Date of Publication
October 1, 2025

Hive Pro

Hiveforce Labs

MONTHLY

THREAT DIGEST

Vulnerabilities, Attacks, and Actors

SEPTEMBER 2025

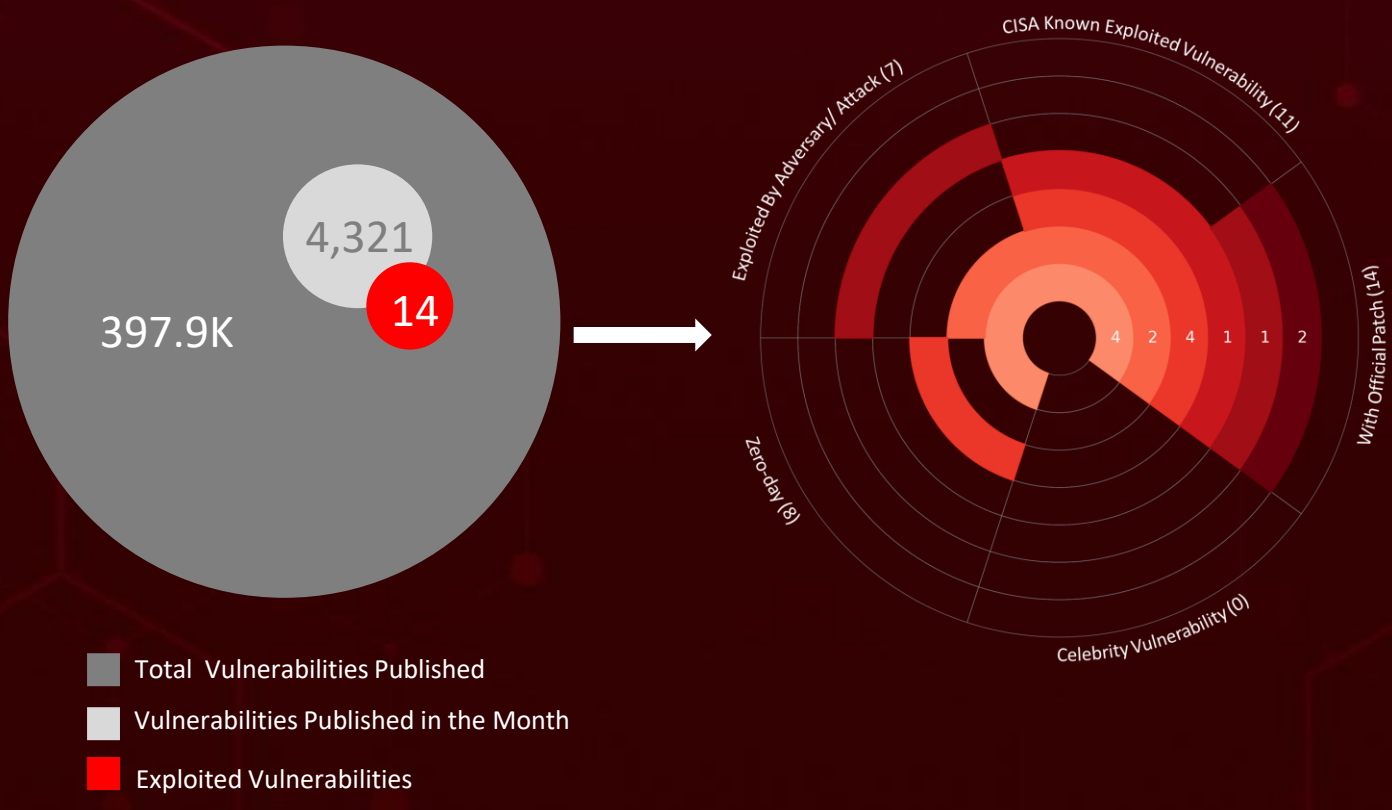
Table Of Contents

Summary

September proved to be one of the most turbulent months in cybersecurity, marked by the active exploitation of **eight zero-day** vulnerabilities. Among the most critical was **CVE-2025-53690** in Sitecore, which is under active attack in the wild to deploy the **WEEPSTEEL** malware. Another high-profile case involved a **zero-click** vulnerability in WhatsApp's iOS and macOS applications (**CVE-2025-55177**). This flaw was exploited as part of a sophisticated zero-day exploit chain in conjunction with Apple's **CVE-2025-43300**, highlighting the growing risks of seamless, user-independent attack vectors.

In parallel, ransomware operations continue to escalate. The **NightSpire** Ransomware-as-a-Service (RaaS) group has been exploiting vulnerabilities such as **CVE-2024-55591** in FortiOS to gain initial access. Meanwhile, **PromptLock** ransomware, the first known **AI-driven ransomware** written in Golang, demonstrates how cybercriminals are weaponizing large language models to generate adaptive malicious code.

Meanwhile, **GhostRedirector**, a newly attributed **China-aligned** actor, has been targeting Windows servers globally. By mid-2025, the group had compromised at least **65 servers** using SQL injection vulnerabilities, privilege escalation exploits, and the deployment of custom malware. Organizations must prioritize proactive defense strategies, patch critical vulnerabilities without delay, and adopt behavior-driven security frameworks to stay ahead in an ever-evolving digital battleground.



Insights

In September 2025, a geopolitical cybersecurity landscape unfolds, revealing the **United States, Japan, South Korea, Singapore,** and **Thailand** as the top-targeted countries

Highlighted in **September 2025** is a cyber battleground encompassing the **Technology, Healthcare, Legal, Education,** and **Manufacturing** sectors, designating them as the top industries

Quad7 Botnet Turns TP-Link Vulnerabilities Into Large-Scale **Brute-Force Attacks**

CVE-2025-10585: Sixth Zero-Day in Chrome This Demands Immediate Update

Operation HanKook Phantom: APT37 Exploits Cloud Services in Fileless Malware Campaign

'EvilAI' Malware Campaign Spreads Across Europe, Americas, and AMEA

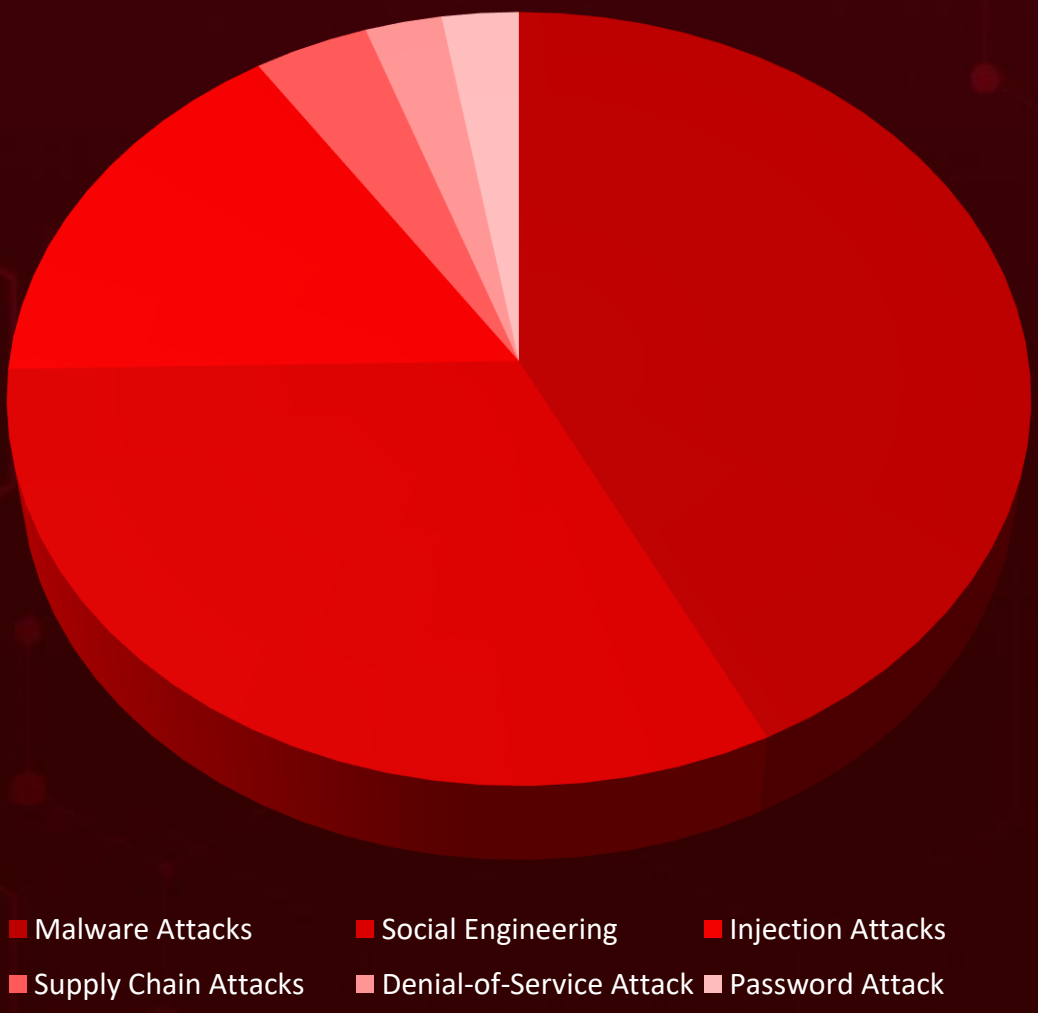
Shai-Hulud Supply Chain Attack Targets npm Ecosystem, Compromises Hundreds of Packages

