African Republic		Burkina Faso		Mauritius		Chile
	United Kingdom		France		Paraguay		Côte d'Ivoire		Afghanistan
	Tanzania		Peru		Italy		Mexico		Holy See
	Zambia		Gabon		Chad		Bahrain		Ireland
					Burundi		Yemen		Luxembourg
					Angola		Lebanon		
					Kenya				

Targeted Industries

Most

Government

Technology

Energy

Media

Healthcare

Manufacturing

Defence

Hospitality

Financial

Agriculture

Banking

Education

Business Services

Automotive

Embassies

Tele-communications

Transportation

Professional Services

Cryptocurrency

Aviation

Retail

NGOs

Least

TOP 25 MITRE ATT&CK TTPS

T1059
Command and Scripting Interpreter

T1588
Obtain Capabilities

T1190
Exploit Public-Facing Application

T1566
Phishing

T1068
Exploitation for Privilege Escalation

T1588.005
Exploits

T1204
User Execution

T1027
Obfuscated Files or Information

T1588.006
Vulnerabilities

T1041
Exfiltration Over C2 Channel

T1203
Exploitation for Client Execution

T1083
File and Directory Discovery

T1059.001
PowerShell

T1036
Masquerading

T1195
Supply Chain Compromise

T1574
Hijack Execution Flow

T1082
System Information Discovery

T1078
Valid Accounts

T1204.002
Malicious File

T1105
Ingress Tool Transfer

T1070
Indicator Removal

T1574.002
DLL Side-Loading

T1566.002
Spearphishing Link

T1071
Application Layer Protocol

T1057
Process Discovery

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Quasar	SHA256	9c3d53c7723bfdd037df85de4c26efcd5e6f4ad58cc24f7a38a774bf22de3876
	URL	hxxps[://]jujuju[.]lat/files/kk[.]cmd
	Domain	captchacdn[.]com[:]7000
	IPv4	154[.]216[.]17[.]47
PowerRAT	SHA256	13252199b18d5257a60f57de95d8c6be7d7973df7f957bca8c2f31e15fcc947b
	IPv4	94[.]103[.]85[.]47
	Domain	disk-yanbex[.]ru
EAGERBEE	MD5	9d93528e05762875cf2d160f15554f44, c651412abdc9cf3105dfbafe54766c44, 26d1adb6d0bcc65e758edaf71a8f665d
Gayfemboy	SHA1	3287158c35c93a23b79b1fbb7c0e886725df5faa, ba9224828252e0197ea5395dad9bb39072933910, fe72a403f2620161491760423d21e6a0176852c3
	SHA256	3ee4d3222dd1856ca58de9715342d5c83562578f869c3482b538ab2c8eb3c832, a0241e3e2a8fb48e2fa0a4ebb72054309f70c79de286b1d00f640347f81e69bd
HexaLocker	SHA256	0347aa0b42253ed46fdb4b95e7ffafa40ba5e249dfb5c8c09119f327a1b4795a, 28c1ec286b178fe06448b25790ae4a0f60ea1647a4bb53fb2ee7de506333b960, d0d8df16331b16f9437c0b488d5a89a4c2f09a84dec4da4bc13eab15aded2e05
Skuld	SHA256	8b347bb90c9135c185040ef5fdb87eb5cca821060f716755471a637c350988d8
	URL	hxxps[:]//hexalocker[.]xyz/SGDYSRE67T43TVD6E5RD[.]exe

Attack Name	TYPE	VALUE
Resocks Toolkit	SHA256	297d1afa309cdf0c84f04994ffd59ee1e1175377c1a0a561eb25869909812c9c
Lumma	MD5	82e5e8ec8e4e04f4d5808077f38752ba, 14d8486f3f63875ef93cfd240c5dc10b, 0ba2afe43cc4deed266354b1c2cfb5a7
	SHA256	b94ddefd39d32a753564e6871d11750fa56b993cad3ea40955139e584ad3bef8, 86d50a7fc8d245876b791efe85eb7f64cd48b9e9648b4bf8bee22dbae66fe3aa, 02a0bba5b3cc6a650d611c2f6d6a8ce6a696c230521f0de43824a19ced716acd
TorNet	SHA256	13ac538c8c6696a59f890677cf451db77b7c33539da1d380640ce549b2b70ca4, 53e7b3b72695a1eaea7146ec3cbd05d0ce2a1eba87f035ae07849feb4f59ec63
Mirai	SHA256	fa1b9e78b59cdb26d98da8b00fe701697a55ae9ea3bd11b00695cfbba2b67a7a, 7c41cb2df7b0c34985a18c20267c46b20ed365141fced770f7cdf0ed2214296d, 3c0c87bbc1a908ee2d698bf59722fc050b29aa5dcc9312a7c33c04910ad2f067
FunkSec	SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, 66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd, dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac, b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb, 5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd, e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22, 20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d, dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-41713	✗	MiCollab Version 9.8 SP1 FP2 (9.8.1.201) and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*:*:*	-
Mitel MiCollab Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1016: System Network Configuration Discovery	https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-55550	✗	MiCollab Version 9.8 SP1 FP2 (9.8.1.201) and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*:*:*	-
Mitel MiCollab Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1078: Valid Accounts	https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-35286	✗	MiCollab Version 9.8.0.33 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*:*:*	-
Mitel MiCollab SQL Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1016: System Network Configuration Discovery	https://www.mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin240014001-v10.pdf

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-12856	✗	Four-Faith F3x24 and F3x36	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:four-faith:f3x24:*:*:*:*:*:*:*:*	Gayfemboy Botnet
Four-Faith OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1499: Endpoint Denial of Service; T1078.001: Default Accounts	No patch