GPUGate Malware Uses Malvertising and GitHub Commits to Lure Victims

s1ngularity Attack Breaches Nx Supply Chain, Exposes Over 6,700 Repositories

Operation Rewrite Exploits IIS Modules to Redirect Users to Scams

Threat Landscape



Vulnerabilities Summary

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-7775	Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✓	✓	✓
CVE-2024-55591	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	Fortinet FortiOS and FortiProxy	✓	✓	✓
CVE-2025-55177	Meta Platforms WhatsApp Incorrect Authorization Vulnerability	WhatsApp for iOS, Mac, WhatsApp Business for iOS	✗	✓	✓
CVE-2025-43300	Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability	macOS, iOS and iPadOS	✓	✓	✓
CVE-2023-50224	TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability	TP-Link TL-WR841N routers	✗	✓	✓
CVE-2025-9377	TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability	Archer C7(EU) V2, TL-WR841N/ND(MS) V9	✗	✓	✓
CVE-2025-53690	Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability	Sitecore Experience Manager (XM), Experience Platform (XP), Experience Commerce (XC), and Managed Cloud	✓	✓	✓
CVE-2025-55234	Windows SMB Elevation of Privilege Vulnerability	Windows Server	✗	✗	✓
CVE-2024-21907	Newtonsoft.Json Denial of Service Vulnerability	Microsoft SQL Server	✗	✗	✓
CVE-2024-7344	Howyar Reloader UEFI Application Untrusted Search Path Vulnerability	Howyar Reloader UEFI Application	✗	✗	✓
CVE-2025-10585	Google Chromium V8 Type Confusion Vulnerability	Google Chrome	✓	✓	✓
CVE-2025-20352	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability	Cisco IOS & IOS XE Software	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	KEV	PATCH
CVE-2025-20333	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability	Cisco ASA Software, Cisco FTD Software	✓	✓	✓
CVE-2025-20362	Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability	Cisco ASA Software, Cisco FTD Software	✓	✓	✓

Attacks Summary

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
RokRAT	RAT	-	-	-	Using fake newsletters and weaponized shortcut files
NightSpire	Ransomware	CVE-2024-55591	Fortinet FortiOS and FortiProxy	✓	Exploiting Vulnerability
PromptLock	Ransomware	-	-	-	-
Rungan	Backdoor	-	Windows	-	Through SQL injection flaws
Gamshen	Trojan	-	Windows	-	Through SQL injection flaws
Quad 7 (7777)	Botnet	CVE-2023-50224 CVE-2025-9377	TP-Link Multiple Routers	✓	Exploiting Vulnerabilities
WEEPSTEEL	Reconnaissance Tool	CVE-2025-53690	Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud	✓	Exploiting Vulnerabilities
EARTHWORM	Tunneler	CVE-2025-53690	Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud	✓	Exploiting Vulnerabilities
DWAGENT	Remote Access Tool	CVE-2025-53690	Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud	✓	Exploiting Vulnerability
SHARPHOUND	Reconnaissance Tool	CVE-2025-53690	Sitecore Experience Manager (XM), Experience Platform (XP), andExperience Commerce (XC), Managed Cloud	✓	Exploiting Vulnerability

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Cephalus	Ransomware	-	-	-	Remote Desktop Protocol (RDP) via compromised accounts
GPUGate	Trojan	-	-	-	Social Engineering, Malvertising
Stealerium	Infostealer	-	-	-	Financial-Themed Phishing Emails
Warp Stealer	Infostealer	-	-	-	Social Engineering
Phantom Stealer	Infostealer	-	-	-	Social Engineering
MostereRAT	RAT	-	-	-	Phishing Emails
The Gentlemen	Ransomware	-	-	-	Exploiting internet-exposed services
ZynorRAT	RAT	-	Windows, Linux	-	-
kkRAT	RAT	-	Windows	-	Phishing
ValleyRAT	RAT	-	Windows	-	Phishing
FatalRAT	RAT	-	Windows	-	Phishing
EvilAI	Stager	-	Windows	-	Social Engineering
HybridPetya	Ransomware	CVE-2024-7344	Howyar Reloader UEFI Application	✓	-
SnakeDisk	USB worm	-	-	-	Social Engineering

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
Yokai	Backdoor	-	-	-	Social Engineering
Pubload	Downloader	-	-	-	Social Engineering
Toneshell	Backdoor	-	-	-	Social Engineering
StealC	Infostealer	-	-	-	Phishing
Yurei	Ransomware	-	-	-	-
BlackNevas	Ransomware	-	-	-	Phishing, Exploiting Vulnerabilities
VenomRAT	RAT	-	Windows	-	Phishing
Shai-Hulud	Worm	-	npm ecosystem, GitHub repositories	-	Phishing
SilentSync	RAT	-	Windows, Linux, macOS	-	Social Engineering
Kazuar	Backdoor	-	-	-	-
PteroOdd	Downloader	-	-	-	-
MINIBIKE	Backdoor	-	Windows	-	Social Engineering
Atomic Stealer	Stealer	-	macOS	-	By abusing GitHub Pages and SEO
BadIIS	Backdoor	-	-	-	Social Engineering
DeerStealer	Information stealer	-	-	-	Phishing
BAITSWITCH	Downloader	-	-	-	Phishing

ATTACK NAME	TYPE	CVEs	IMPACTED PRODUCT	PATCH	DELIVERY METHOD
SIMPLEFIX	Backdoor	-	-	-	Phishing
BRICKSTORM	Backdoor	-	-	-	Exploiting Vulnerabilities
DarkCloud	Information stealer	-	Windows	-	Spear-phishing email
RayInitiator	Bootkit	CVE-2025-20333 CVE-2025-20362	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD)		Firmware / ROM modification
Line Viper	Loader	CVE-2025-20333 CVE-2025-20362	Microsoft SharePoint Server		Reflective in-memory injection