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-0282	✗	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	UNC5337
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*:*	DRYHOOK, PHASEJAM, SPAWNANT, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH
Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-121	T1059: Command and Scripting Interpreter; T1210: Exploitation of Remote Services	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-0283	✗	Ivanti Connect Secure: 22.7R2.4 and prior, 9.1R18.9 and prior Ivanti Policy Secure: 22.7R1.2 and prior Ivanti Neurons for ZTA gateways: 22.7R2.3 and prior	UNC5337
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*:*	DRYHOOK, PHASEJAM, SPAWNANT, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH
Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1068: Exploitation for Privilege Escalation; T1210: Exploitation of Remote Services	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43405	✗	Nuclei prior to version 3.3.2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:projectdiscovery:nuclei:*:*:*:*:*:go:*:*	-
ProjectDiscovery Nuclei Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://github.com/projectdiscovery/nuclei/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-55591	✗	FortiOS Versions 7.0.0 through 7.0.16, FortiProxy Versions 7.2.0 through 7.2.12, FortiProxy Versions 7.0.0 through 7.0.19	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	-
Fortinet FortiOS Authorization Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190 : Exploit Public-Facing Application, T1133 : External Remote Services	https://security.paloaltonetworks.com/CVE-2024-3393

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21333	✗	Windows: 10 - 11 24H2 Windows Server: 2022 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21334	✗	Windows: 10 - 11 24H2 Windows Server 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege 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-2025-21334

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21335	✗	Windows: 10 - 11 24H2 Windows Server 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege 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-2025-21335

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-23006	✗	SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) Version 12.4.3-02804 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:h:sonicwall:sma1000:*:*:*:*:*:*:*:*	-
SonicWall SMA1000 Pre-Authentication Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	https://www.sonicwall.com/support/knowledge-base/product-notice-urgent-security-notification-sma-1000/250120090802840

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24085	✗	Apple visionOS Version affected before 2.3, tvOS Version affected before 18.3, macOS Version affected before 15.3, watchOS Version affected before 11.3, iOS and iPadOS Version affected before 18.3	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	-
Apple Multiple Products Use After Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/118575 , https://support.apple.com/en-us/108382 , https://support.apple.com/en-us/108926 , https://support.apple.com/en-us/108414

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-40891	✗	Zyxel CPE Series	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:zyxel:cpe:*:*:*:*:*	Mirai
Zyxel CPE Telnet Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	No Patch

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-41710	✗	Mitel SIP Phones	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:mitel:sip_firmware:*:*:*:*:*:*:*:*	Aquabotv3
Mitel SIP Phones Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-88	T1059: Command and Scripting Interpreter	https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0019

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-10562	✗	Dasan GPON home routers	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dasannetworks:gpon_router_firmware:*:*:*:*:*:*:*:*	Aquabotv3
Dasan GPON Routers Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	No Patch

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-10561	✗	Dasan GPON home routers	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dasannetworks:gpon_router_firmware:*:*:*:*:*:*:*:*	Aquabotv3
Dasan GPON Routers Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1556: Modify Authentication, T1059: Command and Scripting Interpreter	No Patch

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-26801	✕	lb-link bl-lte300_firmware	-
	ZERO-DAY		
	✕	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:lb-link:bl-lte300_firmware:1.0.8:*:*:*:*:*:*:*	Aquabotv3
lb-link bl-lte300_firmware Command Injection Vulnerability	✕		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	No Patch

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Quasar	Quasar RAT is a remote access trojan (RAT) written in .NET, designed to target Windows devices. Known for being open-source and fully functional, it has become a popular tool among attackers due to its accessibility and flexibility. While its open-source nature allows legitimate use, cybercriminals frequently pack the malware to obfuscate its source code and hinder analysis. Once deployed, Quasar RAT enables attackers to gain unauthorized remote control of infected systems. Its capabilities include spying on victims, stealing sensitive information, and deploying additional malware.	Masqueraded as Malicious npm package	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Compromise, Deploy another malware	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
NonEuclid	NonEuclid Remote Access Trojan (RAT) is a powerful C# malware designed to grant unauthorized control over victim computers while evading detection. This stealthy RAT employs advanced tactics, including antivirus bypass, privilege escalation, AES encryption, and anti-virtual machine checks, to ensure persistence and resilience.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Unauthorized Remote Control, Privilege Escalation, Data Theft, and Exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PowerRAT	PowerRAT is a PowerShell-based reverse shell that facilitates remote control over a compromised system and employs various techniques to evade detection, such as hiding malicious files using environment variables and encrypting payloads.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		System Compromise and Control, Malware Persistence	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Paper Werewolf			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PowerTaskel	PowerTaskel is a PowerShell-based tool used by the Paper Werewolf cyberespionage group for remote command execution, data collection, and maintaining persistence on compromised systems. It integrates seamlessly with post-exploitation frameworks, enabling stealthy operations and evasion of detection mechanisms. Designed for flexibility, it supports advanced tasks such as file manipulation, process management, and network reconnaissance.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Hack Tool		Compromise of Sensitive Data, Persistence on Target Systems	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Paper Werewolf			-

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
QwakMyAgent	QwakMyAgent is a PowerShell script, previously undetected, that functions as a non-public Mythic modular agent. During execution, the script sends information about the infected system and cyclically receives and processes commands from the server.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Hack Tool		Data Exfiltration, Remote Command Execution	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Paper Werewolf			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
EAGERBEE	The EAGERBEE backdoor showcases advanced capabilities, including a service injector for seamless deployment and plugins designed for delivering payloads, accessing files, and enabling remote control. EAGERBEE further enhances its operations by loading additional modules from remotely-hosted PE files managed by C2 server. In its most recent campaign, EAGERBEE employs an injector DLL to activate the backdoor. Once operational, it gathers system information and exfiltrates the collected data to a remote server via a TCP socket.	Exploiting Vulnerabilities	CVE-2021-26855
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	Microsoft Exchange Server
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855

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
Gayfemboy	The Gayfemboy botnet represents a highly evolved variant of Mirai, leveraging a 0-day vulnerability in Four-Faith industrial routers to establish its foothold. Operating with remarkable sophistication, it boasts over 40 distinct grouping categories and maintains more than 15,000 daily active nodes.	Exploiting Vulnerabilities	CVE-2024-12856
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		DDOS attack	Four-Faith F3x24 and F3x36
ASSOCIATED ACTOR			**PATCH LINK**
-			No patch

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DRYHOOK	DRYHOOK is a Python-based malware designed to steal credentials. Specifically, it modifies a system component called DSAuth.pm, which is responsible for handling authentication, in order to capture successful login attempts. When executed, the malicious script accesses the file located at /home/perl/DSAuth.pm, reading its contents into a buffer. It then employs regular expressions to search for and replace specific lines of code, effectively manipulating the authentication process to exfiltrate sensitive information.	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal Data	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5337			https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

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
PHASEJAM	PHASEJAM is a malicious bash shell script that targets Ivanti Connect Secure appliances. Its primary functionality includes embedding a web shell into the getComponent.cgi and restAuth.cgi files, providing attackers with remote access to the system. Additionally, PHASEJAM disrupts system upgrades by modifying the DSUpgrade.pm file, effectively preventing crucial security updates. The malware also alters the remotedebug executable, enabling the execution of arbitrary commands when a specific parameter is provided. These capabilities allow attackers to maintain persistent control over the compromised system.	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		System Compromise	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5337			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 CVEs
SPAWNANT	SPAWNANT is an ELF32 executable that installs three malicious components from the SPAWN family, each serving a distinct purpose. The three are component, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH. Together, these components enable SPAWNANT to maintain persistence across system upgrades. This ensures that SPAWNANT and its supporting components remain active, even after system upgrades, securing the attacker's foothold for long-term exploitation.	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		Drops other Malware	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5337			https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

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
SPAWNMOLE	SPAWNMOLE is a tunneler that embeds itself into the web process, quietly monitoring network traffic. It takes control of the accept function to inspect incoming connections, filtering out any malicious traffic from the attacker. SPAWNMOLE stays inactive until it detects a specific pattern of magic bytes, which triggers its malicious behavior. Once activated, it redirects the harmful traffic to a remote host provided by the attacker, while allowing harmless traffic to flow to the legitimate web server without alteration. This stealthy method enables SPAWNMOLE to deliver its payload while avoiding detection.	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Web Shell		Deliver Payloads	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5337			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 CVEs
SPAWNSNAIL	SPAWNSNAIL is an SSH backdoor specifically targeting Ivanti devices. It has the capability to inject a chosen binary into other processes, enabling it to run a local SSH backdoor when injected into the dsmdm process. Additionally, SPAWNSNAIL can inject further malware into the dslogserver, expanding its control and enabling additional malicious activities on the compromised system. This allows attackers to maintain persistent access and deploy further threats with minimal detection.	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5337			https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

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
SPAWNSLOTH	SPAWNSLOTH is a log tampering utility designed to manipulate system logs, effectively hiding traces of malicious activity. By altering or erasing log entries, SPAWNSLOTH helps attackers cover their tracks, making it difficult to detect their presence or the actions they've taken on the compromised system.	Exploiting Vulnerabilities	CVE-2025-0282 CVE-2025-0283
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Log Tampering/ Rootkit		Manipulate system logs	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5337			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 CVEs
HexaLocker	HexaLocker ransomware, first identified in mid-2024, has evolved with a significant update in its latest version. This update integrates the open-source Skuld Stealer, a tool specifically designed to extract sensitive data from infected systems before initiating file encryption. The newest iteration of HexaLocker, written in Go, showcases more advanced capabilities, including the ability to download and execute Skuld Stealer, enabling attackers to harvest valuable information before encrypting the victim's files.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data, Steal Data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Skuld	Skuld is an open-source tool designed to target Windows systems and steal sensitive user data from a wide range of applications, including Discord, web browsers, cryptocurrency wallets, and more. Once deployed on a victim's machine, Skuld extracts valuable information such as login credentials, personal data, and wallet keys. Its ability to compromise various applications makes Skuld a versatile and dangerous tool for attackers looking to collect and exploit user information.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Steal Data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Silver	Sliver is an advanced malware framework used in cyberattacks, leveraging DLL sideloading and proxying techniques for persistence and stealth. It targets organizations, enabling data exfiltration and espionage while evading detection.	Spear-phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data exfiltration and Espionage	Windows
Framework			**PATCH LINK**
ASSOCIATED ACTOR			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Resocks	The Resocks Toolkit is an open-source red-team tool used for proxy management and covert communication in cyber operations. It enables attackers to create and manage SOCKS proxies for obfuscating traffic and maintaining anonymity.	Spear-phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data exfiltration and Espionage	Windows
Toolkit			**PATCH LINK**
ASSOCIATED ACTOR			-
Silent Lynx			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SlowStepper	SlowStepper is a backdoor malware deployed in a supply-chain attack against South Korea's VPN service users. It enables attackers to maintain system persistence, collect data, and execute espionage. Built with C++, Python, and Go, SlowStepper infiltrates systems via trojanized VPN installers, compromising victims' devices.	Trojanized VPN installers	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data collection and Espionage	-
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
Cloud Atlas			