Adversaries Summary

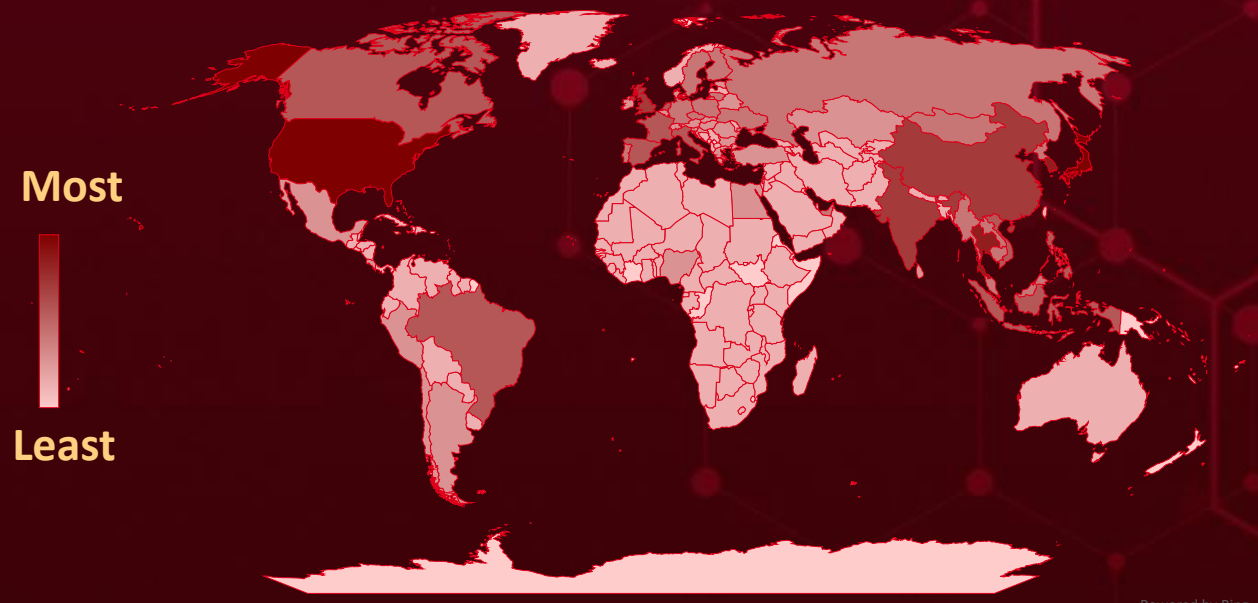
ACTOR NAME	MOTIVE	ORIGIN	CVEs	ATTACK	PRODUCT
APT37	Information theft and espionage	North Korea	-	RokRAT	-
GhostRedirector	Information theft	China	-	Rungan, Gamshen	-
Storm-0940	Information theft	China	CVE-2023-50224 CVE-2025-9377	Quad 7 (7777) Botnet	TP-Link Multiple Routers
Hive0154	Information theft and espionage	China	-	SnakeDisk, Yokai, Pubload, Toneshell	-
RevengeHotels	Financial crime	-	-	VenomRAT	-
Gamaredon	Information theft and espionage	Russia	-	Kazuar backdoor, PteroOdd	-
Turla	Information theft and espionage	Russia	-	Kazuar backdoor, PteroOdd	-
Subtle Snail	Information theft and espionage	Iran	-	MINIBIKE	-
COLDRIVER	Information theft and espionage	Russia	-	BAITSWITCH, SIMPLEFIX	-
UNC5221	Information theft and espionage	China	-	BRICKSTORM	-
UAT4356	Espionage	China	CVE-2025-20333 CVE-2025-20362	RayInitiator bootkit, Line Viper loader	Cisco ASA and FTD

Targeted Products

VENDOR	PRODUCT TYPE	PRODUCT WITH VERSION
citrix	Application Delivery Controller (ADC)	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.48, NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1- 59.22
	Security Appliance	NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.241-FIPS and NDcPP, NetScaler ADC 12.1-FIPS and NDcPP BEFORE 12.1-55.330-FIPS and NDcPP
FORTINET	Network Security Platform	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
WhatsApp	Application	WhatsApp for iOS prior to v2.25.21.73, WhatsApp Business for iOS v2.25.21.78, WhatsApp for Mac v2.25.21.78
	Operating System (OS)	macOS: All versions before macOS Sequoia 15.6.1, macOS Sonoma 14.7.8, and macOS Ventura 13.7.8. iOS and iPadOS: All versions before iOS/iPadOS 18.6.2 and 17.7.10.
tp-link	Networking Equipment	TP-Link TL-WR841N routers, Archer C7(EU) V2: before 241108 and TL-WR841N/ND(MS) V9: before 241108
SITECORE	Application	Sitecore Experience Manager (XM) and Experience Platform (XP) Through Version 9.0, Experience Commerce (XC), Managed Cloud, AD Version 1.4 and earlier
Microsoft	Operating Systems	Windows 10 Version 21H2; Windows 11 Version: 21H2, 24H2, Windows Server: 2025, 2022, 2019, 2012 R2, 2016
	Enterprise Application Server	Microsoft SQL Server 2019, 2017, 2016

VENDOR	PRODUCT TYPE	PRODUCT ALONG WITH VERSION
	Open-Source Library	Newtonsoft.Json before version 13.0.1
	Application	Howyar Reloader UEFI Application
	Web Browser	Google Chrome prior to 140.0.7339.185
CISCO	Network Device	Cisco IOS & IOS XE Software, Meraki MS390 Switches – Meraki CS 17 and earlier, Cisco Catalyst 9300 Series Switches - Meraki CS 17 and earlier
	Security Appliance	Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23, Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7

Targeted Countries



Color	Countries
	United States
	Japan
	South Korea
	Singapore
	Thailand
	India
	China
	United Kingdom
	Brazil
	France
	Canada
	Indonesia
	Philippines
	Italy
	Spain
	Vietnam
	Netherlands
	Ukraine
	United Arab Emirates
	Lithuania
	Mongolia

Color	Countries
	Finland
	Myanmar
	Russia
	Cambodia
	Czech Republic
	North Korea
	Sweden
	Germany
	Timor-Leste
	Poland
	Brunei
	Portugal
	Luxembourg
	Malaysia
	Laos
	Malta
	Slovenia
	Republic of Ireland
	Costa Rica
	Chile
	Croatia

Color	Countries
	Nigeria
	Cyprus
	Bulgaria
	Argentina
	Switzerland
	Denmark
	Belgium
	Egypt
	Monaco
	Estonia
	Peru
	Austria
	Romania
	Greece
	Slovakia
	Hungary
	Sri Lanka
	Kazakhstan
	Turkey
	Liechtenstein
	Belarus
	Mexico
	Algeria
	Togo
	Ghana
	Guyana
	Oman

Color	Countries
	Haiti
	Holy See
	Cameroon
	Honduras
	Antigua and Barbuda
	Hong Kong
	Paraguay
	Dominican Republic
	Djibouti
	Iceland
	Serbia
	Azerbaijan
	Andorra
	Bahamas
	Tajikistan
	Iran
	Turkmenistan
	Iraq
	North Macedonia
	Israel
	Palestine

Color	Countries
	Bahrain
	Botswana
	Jamaica
	Gabon
	Bangladesh
	Saint Kitts and Nevis
	Jordan
	Saudi Arabia
	Ecuador
	Sierra Leone
	Kenya
	South Africa
	Kuwait
	Sudan
	Kyrgyzstan
	Syria
	Barbados
	Angola
	Yemen
	Tunisia
	Zimbabwe
	Chad

Targeted Industries

TOP 25 MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1204** User Execution	**T1036** Masquerading	**T1071** Application Layer Protocol
T1041 Exfiltration Over C2 Channel	**T1566** Phishing	**T1083** File and Directory Discovery	**T1005** Data from Local System	**T1082** System Information Discovery
T1547 Boot or Logon Autostart Execution	**T1059.001** PowerShell	**T1068** Exploitation for Privilege Escalation	**T1071.001** Web Protocols	**T1053** Scheduled Task/Job
T1190 Exploit Public-Facing Application	**T1140** Deobfuscate/ Decode Files or Information	**T1078** Valid Accounts	**T1070** Indicator Removal	**T1021** Remote Services
T1588 Obtain Capabilities	**T1562** Impair Defenses	**T1204.002** Malicious File	**T1087** Account Discovery	**T1555** Credentials from Password Stores

Top Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
NightSpire	SHA256	32e10dc9fe935d7c835530be214142041b6aa25ee32c62648dea124401137ea5
PromptLock	SHA256	2755e1ec1e4c3c0cd94ebe43bd66391f05282b6020b2177ee3b939fdd33216f6, 1612ab799df51a7f1169d3f47ea129356b42c8ad81286d05b0256f80c17d4089, b43e7d481c4fdc9217e17908f3a4efa351a1dab867ca902883205fe7d1aab5e7, 09bf891b7b35b2081d3ebca8de715da07a70151227ab55aec1da26eb769c006f, e24fe0dd0bf8d3943d9c4282f172746af6b0787539b371e6626bdb86605ccd70, 1458b6dc98a878f237bfb3c3f354ea6e12d76e340cefe55d6a1c9c7eb64c9aee
Quad 7	SHA256	f8a78c33d4f37fd5b367f84536a738bc91d50a76a58d1b595c878f4c4d7f4dd1
WEEPSTEEL	SHA256	a566cceaf9a66332470a978a234a8a8e2bbdd4d6aa43c2c75c25a80b3b744307
	MD5	117305c6c8222162d7246f842c4bb014
Cephalus	SHA256	b3e53168fc05aeedea828bd2042e2cc34bbf8193deadab9dd4aa507e5b9c045a, a34acd47127196ab867d572c2c6cf2fcccffa3a7a87e82d338a8efed898ca722, 91c459804dbf8739e2acbc6f13d8d324bceeed3f9a004f78d5475c717b04c8b5, cd28d8cc58d17521f68f04ce33ec23a3ccce95a6a4a94e8dd19697fb0bbf04b4
	Email	sadklajsdioqw[@]proton[.]me
	Tox ID	91C24CC1586713CA606047297516AF534FE57EFA8C3EA2031B7DF8D116AC751B156869CB8838
	TOR Address	cephalus6oiypuwumqlwurvbmwsfglg424zjdmywfgqm4iehkqivsjyd[.]onion
Stealerium	SHA256	a00fda931ab1a591a73d1a24c1b270aee0f31d6e415dfa9ae2d0f126326df4bb
The Gentlemen	SHA1	c12c4d58541cc4f75ae19b65295a52c559570054

Attack Name	TYPE	VALUE
ZynorRAT	SHA256	037e5fe028a60604523b840794d06c8f70a9c523a832a97ecaaccd9f419e364a, 47338da15a35c49bcd3989125df5b082eef64ba646bb7a2db1565bb413b69323, c890c6e6b7cc6984cd9d9061d285d814841e0b8136286e6fd943013260eb8461, 237a40e522f2f1e6c71415997766b4b23f1526e2f141d68ff334de3ff5b0c89f, 48c2a8453feea72f8d9bfb9c2731d811e7c300f3e1935bddd7188324aab7d30d, 4cd270b49c8d5c31560ef94dc0bee2c7927d6f3e77173f660e2f3106ae7131c3, a6c450f9abff8a22445ba539c21b24508dd326522df525977e14ec17e11f7d65, bceccc566fe3ae3675f7e20100f979eaf2053d9a4f3a3619a550a496a4268ef5, 8b09ba6e006718371486b3655588b438ade953beecf221af38160cbe6fedd40a, f9eb2a54e500b3ce42950fb75af30955180360c978c00d081ea561c86e54262d
kkRAT	SHA256	f557a90c1873eeb7f269ae802432f72cc18d5272e13f86784fdc3c38cbaca019
	IPv4:Port	154[.]44[.]30[.]27[:]8250
EvilAI	SHA256	8ecd3c8c126be7128bf654456d171284f03e4f212c27e1b33f875b8907a7bc65
HybridPetya ransomware	Filenames	bootmgfw.efi, core.dll, f20000.mbam _update.exe, improved_not petyanew.exe, notpetya _new.exe, notpetyanew.exe, notpetyanew_improved_final.exe, bootmgfw.efi, cloak.dat
	SHA1	BD35908D5A5E9F7E41A61B7AB598AB9A88DB723D, 9DF922D00171AA3C31B75446D700EE567F8D787B, 9B0EE05FFFDA0B16CF9DAAC587CB92BB06D3981B, CDC8CB3D211589202B49A48618B0D90C4D8F86FD, D31F86BA572904192D7476CA376686E76E103D28, A6EBFA062270A321241439E8DF72664CD54EA1BC, C8E3F1BF0B67C83D2A6D9E594DE8067F0378E6C5, C7C270F9D3AE80EC5E8926A3CD1FB5C9D208F1DC, 3393A8C258239D6802553FD1CCE397E18FA285A1, 98C3E659A903E74D2EE398464D3A5109E92BD9A9, D0BD283133A80B47137562F2AAAB740FA15E6441

Attack Name	TYPE	VALUE
Shai-Hulud	SHA256	46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09, b74caeaa75e077c99f7d44f46daaf9796a3be43ecf24f2a1fd381844669da777, dc67467a39b70d1cd4c1f7f7a459b35058163592f4a9e8fb4dffcbba98ef210c, 4b2399646573bb737c4969563303d8ee2e9ddbd1b271f1ca9e35ea78062538db, de0e25a3e6c1e1e5998b306b7141b3dc4c0088da9d7bb47c1c00c91e6e4f85d6, 81d2a004a1bca6ef87a1caf7d0e0b355ad1764238e40ff6d1b1cb77ad4f595c3, 83a650ce44b2a9854802a7fb4c202877815274c129af49e6c2d1d5d5d55c501e
StealC	SHA256	70ae293eb1c023d40a8a48d6109a1bf792e1877a72433bcc89613461cffc7b61
VenomRAT	SHA256	a5d1e69076fd9f52d8a804202a21852fe2b76fb4534f48455def652e84cceaab
DeerStealer	SHA256	b57c56e5f0d15eea013c39b5c169f3308ca3e8ffd0cf5b1ef001dba894beeef0, 24475ae7781189075f64a2de1a7d1fd69b341b7adee67f0bd2286cfbf1f0b7f9, eb17f8296482b0c096a2249844a62988b6abdd8ffe8cbbe3398f422968d46875, e34d753f2b992cf74c1b9db61bad4d6c6089ab8ef9fb942c865290b2dd64b4ad, 9163f9237ad869a74715f9b126f7c577bd1f12afb8eae37ba07c11f00a39fa3e, 4640d425d8d43a95e903d759183993a87bafcb9816850efe57ccfca4ace889ec, 569ac32f692253b8ab7f411fec83f31ed1f7be40ac5c4027f41a58073fef8d7d, 66282239297c60bad7eeae274e8a2916ce95afeb932d3be64bb615ea2be1e07a, a6f6175998e96fcecad5f9b3746db5ced144ae97c017ad98b2caa9d0be8a3cb5, b5ab21ddb7cb5bfbedee68296a3d98f687e9acd8ebcc4539f7fd234197de2227, d9db8cdef549e4ad0e33754d589a4c299e7082c3a0b5efdee1a0218a0a1bf1ee, e24c311a64f57fd16ffc98f339d5d537c16851dc54d7bb3db8778c26ccb5f2d1
Kazuar	SHA256	3ecb09e659bcb500f9f40d022579a09acb11aec3a92c03e7d3fd2e56982d9eea
	SHA1	da7d5b9ab578ef6487473180b975a4b2701fda9e, d7df1325f66e029f4b77e211a238aa060d7217ed,