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TorNet	TorNet is a sophisticated .NET-based backdoor designed to give attackers remote control over compromised systems. It can download and execute arbitrary .NET assemblies directly in the victim's memory. Once active, TorNet establishes a connection with its command-and-control (C2) server while also routing the infected machine's traffic through the TOR network. This dual connection not only facilitates secure communication with the attackers but also helps mask their activities.	PureCrypter drops the TorNet backdoor	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	-
ASSOCIATE D 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
PureCrypter	PureCrypter is a .NET-based malware loader obfuscated using SmartAssembly, employing compression, encryption, and obfuscation techniques to evade detection by antivirus software. Its key features include persistence, code injection, and defense mechanisms, which are configurable using Google's Protocol Buffer message format. PureCrypter has been observed distributing a range of malicious payloads, including RATs and information stealers, making it a versatile and dangerous tool in cybercriminal campaigns.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Deploy malware	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mirai	Mirai is a well-known malware that targets Internet of Things (IoT) devices by exploiting weak or default passwords. Once infected, these devices are added to a botnet to carry out large-scale Distributed Denial of Service (DDoS) attacks. Its open-source release has led to the creation of several variants.	Exploiting Vulnerabilities	CVE-2024-40891
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Network Overload, Widespread IoT Device Compromise	Zyxel CPE series devices
ASSOCIATED ACTOR			**PATCH LINK**
-			No Patch

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
FunkSec	FunkSec is a file-encrypting ransomware strain written in Rust, believed to be crafted with the assistance of AI. Operating under the ransomware-as-a-service (RaaS) model, FunkSec employs double extortion tactics encrypting victims' data while threatening to leak stolen information to intensify ransom demands. It employs RSA and AES encryption, appends a ".funksec" extension to encrypted files, and aggressively disables security features.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Encrypt Data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Aquabotv3	Aquabotv3 is the latest iteration of the Aquabot botnet, built upon the foundation of the notorious Mirai malware. At first glance, it appears to be a typical Mirai variant, equipped with standard distributed denial-of-service (DDoS) capabilities like flood attacks and bypass techniques. However, Aquabotv3 introduces a significant innovation: the ability to establish direct communication with its command-and-control (C2) server in response to specific system signals. This adaptive feature enhances the botnet's resilience, making it more difficult to detect, disrupt, and dismantle compared to its predecessors.	Exploiting Vulnerabilities	CVE-2024-41710 CVE-2018-17532 CVE-2023-26801 CVE-2022-31137 CVE-2018-10562 CVE-2018-10561
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Network Compromise	Mitel SIP Phones, Teltonika RUT9XX, lb-link bl-lte300_firmwareRoxy Wi, Dasan GPON home routers
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0019 , https://wiki.teltonika-networks.com/view/RUT900_Firmware_Downloads_(legacy_WebUI) , https://github.com/roxy-wi/roxy-wi/releases/tag/v8.1.4

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
Daixin Team	The Daixin Team is a ransomware group notorious for targeting various sectors, with a particular focus on VMware ESXi servers. Their attack methods typically involve exploiting VPN vulnerabilities, conducting phishing campaigns, and taking advantage of weak authentication mechanisms to gain initial access. Once inside a network, they exfiltrate and encrypt sensitive data to maximize the impact of their ransom demands .	Exploit VPN vulnerabilities, Phishing, and weak authentication	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data, Data Theft	-
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 COUNTRY
Paper Werewolf (aka GOFFEE)	-	Government, Energy, Financial, and Media	Russia
	MOTIVE		
	Espionage and Destruction		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	-	PowerRAT, PowerTaskel and QwakMyAgent	Windows

TTPs
TA0005: Defense Evasion; TA0007: Discovery; TA0042: Resource Development; TA0008: Lateral Movement; TA0002: Execution; TA0001: Initial Access; TA0040: Impact; TA0011: Command and Control; TA0003: Persistence; TA0006: Credential Access; T1583: Acquire Infrastructure; T1583.001: Domains; T1008: Fallback Channels; T1583.003: Virtual Private Server; T1105: Ingress Tool Transfer; T1587: Develop Capabilities; T1587.001: Malware; T1608.001: Upload Malware; T1588: Obtain Capabilities; T1566: Phishing; T1588.002: Tool; T1059.001: PowerShell; T1059.005: Visual Basic; T1204: User Execution; T1505: Server Software Component: T1564: Hide Artifacts; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1505.004: IIS Components; T1027.009: Embedded Payloads; T1056: Input Capture; T1529: System Shutdown/Reboot; T1485: Data Destruction; T1564.001: Hidden Files and Directories; T1027.011: Fileless Storage; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1027.007: Dynamic API Resolution; T1027.013: Encrypted/Encoded File; T1033: System Owner/User Discovery; T1573: Encrypted Channel; T1608: Stage Capabilities; T1059: Command and Scripting Interpreter; T1547.001: Registry Run Keys / Startup Folder; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1056.003: Web Portal Capture; T1570: Lateral Tool Transfer; T1573.002: Asymmetric Cryptography