Attack Name	TYPE	VALUE
Kazuar	SHA1	a7acee41d66b537d900403f0e6a26ab6a1290a32, 54f2245e0d3adec566e4d822274623bf835e170c, 371ab9eb2a3da44099b2b7716de0916600450cfd, 4a58365eb8f928ec3cd62ff59e59645c2d8c0ba5, 214dc22fa25314f9c0dda54f669ede72000c85a4
PteroOdd	SHA1	7db790f75829d3e6207d8ec1cbcd3c133f596d67, 2610a899fe73b8f018d19b50be55d66a6c78b2af, 3a24520566bbe2e262a2911e38fd8130469ba830
BAITSWITCH	SHA256	87138f63974a8ccbbf5840c31165f1a4bf92a954bacccfbf1e7e5525d750aa48
SIMPLEFIX	SHA256	16a79e36d9b371d1557310cb28d412207827db2759d795f4d8e27d5f5afaf63f
BRICKSTORM	SHA256	90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035, 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df, aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-7775	✗	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.48 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-59.22 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.241-FIPS and NDcPP NetScaler ADC 12.1-FIPS and NDcPP BEFORE 12.1-55.330-FIPS and NDcPP	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-119	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1499: Endpoint Denial of Service	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_7775_CVE_2025_7776_and_CVE_2025_8424

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:*:*:*:*:*:*:*:*	NightSpire ransomware
Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190 : Exploit Public-Facing Application, T1133 : External Remote Services	https://fortiguard.fortinet.com/psirt/FG-IR-24-535

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-55177	✗	WhatsApp for iOS prior to v2.25.21.73, WhatsApp Business for iOS v2.25.21.78, WhatsApp for Mac v2.25.21.78	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:whatsapp:whatsapp:*:*:*:*:*:*:iphone_os:*:* cpe:2.3:a:whatsapp:whatsapp:*:*:*:*:*:*:macos:*:* cpe:2.3:a:whatsapp:whatsapp_business:*:*:*:*:*:*:iphone_os:*:*	-
Meta Platforms WhatsApp Incorrect Authorization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1204: User Execution; T1204.001: Malicious Link	https://www.whatsapp.com/download

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-43300</td><td>✗</td><td rowspan="2">macOS: All versions before macOS Sequoia 15.6.1, macOS Sonoma 14.7.8, and macOS Ventura 13.7.8.
iOS and iPadOS: All versions before iOS/iPadOS 18.6.2 and 17.7.10.</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:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Apple iOS, iPadOS, and macOS Out-of-Bounds Write 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>T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution</td><td>https://support.apple.com/en-us/124925 , https://support.apple.com/en-us/124926 , https://support.apple.com/en-us/124927 , https://support.apple.com/en-us/124928 , https://support.apple.com/en-us/124929</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-50224		TP-Link TL-WR841N routers	Storm-0940
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:tp-link:tl-wr841n_firmware:3.16.9:build_200409:*:*:*:*:*:*:* cpe:2.3:h:tp-link:tl-wr841n:12:*:*:*:*:*:*:*	Quad 7 (7777)
TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-290	T1190: Exploit Public-Facing	https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-9377</td><td>  </td><td rowspan="2">Archer C7(EU) V2: before 241108 and TL-WR841N/ND(MS) V9: before 241108</td><td rowspan="2">Storm-0940</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:tp-link:tl-wr841n_firmware:*:*:*:*:*:*:*:*
cpe:2.3:h:tp-link:tl-wr841n:v9:*:*:*:*:*:*:*
cpe:2.3:o:tp-link:tl-wr841nd_firmware:*:*:*:*:*:*:*:*
cpe:2.3:h:tp-link:tl-wr841nd:9:*:*:*:*:*:*:*
cpe:2.3:o:tp-link:archer_c7_firmware:*:*:*:*:*:*:*:*
cpe:2.3:h:tp-link:archer_c7:2.0:*:*:*:*:*:*:*</td><td rowspan="2">Quad 7 (7777)</td></tr>
<tr><td rowspan="2">TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-78</td><td>T1190: Exploit Public-Facing; T1059: Command and Scripting Interpreter</td><td>https://www.tp-link.com/us/support/faq/4308/</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-2025-53690</td><td>  </td><td rowspan="2">Sitecore Experience Manager (XM) and Experience Platform (XP) Through Version 9.0, Experience Commerce (XC), Managed Cloud, AD Version 1.4 and earlier</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:sitecore:experience_platform:*:*:*:*:*:*:*:* cpe:2.3:a:sitecore:experience_manager:*:*:*:*:*:*:*:* cpe:2.3:a:sitecore:experience_commerce:*:*:*:*:*:*:*:*</td><td rowspan="2">WEEPSTEEL, EARTHWORM, DWAGENT, SHARPHOUND</td></tr>
<tr><td rowspan="2">Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-502</td><td>T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter</td><td>https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-55234	✗	Windows Server: 2025, 2022, 2019, 2012 R2, 2016; Windows 10 Version 21H2; Windows 11 Version: 21H2, 24H2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	-
Windows SMB Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1021.002: SMB/Windows Admin Shares, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-55234

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTOR
CVE-2024-21907	✗	Microsoft SQL Server 2019, 2017, 2016, Newtonsoft.Json before version 13.0.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:newtonsoft:json.net:*:*:*:*:*:*:*:*	-
Newtonsoft.Json Denial of Service Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-755	T1498: Network Denial of Service	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-21907

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7344		Howyar Reloader UEFI Application	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cs-grp:neo_impact:*:*:*:*:*:*:*:* cpe:2.3:a:greenware:greenguard:*:*:*:*:*:*:*:* cpe:2.3:a:howyar:sysreturn:*:*:*:*:*:*:*:* cpe:2.3:a:radix:smart_recovery:*:*:*:*:*:*:*:* cpe:2.3:a:sanfong:ez-back_system:*:*:*:*:*:*:*:* cpe:2.3:a:signalcomputer:hdd_king:*:*:*:*:*:*:*:* cpe:2.3:a:wasay:erecoveryrx:*:*:*:*:*:*:*:*	HybridPetya ransomware
Howyar Reloader UEFI Application Untrusted Search Path Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-347	T1542: Pre-OS Boot	https://uefi.org/revocationlistfile , https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7344

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-10585	✗	Google Chrome prior to 140.0.7339.185	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium V8 Type Confusion Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html , https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-20352	✗ ZERO-DAY	Cisco IOS & IOS XE Software, Meraki MS390 Switches – Meraki CS 17 and earlier, Cisco Catalyst 9300 Series Switches - Meraki CS 17 and earlier	-
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:cisco:ios:*:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:*:*	-
Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-121	T1059:Command and Scripting Interpreter; T1499: Endpoint Denial of Service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-20333	✗ ZERO-DAY	Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23, Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7	UAT4356 (aka Storm-1849)
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*:*	RayInitiator bootkit, Line Viper loader
Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-120	T1071.001: Web Protocols, T1071: Application Layer Protocol, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-20362</td><td>  </td><td rowspan="2">Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23, Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7</td><td rowspan="2">UAT4356 (aka Storm-1849)</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:cisco:firepower_threat_defense:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*</td><td rowspan="2">RayInitiator bootkit, Line Viper loader</td></tr>
<tr><td>Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization 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-862</td><td>T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts</td><td>https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks</td></tr>
</table>

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RokRAT	RokRAT is a sophisticated remote access trojan that collects sensitive system data, captures live screenshots, monitors processes, and maintains encrypted command-and- control communications via cloud APIs on services like Dropbox, pCloud, and Yandex.	Using fake newsletters and weaponized shortcut files	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
APT37			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
NightSpire	NightSpire is a ransomware group that surfaced in February 2025, quickly making a name for itself with an aggressive strategy and a structured infrastructure resembling the Ransomware-as-a-Service (RaaS) model. The group runs a Dedicated Leak Site (DLS), where it publishes stolen data from victims alongside a countdown timer, using the threat of public exposure as leverage to pressure organizations into paying ransoms.	Exploiting Vulnerability	CVE-2024-55591
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		Encrypt data, Data Theft	Fortinet FortiOS and FortiProxy
ASSOCIATED ACTOR			**PATCH LINK**
-			https://fortiguard.fortinet.com/psirt/FG-IR-24-535

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
PromptLock	PromptLock is the first known AI-powered ransomware written in Golang. Unlike traditional strains, this proof-of-concept demonstrates how large language models can be leveraged to dynamically generate malicious code, significantly complicating detection and defense. It uses Lua scripts in combination with OpenAI's gpt-oss-20b model through the Ollama API, enabling the ransomware to adapt in ways static signature-based tools struggle to keep up with. PromptLock employs the rarely used SPECK 128-bit encryption algorithm, showcasing a future where ransomware constantly evolves.	-	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Ransomware		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Rungan	Rungan is a backdoor written in C++ that quietly establishes persistence on compromised servers. It relies on AES encryption in CBC mode to decrypt its strings, helping it evade simple detection techniques. Once active, Rungan can execute attacker-supplied commands on the victim's server, but it doesn't openly beacon; instead, it listens for incoming HTTP requests that match specific hardcoded patterns.	Through SQL injection flaws	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		System Compromise	Windows
ASSOCIATED ACTOR			**PATCH LINK**
GhostRedirector			-

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
Gamshen	Gamshen is a malicious IIS module built as a C/C++ DLL, designed to discreetly manipulate web server traffic. Its primary function is to intercept requests coming specifically from the Googlebot search engine crawler, ensuring that only these requests trigger malicious behavior. When activated, Gamshen alters the legitimate server response, dynamically pulling instructions and data from its command-and-control (C&C) server. This selective targeting allows the malware to tamper with search engine visibility while avoiding detection by regular users, making it a stealthy and strategic tool for attackers.	Through SQL injection flaws	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data Theft	Windows
Trojan			
ASSOCIATED ACTOR			**PATCH LINK**
GhostRedirector			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Quad 7 (7777)	Quad7, also known as 7777, is a botnet identified by the presence of TCP port 7777 left open on compromised devices, often showing a mysterious xlogin: banner. Its primary role is to deploy SOCKS5 proxies across infected systems, which are then abused to relay brute-force attempts against Microsoft 365 accounts worldwide. These attacks are characterized by their unusually slow pace, likely intended to evade detection while steadily targeting organizations across different sectors.	Exploiting Vulnerabilities	CVE-2023-50224 CVE-2025-9377
		IMPACT	**AFFECTED PRODUCT**
TYPE		Network Compromise	TP-Link Multiple Routers
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
Storm-0940			https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware , https://www.tp-link.com/us/support/faq/4308/

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
WEEPSTEEL	WEEPSTEEL is a malware tool built for internal reconnaissance, showing similarities to the GhostContainer backdoor in its approach. Its primary purpose is to collect detailed information about the compromised environment, including system details, network configurations, and user data. To avoid detection, the gathered information is encrypted and exfiltrated by masquerading as a harmless __VIEWSTATE response, allowing attackers to stealthily extract valuable intelligence from within targeted networks.	Exploiting Vulnerabilities	CVE-2025-53690
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft	Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud
Reconnaissance Tool			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
EARTHWORM	EARTHWORM is an open-source network tunneling tool that includes a built-in SOCKS v5 server, often abused by attackers to establish covert channels. By tunneling traffic over alternative protocols, it enables communication to and from a victim system while bypassing detection mechanisms and network filtering. This capability also allows threat actors to reach systems that would otherwise be inaccessible, making EARTHWORM a versatile tool for stealthy lateral movement and persistence within compromised environments.	Exploiting Vulnerabilities	CVE-2025-53690
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Lateral Movement, persistent access	Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud
Tunneler			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865

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
DWAGENT	DWAgent, a legitimate remote access tool, abused by attackers to establish persistent control over compromised systems and conduct Active Directory reconnaissance. To ensure redundancy and continued access, the tool was installed as a service running with SYSTEM privileges, allowing it to start automatically and provide elevated persistence.	Exploiting Vulnerability	CVE-2025-53690
		IMPACT	AFFECTED PRODUCTS
TYPE		persistent control	Sitecore Experience Manager (XM), Experience Platform (XP), and Experience Commerce (XC), Managed Cloud
Remote Access Tool			
ASSOCIATED ACTOR			PATCH LINK
-			https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SHARPHOUND	SHARPHOUND, an open-source Active Directory (AD) reconnaissance tool, was retrieved via a browser and used to map relationships within the domain. As the data collection component of the BLOODHOUND platform, SHARPHOUND gathers extensive information on AD objects, permissions, and trust relationships, providing attackers with a detailed blueprint of the environment to identify potential privilege escalation paths.	Exploiting Vulnerability	CVE-2025-53690
		IMPACT	AFFECTED PRODUCTS
TYPE		Reconnaissance	Sitecore Experience Manager (XM), Experience Platform (XP), andExperience Commerce (XC), Managed Cloud
Reconnaissance Tool			
ASSOCIATED ACTOR			PATCH LINK
-			https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865