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
UNC5337	China	All	Worldwide
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2025-0282, CVE-2025-0283	DRYHOOK, PHASEJAM, SPAWNANT, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
TTPs			
TA0001: Initial Access; TA0042: Resource Development; TA0002: Execution; TA0004: Privilege Escalation; T1059: Command and Scripting Interpréter; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1588.005: Exploits; T1190: Exploit Public-Facing Application; T1565: Data Manipulation; T1068: Exploitation for Privilege Escalation; T1505.003: Web Shell; T1003: OS Credential Dumping; T1070: Indicator Removal; T1562.001: Disable or Modify Tools; T1562: Impair Defenses			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Star Blizzard (aka Cold River, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto, UNC4057)	Russia **MOTIVE** Information theft and espionage	Government, Diplomacy, Defense Policy, International Relations	Worldwide
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0008: Lateral Movement; TA0010: Exfiltration; T1566: Phishing; T1566.002: Spearphishing Link; T1598: Phishing for Information; T1598.003: Spearphishing Link; T1036: Masquerading; T1589: Gather Victim Identity Information; T1534: Internal Spearphishing; T1078: Valid Accounts; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1204: User Execution; T1204.001: Malicious Link; T1176: Browser Extensions; T1656: Impersonation			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Silent Lynx APT	Iran	Government banks, think tanks, embassies, legal entities	Central Asia and Special Programme for the Economies of Central Asia (SPECA) based nations
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Resocks Toolkit	Windows
TTPs			
TA0043: Reconnaissance; TA0006: Credential Access; T1589.002: Email Addresses; T1078.002: Domain Accounts; T1547.001: Registry Run Keys / Startup Folder; T1552.001: Credentials In Files; T1046: Network Service Discovery; T1007; TA0003: Persistence; TA0007: Discovery; T1589: Gather Victim Identity Information; T1078: Valid Accounts; T1547: Boot or Logon Autostart Execution; T1552; TA0001: Initial Access; TA0009: Collection; T1204.002: Malicious File; T1059.001: PowerShell; TA0002: Execution; TA0010: Exfiltration; T1204: User Execution; T1059: Command and Scripting Interpreter; T1056.001: Keylogging; T1087: Unsecured Credentials; T1012: Query Registry; T1560.001: System Service Discovery Archive via Utility; T1567.002: Exfiltration to Cloud Storage Account Discovery; T1018: Remote System Discovery; T1560: Archive Collected Data; T1056: Input Capture; T1083: File and Directory Discovery; T1016: System Network Configuration Discovery; T1567: Exfiltration Over Web Service			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
STAC5143	Iran	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Unknown Ransomware	Windows

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1090: Proxy; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1049: System Network Connections Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1018: Remote System Discovery; T1482: Domain Trust Discovery; T1656: Impersonation; T1036: Masquerading; T1566: Phishing; T1037: Boot or Logon Initialization Scripts; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1021.006: Windows Remote Management; T1005: Data from Local System; T1486: Data Encrypted for Impact; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
STAC5777	-	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Unknown Ransomware	Windows

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1090: Proxy; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1049: System Network Connections Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1018: Remote System Discovery; T1482: Domain Trust Discovery; T1656: Impersonation; T1036: Masquerading; T1566: Phishing; T1037: Boot or Logon Initialization Scripts; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1021.006: Windows Remote Management; T1005: Data from Local System; T1486: Data Encrypted for Impact; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
PlushDaemon	China	-	South Korea, China, Taiwan, Hong Kong, United States, New Zealand
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	SlowStepper Backdoor	-

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583.001: Domains; T1583.004: Server; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.002: Upload Tool; T1588: Obtain Capabilities; T1588.001: Malware; T1588.002: Tool; T1588.003: Code Signing Certificates; T1588.005: Exploits; T1659: Content Injection; T1190: Exploit Public-Facing Application; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.006: Python; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder; T1547.004: Winlogon Helper DLL; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1222: File and Directory Permissions Modification; T1222.001: Windows File and Directory Permissions Modification; T1070: Indicator Removal; T1070.004: File Deletion; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1112: Modify Registry; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1027.013: Encrypted/Encoded File; T1553: Subvert Trust Controls; T1553.002: Code Signing; T1217: Browser Bookmark Discovery; T1083: File and Directory Discovery; T1120: Peripheral Device Discovery; T1057: Process Discovery; T1012: Query Registry; T1518: Software Discovery; T1082: System Information Discovery; T1614: System Location Discovery; T1016: System Network Configuration Discovery; T1016.002: Wi-Fi Discovery; T1033: System Owner/User Discovery; T1560: Archive Collected Data; T1560.002: Archive via Library; T1123: Audio Capture; T1005: Data from Local System; T1074.001: Local Data Staging; T1113: Screen Capture; T1125: Video Capture; T1071.004: DNS; T1132.001: Standard Encoding; T1573.001: Symmetric Cryptography; T1008: Fallback Channels; T1105: Ingress Tool Transfer; T1104: Multi-Stage Channels; T1095: Non-Application Layer Protocol; T1090: Proxy; T1219: Remote Access Software; T1020: Automated Exfiltration; T1041: Exfiltration Over C2 Channel; T1583: Acquire Infrastructure

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1590: Gather Victim Network Information	
	T1592: Gather Victim Host Information	
	T1598: Phishing for Information	T1598.003: Spearphishing Link
		T1598.002: Spearphishing Attachment
	T1595: Active Scanning	T1595.002: Vulnerability Scanning
TA0042: Resource Development	T1587: Develop Capabilities	T1587.004: Exploits
		T1587.001: Malware
	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.006: Vulnerabilities
		T1588.005: Exploits
	T1583: Acquire Infrastructure	T1583.006: Web Services
		T1583.003: Virtual Private Server
		T1583.001: Domains
	T1608: Stage Capabilities	T1608.001: Upload Malware
	T1650: Acquire Access	
	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1584: Compromise Infrastructure	T1584.001: Domains
		T1584.003: Virtual Private Server
		T1584.004: Server
		T1584.005: Botnet
TA0001: Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.001: Spearphishing Attachment
	T1190: Exploit Public-Facing Application	
	T1133: External Remote Services	
	T1659: Content Injection	
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.001: Default Accounts
	T1091: Replication Through Removable Media	
	T1189: Drive-by Compromise	
	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
	T1659: Content Injection	

Tactic	Technique	Sub-technique
TA0002: Execution	T1204: User Execution	T1204.002: Malicious File
		T1204.001: Malicious Link
	T1609: Container Administration Command	
	T1047: Windows Management Instrumentation	
	T1203: Exploitation for Client Execution	
	T1053: Scheduled Task/Job	T1053.006: Systemd Timers
		T1053.005: Scheduled Task
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.002: AppleScript
		T1059.003: Windows Command Shell
		T1059.005: Visual Basic
		T1059.006: Python
		T1059.004: Unix Shell
		T1059.007: JavaScript
TA0011: Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
		T1071.002: File Transfer Protocols
	T1090: Proxy	
	T1572: Protocol Tunneling	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1571: Non-Standard Port	
	T1659: Content Injection	
	T1573: Encrypted Channel	
	T1219: Remote Access Software	
	T1001: Data Obfuscation	
TA0006: Credential Access	T1003: OS Credential Dumping	
	T1056: Input Capture	T1056.001: Keylogging
	T1212: Exploitation for Credential Access	
	T1555: Credentials from Password Stores	T1555.005:Password Managers
		T1555.003: Credentials from Web Browsers
	T1556: Modify Authentication Process	
	T1040: Network Sniffing	
	T1539: Steal Web Session Cookie	
	T1110: Brute Force	T1110.003: Password Spraying
	T1552: Unsecured Credentials	T1552.004: Private Keys

Tactic	Technique	Sub-technique
TA0006: Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.003: NTDS
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
TA0009: Collection	T1560: Archive Collected Data	
	T1056: Input Capture	T1056.001: Keylogging
	T1115: Clipboard Data	
	T1584: Compromise Infrastructure	
	T1005: Data from Local System	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1113: Screen Capture	
TA0008: Lateral Movement	T1021: Remote Services	T1021.004: SSH
		T1021.001: Remote Desktop Protocol
	T1570: Lateral Tool Transfer	
	T1563: Remote Service Session Hijacking	T1563.002: RDP Hijacking
	T1210: Exploitation of Remote Services	
	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
		T1550.002: Pass the Hash
TA0010: Exfiltration	T1048: Exfiltration Over Alternative Protocol	T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
		T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol
	T1567: Exfiltration Over Web Service	
	T1041: Exfiltration Over C2 Channel	
	T1020: Automated Exfiltration	
TA0003: Persistence	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1556: Modify Authentication Process	
	T1098: Account Manipulation	T1098.005: Device Registration
	T1176: Browser Extensions	
	T1133: External Remote Services	
	T1136.002: Create Account	T1136.001: Local Account
		T1136.002: Domain Account

Tactic	Technique	Sub-technique
TA0003: Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1556: Modify Authentication Process	
	T1543: Create or Modify System Process	T1543.003: Windows Service
TA0004: Privilege Escalation	T1098: Account Manipulation	T1098.005: Device Registration
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1055: Process Injection	
	T1134: Access Token Manipulation	
	T1068: Exploitation for Privilege Escalation	
	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.014: AppDomainManager
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
TA0005: Defense Evasion	T1112: Modify Registry	
	T1218: System Binary Proxy Execution	T1218.007: Msiexec
		T1218.005: Mshta
	T1070: Indicator Removal	
	T1078: Valid Accounts	T1078.002: Domain Accounts
	T1556: Modify Authentication Process	T1556.008: Network Provider DLL
	T1600: Weaken Encryption	
	T1564: Hide Artifacts	T1564.001:Hidden Files and Directories
	T1550: Use Alternate Authentication Material	
	T1036: Masquerading	
	T1656: Impersonation	
	T1134: Access Token Manipulation	
	T1140: Deobfuscate/Decode Files or Information	
	T1027: Obfuscated Files or Information	
	T1562: Impair Defenses	T1562.001:Disable or Modify Tools

Tactic	Technique	Sub-technique
TA0007: Discovery	T1087: Account Discovery	T1087.002: Domain Account
	T1057: Process Discovery	
	T1007: System Service Discovery	
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1124: System Time Discovery	
	T1217: Browser Information Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1518: Software Discovery	
	T1046: Network Service Discovery	
	T1016: System Network Configuration Discovery	
	T1482: Domain Trust Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
TA0040: Impact	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	
	T1565: Data Manipulation	
	T1489: Service Stop	
	T1486: Data Encrypted for Impact	
	T1485: Data Destruction	
	T1490: Inhibit System Recovery	

Top 5 Takeaways

#1 In **January**, there were ten zero-day vulnerabilities with 'Three Celebrity Vulnerabilities' taking center stage. These featured flaws such as **ProxyLogon, LDAPBleed**, and **LDAPNightmare**.

#2 Throughout the month, ransomware strains including **Hexalocker, FunkSec,** and **Daixin Team** actively targeted victims. **FunkSec**, an AI-driven ransomware group, rapidly rose in late 2024, blending cybercrime with hacktivism.

#3 A diverse array of malware families has been recently detected actively targeting victims in real-world environments. These include the **EAGERBEE, Gayfemboy, Quasar, PowerRAT, SlowStepper, Lumma ,** and **Mirai.**

#4 **Seven** active adversaries were identified across multiple campaigns, targeting the following key industries: **Government, Technology, Media,** and **Energy.**

#5 Multiple campaigns leveraging sophisticated, previously unseen malware and ransomware variants orchestrated a total of **25** attacks. These attacks top impacted **Germany, Russia, United States,** and **Egypt.**

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **21 significant vulnerabilities** and block the indicators related to the **7 active threat actors, 25 active malware,** and **164 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 **21 significant vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to **active threat actors, active malware**, and **potential MITRE TTPs** in Breach and Attack Simulation(BAS).