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
Cephalus	Cephalus ransomware is known for using DLL sideloading, where a legitimate SentinelOne executable from the user's Downloads folder loads a malicious SentinelAgentCore.dll. This DLL then loads a file named data.bin, which triggers the ransomware and executes a series of commands to block system recovery.	Remote Desktop Protocol (RDP) via compromised accounts	-
		IMPACT	AFFECTED PLATFORM
TYPE		Prevention of Recovery, Information theft, Financial Loss	-
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
-			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GPUGate	GPUGate is an advanced malware that exploits users' trust by embedding malicious links within legitimate-looking GitHub commits, leading victims to download a convincing counterfeit installer. What makes GPUGate particularly dangerous is its hardware-aware design; it only activates on real devices with compatible GPUs, allowing it to avoid detection by sandboxes and most security tools.	Social Engineering, Malvertising	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Infiltration, Information theft	-
Trojan			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
Stealerium	Stealerium is an open-source information stealer built on the .NET framework. It uses 'netsh wlan' commands to gather saved Wi-Fi profiles and nearby networks, which could be used for tracking locations or moving laterally across systems. With advanced persistence methods, wide-ranging data theft capabilities, and multiple ways to exfiltrate information, Stealerium's flexibility and availability make it an increasingly dangerous threat.	Financial-Themed Phishing Emails	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information theft, Persistence	-
Infostealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Warp Stealer	Warp is a powerful malware designed to steal and exfiltrate sensitive information. Its code shows significant overlap with Stealerium, suggesting it may have borrowed elements from it. Warp Stealer can extract a wide range of data, including browser credentials, cryptocurrency wallets, Wi-Fi profiles, and VPN settings. The stolen information is then transmitted to attackers through multiple channels such as Discord, Telegram, and email.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Network Exposure	-
Infostealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Phantom Stealer	Phantom Stealer is promoted as an 'ethical hacking' tool for 'educational purposes' and is sold using a pricing model ranging from $70 to $700. It shares code similarities with Stealerium. Once installed and executed, it gathers extensive system information, including Windows version, hardware details, browser cookies, passwords, card data, images, and documents and sends the stolen data to attackers through channels like Telegram, Discord, or SMTP.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Stealthy Exfiltration	-
Infostealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MostereRAT	MostereRAT is a stealthy Remote Access Trojan that silently infiltrates systems by disguising itself with celebrity images, creating fake services, and disabling security protections to avoid detection. Built with Easy Programming Language (EPL), it uses secure, encrypted channels to deliver malicious payloads, bypass defenses, and provide attackers with full remote access.	Phishing Emails	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Security Evasion, Complete Remote Control	-
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
The Gentlemen	The Gentlemen ransomware group systematically targets infrastructure, adjusting their tools during attacks to evade endpoint defenses and security software. Their campaign involves thorough enumeration of groups and accounts, manipulation of Group Policy using elevated PowerShell and console tools, and tailored payload delivery. They maintain persistence and stealth through remote access with AnyDesk, registry changes, and encrypted data exfiltration using WinSCP.	Exploiting internet-exposed services	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Financial Loss	-
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ZynorRAT	ZynorRAT is a Go-based remote access trojan that transforms a simple Telegram bot into a powerful command-and-control platform. It offers a complete set of RAT capabilities, including remote command execution, file theft, system and process enumeration, screenshot capture, and persistence to maintain long-term access.	-	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Remote Control, Information Theft, System Surveillance	Windows, Linux
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
kkRAT	kkRAT is a remote access trojan that uses advanced anti-analysis techniques, privilege escalation, and BYOVD methods to evade detection and disable security tools. It maintains persistence through scheduled tasks, registry modifications, and startup shortcuts. Its plugin-based architecture allows attackers to remotely control systems, gather system information, proxy connections, and hijack the clipboard to steal cryptocurrency.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Evasion of Detection, Financial Theft, Remote Access	Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ValleyRAT	ValleyRAT is a remote access trojan (RAT) designed to infiltrate systems and give attackers unauthorized control. It adds new capabilities, including screenshot capture, process filtering, forced shutdown, and clearing Windows event logs to cover its tracks.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Service Disruption, Remote Access, Information Theft	Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
FatalRAT	FatalRAT is a remote access trojan (RAT) that provides attackers with persistent, full control over compromised systems. It enables keystroke logging, data theft, and remote command execution. To evade detection, attackers exploit legitimate Chinese cloud services like myqcloud CDN and Youdao Cloud Notes, using a multi-stage payload delivery to silently deploy the malware and bypass security defenses.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Persistent Access, Information Theft, Bypassing Security Defenses	Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
EvilAI	EvilAI is a deceptive malware family that impersonates legitimate AI software, using polished user interfaces, functional features, and even stolen code-signing certificates, to trick victims into installing it. After deployment it blends into the environment by mimicking common processes, registering misleading scheduled tasks, and applying multi-layered obfuscation to evade detection. Covertly it establishes encrypted channels to attacker-controlled command-and-control servers, exfiltrates browser-stored credentials and other sensitive artifacts, and prepares the host for follow-on modules, creating a stealthy staging ground that can turn a single compromised workstation into a broader data-theft incident.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data Theft	Windows
Stager			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
HybridPetya	HybridPetya is an emerging ransomware variant that fuses elements of both Petya and NotPetya while introducing modern enhancements tailored for today's environments. Once executed, it tampers with boot components, initiates a fake "CHKDSK" routine to mask its activity, and ultimately presents victims with a ransom note demanding Bitcoin in exchange for decryption. What makes HybridPetya particularly concerning is its ability to bypass Secure Boot and target systems with UEFI support, extending its reach to more modern infrastructures.	-	CVE-2024-7344
		IMPACT	**AFFECTED PRODUCT**
TYPE		Encrypt Data, Data Theft	Howyar Reloader UEFI Application
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://uefi.org/revocationlistfile , https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7344

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SnakeDisk	SnakeDisk is a USB-propagating worm attributed to Hive0154 that runs via DLL sideloading. It uses a deceptive export stub and accepts two modes: -Embedding (infects USB drives and drops the embedded payload when a device is removed) and -hope (immediately drops and executes the embedded payload), enabling both delayed USB-based spread and instant execution.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data Theft	-
USB worm			
ASSOCIATED ACTOR			**PATCH LINK**
Hive0154			-

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
Yokai	Yokai is a lightweight backdoor that establishes a reverse shell over anonymous pipes, giving operators remote command execution on the infected host. It shares architectural and tradecraft similarities with Hive0154-linked families like Pubload/Pubshell and Toneshell, similar pipe-based shell mechanics and C2 patterns, though it remains a distinct implant.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Hive0154			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Pubload	Pubload is a modular downloader that supports decoy C2 servers and can retrieve shellcode both via HTTP POST and over raw TCP streams that mimic TLS traffic, making its network activity harder to distinguish from legitimate encrypted connections.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Espionage, Exfiltration	-
Downloader			
ASSOCIATED ACTOR			**PATCH LINK**
Hive0154			-

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">Toneshell</td><td rowspan="6">Toneshell is a sophisticated backdoor that leverages DLL side-loading to execute stealthily and uses a tightly scripted command set to locate and extract files from compromised networks. The latest variant, Toneshell9, adds enterprise-evasion features: C2 traffic can be routed through locally configured proxies to blend with normal network flows, and the implant can maintain two concurrent reverse shells for parallel operator access and redundancy. These capabilities make it effective at covert data extraction and persistent remote control within large, proxy-enabled environments.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Data Theft, System Compromise</td><td>-</td></tr>
<tr><td>Backdoor</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>-</td></tr>
<tr><td>Hive0154</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">StealC</td><td rowspan="6">StealC is a versatile information-stealing implant that primarily harvests sensitive data from infected hosts. Once present, it enumerates the user environment to extract stored credentials, browser artifacts (cookies, history, autofill), data from popular gaming and chat clients, and cryptocurrency wallet files or keys, packaging this loot and exfiltrating it to attacker-controlled servers.</td><td>Phishing</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Data Theft</td><td>-</td></tr>
<tr><td>Infostealer</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>-</td></tr>
<tr><td>-</td></tr>
</table>

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
Yurei	Yurei is a Go-based ransomware first observed on September 5, 2025, that appears to be a light fork of the open-source Prince ransomware, sharing most of the same code with only minor edits, and has been seen in campaigns that overlap with activity attributed to CrazyHunter. It encrypts victim files using the ChaCha20 cipher and appends the .Yurei extension, leaving systems and data inaccessible until a ransom is paid.	-	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data Theft, Encrypt Data	-
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
BlackNevas	BlackNevas (aka Trial Recovery) is a sophisticated double-extortion ransomware variant, first identified in November 2024 and descended from the Trigona family. It combines strong file encryption with aggressive data theft, renaming encrypted files with a distinctive .-encrypted extension and dropping how_to_decrypt.txt ransom notes in every folder. Victims are pressured to negotiate via email or Telegram and threatened with public leaks, auctions, or publication of exfiltrated data if they do not pay within seven days.	Phishing, Exploiting Vulnerabilities	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data Theft, Encrypt Data	-
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
VenomRAT	VenomRAT is a commercialized remote-access trojan that evolved from the open-source QuasarRAT and has been sold on underground markets since its discovery in mid-2020 (lifetime licenses have advertised prices up to ~$650). Despite portions of its source leaking, actors continue to build and sell custom clients: each implant is generated with tailored configuration data that the malware protects using AES encryption under PKCS #5 v2.0, plus an HMAC-SHA256 authenticity check. The implant's configuration handling repeatedly applies the same AES algorithm but with different keys and initialization vectors scattered through the codebase, complicating analysis while preserving a consistent cryptographic design.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data Theft	Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
RevengeHotels			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Shai-Hulud	Shai-hulud is a supply-chain worm hidden in compromised packages that executes automatically on install via a bundled bundle.js. Once running, it leverages legitimate tooling to hunt for secrets, scans the host and developer environments for cloud and CI tokens, and validates any credentials it finds, so stolen tokens are immediately usable. The worm then abuses those credentials to propagate, injecting unauthorized GitHub Actions workflows into repositories and moving laterally across accounts, while exfiltrating harvested secrets to a hardcoded webhook. Because it targets packages from multiple maintainers and automates both secret discovery and repository-level persistence.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		System Compromise	npm ecosystem, GitHub repositories
Worm			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SilentSync	SilentSync is a Python-based remote-access trojan (RAT) that provides attackers with full control over infected systems. Its capabilities include executing arbitrary commands, exfiltrating files, capturing screens, and harvesting sensitive data from web browsers, such as passwords, cookies, browsing history, and autofill information from Chrome, Brave, Edge, and Firefox. The malware maintains contact with a command-and-control (C2) server over HTTP, using regular beaconing and task polling to receive instructions and exfiltrate collected data, making it a versatile tool for surveillance and data theft.	Social Engineering	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft	Windows, Linux, macOS
RAT			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Kazuar	Kazuar backdoor is an advanced espionage implant used by Turla in its attack chain. Kazuar Versions 2 and 3 share the same codebase. This modular malware provides persistent remote control over infected systems, making it a powerful tool.	-	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data Theft, System Compromise	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Turla, Gamaredon			-