Hive Pro Threat Advisories (January 2025)

MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY	SUNDAY
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

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

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

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

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

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

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

Glossary:

CISA KEV - Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities
CVE - Common Vulnerabilities and Exposures
CPE - Common Platform Enumeration
CWE - Common Weakness Enumeration

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Quasar	SHA256	9c3d53c7723bfdd037df85de4c26efcd5e6f4ad58cc24f7a38a774bf22de3876
	URL	hxxps[://]jujuju[.]lat/files/kk[.]cmd
	Domain	captchacdn[.]com[:]7000
	IPv4	154[.]216[.]17[.]47
NonEuclid	SHA256	d32585b207fd3e2ce87dc2ea33890a445d68a4001ea923daa750d32b5de52bf0, 0521aeba49554242674994b1a8881e819c24f0047870d7e1d120deed76895b55
PowerRAT	SHA256	13252199b18d5257a60f57de95d8c6be7d7973df7f957bca8c2f31e15fcc947b
	IPv4	94[.]103[.]85[.]47
	Domain	disk-yanbex[.]ru
EAGERBEE	MD5	9d93528e05762875cf2d160f15554f44, c651412abdc9cf3105dfbafe54766c44, 26d1adb6d0bcc65e758edaf71a8f665d
Gayfemboy	SHA1	3287158c35c93a23b79b1fbb7c0e886725df5faa, ba9224828252e0197ea5395dad9bb39072933910, fe72a403f2620161491760423d21e6a0176852c3
	SHA256	3ee4d3222dd1856ca58de9715342d5c83562578f869c3482b538ab2c8eb3c832, a0241e3e2a8fb48e2fa0a4ebb72054309f70c79de286b1d00f640347f81e69bd

Attack Name	TYPE	VALUE
DRYHOOK	MD5	61bb586dc4e047ab081ef6ca65684e48
PHASEJAM	MD5	d18e5425ecd9608ecb992606b974e15d
	File Path	/tmp/s
SPAWNANT	File Path	/root/lib/libupgrade.so
SPAWNMOLE	File Path	/root/home/lib/libsocks5.so
	MD5	a638fd203ddb540d0484d8e00490df06, 4f79c70cce4207d0ad57a339a9c7f43c
	Domain	libdsproxy[.]so
SPAWNSNAIL	File Path	/root/home/lib/libsshd.so
	MD5	e7d24813535f74187db31d4114f607a1
	Domain	libdsmeeting[.]so
SPAWNSLOTH	File Path	/tmp/.liblogblock.so
	MD5	4acfc5df7f24c2354384f7449280d9e0
HexaLocker	SHA256	0347aa0b42253ed46fdb4b95e7ffafa40ba5e249dfb5c8c09119f327a1b4795a, 28c1ec286b178fe06448b25790ae4a0f60ea1647a4bb53fb2ee7de506333b960, d0d8df16331b16f9437c0b488d5a89a4c2f09a84dec4da4bc13eab15aded2e05
Skuld	SHA256	8b347bb90c9135c185040ef5fdb87eb5cca821060f716755471a637c350988d8
	URL	hxxps[:]//hexalocker[.]xyz/SGDYSRE67T43TVD6E5RD[.]exe
Silver	SHA256	f778825b254682ab5746d7b547df848406bb6357a74e2966b39a5fa5eae006c2, 83a70162ec391fde57a9943b5270c217d63d050aae94ae3efb75de45df5298be
Resocks Toolkit	SHA256	297d1afa309cdf0c84f04994ffd59ee1e1175377c1a0a561eb25869909812c9c

Attack Name	TYPE	VALUE
SlowStepper	SHA256	40df05b4f04ad093b31c9ca07a559be56a700e49f6051b5cb7462db5f85be8c3
	SHA1	068fd2d209c0bbb0c6fc14e88d63f92441163233
	MD5	e2bc2361ead7c80eba86a5d1c492865d
	Domains	7051[.]gsm[.]360safe[.]company, st[.]360safe[.]company
	IPv4	8[.]130[.]87[.]195 47[.]108[.]162[.]218 47[.]113[.]200[.]18, 202[.]105[.]1[.]187, 47[.]74[.]159[.]166, 47[.]104[.]138[.]190, 120[.]24[.]193[.]58, 202[.]189[.]8[.]87, 202[.]189[.]8[.]69, 202[.]189[.]8[.]193, 47[.]92[.]6[.]64
Lumma	MD5	82e5e8ec8e4e04f4d5808077f38752ba, 14d8486f3f63875ef93cfd240c5dc10b, 0ba2afe43cc4deed266354b1c2cfb5a7
	SHA256	b94ddefd39d32a753564e6871d11750fa56b993cad3ea40955139e584ad3bef8, 86d50a7fc8d245876b791efe85eb7f64cd48b9e9648b4bf8bee22dbae66fe3aa, 02a0bba5b3cc6a650d611c2f6d6a8ce6a696c230521f0de43824a19ced716acd
TorNet	SHA256	13ac538c8c6696a59f890677cf451db77b7c33539da1d380640ce549b2b70ca4, 53e7b3b72695a1eaea7146ec3cbd05d0ce2a1eba87f035ae07849feb4f59ec63
PureCrypter	SHA256	3b4e709768d7cd0cb895de74267f45a6ef6565ebed445393878f17ae02a983e3, 84570dac910557d0d8217db746c9a8fd4a27cd3db89135731c7f3584b37df533, 7ce9af599857827317a444c5a63a08929ec97765bc2624076f4834f323a41da2, 57543fd3673c9595a73c836b153faf68e23938662c5a4b6675205734b688ae95, bff0ec65af8b2bb37fcc5202f823b5877ebdcc8efbd32e08f309cbcb4dc2570c,

Attack Name	TYPE	VALUE
PureCrypter	SHA256	c32d97fb9a1681a7bea3f417abde0264a2332221e317c8543e337baac9307c67, 4280eb4cfa0445a40d8e1dfafdc0eb24613f3536c5959270ef0079034b30e653,edac6216665f1c8b0a09158abdd5e7fab63a386a1c9ad31ddd5ee92a6aa811fc
Mirai	SHA256	fa1b9e78b59cdb26d98da8b00fe701697a55ae9ea3bd11b00695cfbba2b67a7a, 7c41cb2df7b0c34985a18c20267c46b20ed365141fced770f7cdf0ed2214296d, 3c0c87bbc1a908ee2d698bf59722fc050b29aa5dcc9312a7c33c04910ad2f067
FunkSec	SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, 66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd, dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac, b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb, 5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd, e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22, 20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d, dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966
Daixin Team	SHA256	9E42E07073E03BDEA4CD978D9E7B44A9574972818593306BE1F3DCFDEE722238, 19ED36F063221E161D740651E6578D50E0D3CACEE89D27A6EBED4AB4272585BD, 54E3B5A2521A84741DC15810E6FED9D739EB8083CB1FE097CB98B345AF24E939, EC16E2DE3A55772F5DFAC8BF8F5A365600FAD40A244A574CBAB987515AA40CBF, 475D6E80CF4EF70926A65DF5551F59E35B71A0E92F0FE4DD28559A9DEBA60C28
	File Path	rclone-v1.59.2-windows-amd64\git-log.txt, rclone-v1.59.2-windows-amd64\rclone.1, rclone-v1.59.2-windows-amd64\rclone.exe, rclone-v1.59.2-windows-amd64\README.html, rclone-v1.59.2-windows-amd64\README.txt
	Tor Address	7ukmkdtyxdkdivtjad57klqnd3kdsmq6tp45rrsxqnu76zzv3jvitlqd[.]onion, 232fwh5cea3ub6qguz3pynijxfzl2uj3c73nbrayipf3gq25vtq2r4qd[.]onion

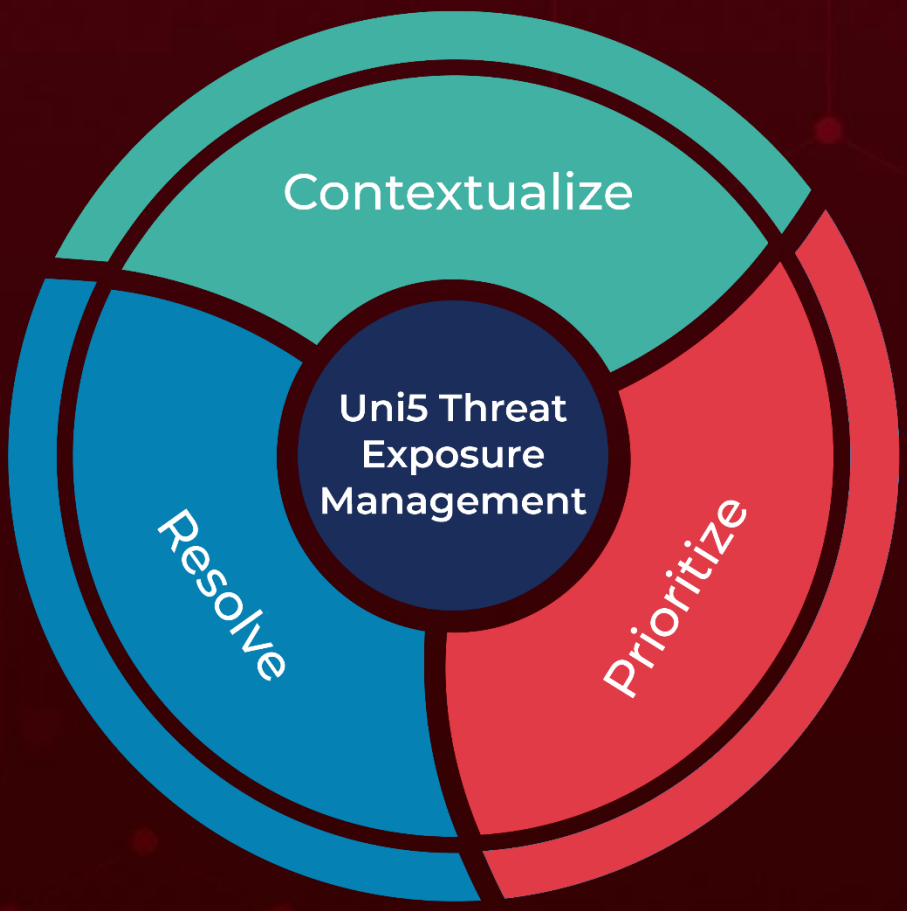
Attack Name	TYPE	VALUE
PureCrypter	SHA256	c32d97fb9a1681a7bea3f417abde0264a2332221e317c8543e337baac9307c67, 4280eb4cfa0445a40d8e1dfafdc0eb24613f3536c5959270ef0079034b30e653,edac6216665f1c8b0a09158abdd5e7fab63a386a1c9ad31ddd5ee92a6aa811fc
Mirai	SHA256	fa1b9e78b59cdb26d98da8b00fe701697a55ae9ea3bd11b00695cfbba2b67a7a, 7c41cb2df7b0c34985a18c20267c46b20ed365141fced770f7cdf0ed2214296d, 3c0c87bbc1a908ee2d698bf59722fc050b29aa5dcc9312a7c33c04910ad2f067
FunkSec	SHA256	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c, 66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd, dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac, b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb, 5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd, e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22, 20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d, dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966
Daixin Team	SHA256	9E42E07073E03BDEA4CD978D9E7B44A9574972818593306BE1F3DCFDEE722238, 19ED36F063221E161D740651E6578D50E0D3CACEE89D27A6EBED4AB4272585BD, 54E3B5A2521A84741DC15810E6FED9D739EB8083CB1FE097CB98B345AF24E939, EC16E2DE3A55772F5DFAC8BF8F5A365600FAD40A244A574CBAB987515AA40CBF, 475D6E80CF4EF70926A65DF5551F59E35B71A0E92F0FE4DD28559A9DEBA60C28

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 4, 2025 • 9:30 AM

More at www.hivepro.com