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
PteroOdd	PteroOdd is a PowerShell downloader used by Gamaredon to retrieve payloads that executed the Kazuar backdoor.	-	-
		IMPACT	AFFECTED PRODUCT
TYPE		Downloads other malware	-
Downloader			
ASSOCIATED ACTOR			PATCH LINK
Turla, Gamaredon			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MINIBIKE	MINIBIKE is a backdoor that maintains a foothold by loading additional DLLs and keeping a persistent link to its operators; it hides key data with runtime XOR decryption, using a separate routine for each string length to frustrate static analysis and routes command-and-control traffic through Microsoft Azure to blend in with legitimate cloud activity. From an infected host, the attackers can run arbitrary commands and browse the file system remotely.	Social Engineering	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft	Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Subtle Snail			-

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
Atomic Stealer	Atomic Stealer, or AMOS, is a prevalent macOS-targeting malware designed to harvest and exfiltrate sensitive data, including account credentials, browser information, and cryptocurrency wallet details.	By abusing GitHub Pages and SEO	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft	macOS
Stealer			
ASSOCIATED ACTOR			PATCH LINK
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
BadIIS	BadIIS is a family of malicious native IIS modules that embed directly into a web server's request pipeline and inherit the server's full privileges, allowing a single implant to manipulate traffic and site behavior with powerful stealth. BadIIS can inject JavaScript or invisible iframes into pages, tunnel traffic through a built-in reverse proxy, issue 302 redirects that mislead search engine crawlers, and exfiltrate sensitive data from visitors. Attackers leverage these capabilities to perform SEO poisoning.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		System Compromise	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			-

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
DeerStealer	DeerStealer is a commercially marketed information-stealer that poses as legitimate software to trick victims into running it and then quietly harvests passwords, browser data, cryptocurrency wallets, and other sensitive information from infected machines. The malware is openly sold on dark-web forums and Telegram channels by an actor using the handle "LuciferXfiles," offered through tiered subscriptions, from a $200/month "Premium" tier up to a $3,000/month "Professional" package, making it a turnkey tool for criminal operators who want scalable, low-effort access to harvested credentials and financial data.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data Theft	-
Information stealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
BAITSWITCH	BAITSWITCH is a downloader that establishes persistence on a victim machine and reaches out to attacker-controlled servers to fetch and run a PowerShell stager that installs the SIMPLEFIX backdoor. It uses a hard-coded user-agent string as a gatekeeper, the C2 only returns commands when that exact user-agent is presented and otherwise serves a "404 Not Found" page, and performs five HTTP requests to the actor-controlled domain to retrieve different commands and payloads.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Downloads other payloads	-
Downloader			
ASSOCIATED ACTOR			**PATCH LINK**
COLDRIVER			-

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
SIMPLEFIX	SIMPLEFIX is a PowerShell-based backdoor delivered by the BAITSWITCH that uses the same layered obfuscation techniques found in the installer to hide its true logic; when those layers are stripped away the deobfuscated script reveals the backdoor's core runtime logic invoked by the stager, making SIMPLEFIX a stealthy, script-native implant that is designed to be hard to detect and straightforward for operators to control once executed.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
COLDRIVER			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
BRICKSTORM	BRICKSTORM is a Go-based backdoor attributed to a China-nexus group tracked as UNC5221 and first observed in early 2024 amid attacks exploiting Ivanti Connect Secure flaws. The implant works alongside a companion tool, BRICKSTEAL, to harvest vCenter credentials and escalate privileges, and it uses advanced evasion techniques that let intrusions persist for long periods, on average about 393 days, before detection. Operators using BRICKSTORM have also been observed cloning sensitive VMware vCenter virtual machines, notably domain controllers and password vaults, to siphon secrets and broaden their foothold, making the toolkit both opportunistic and highly targeted against high-value virtualization infrastructure.	Exploiting Vulnerabilities	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data Theft	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
UNC5221			-

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
DarkCloud	DarkCloud is a commercial information stealer that targets browser passwords, keystrokes, FTP logins, and cryptocurrency wallets. Its public storefront and feature-rich builder lower the bar for criminals. Combined with VB6-based obfuscation, sandbox/VM checks, and multiple exfiltration methods (SMTP, Telegram, FTP, web panel), it can evade detection and quietly siphon high-value data.	Spear-phishing email	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Theft of credentials, account takeover, Financial loss	Windows
Information stealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RayInitiator	RayInitiator is a stealthy bootkit that infects the device's firmware/ROM or ROMMON to insert itself into the boot chain, ensuring early execution before the OS and surviving reboots and many firmware upgrades; it decrypts and stages secondary payloads while evading simple integrity checks.	Firmware / ROM modification	CVE-2025-20333 CVE-2025-20362
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Persistent early-boot compromise	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD)
Bootkit			
ASSOCIATED ACTOR			**PATCH LINK**
UAT4356 (aka Storm-1849)			https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>Line Viper</td><td rowspan="6">Line Viper is a user-mode loader that performs in-memory/reflective loading of modules into trusted processes, using process injection, API hooking, and runtime obfuscation to fetch and run plugins for C2, credential harvesting, and lateral movement, together they provide a resilient, layered persistence and post-exploitation framework on compromised network appliances.</td><td>Reflective in-memory injection</td><td>CVE-2025-20333
CVE-2025-20362</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Loader</td><td rowspan="3">Credential theft & lateral movement</td><td>Microsoft SharePoint Server</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>UAT4356 (aka Storm-1849)</td><td>https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks</td></tr>
</table>

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
 APT37 (aka Reaper, TEMP.Reaper ,Ricochet Chollima, ScarCruft, Cerium, Group 123,Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet, TA-RedAnt, G0067)	North Korea	Academic, Government officials, and Researchers	South Korea
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	RokRAT	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1574: Hijack Execution Flow; T1574.001: DLL; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1055: Process Injection; T1055.001: Dynamic-link Library Injection; T1055.009: Proc Memory; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1140: Deobfuscate/Decode Files or Information; T1070: Indicator Removal; T1070.004: File Deletion; T1027: Obfuscated Files or Information; T1027.009: Embedded Payloads; T1027.013: Encrypted/Encoded File; T1056: Input Capture; T1056.002: GUI Input Capture; T1087: Account Discovery; T1087.001: Local Account; T1217: Browser Information Discovery; T1083: File and Directory Discovery; T1082: System Information Discovery; T1123: Audio Capture; T1005: Data from Local System; T1113: Screen Capture; T1102: Web Service; T1102.002: Bidirectional Communication; T1041: Exfiltration Over C2 Channel; T1529: System Shutdown/Reboot

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 

GhostRedirector</td><td>China</td><td rowspan="3">Education, Healthcare, Insurance, Transportation, Technology, Retail</td><td rowspan="3">Brazil, Peru, Thailand, Vietnam, United States, Canada, Finland, India, Netherlands, Philippines, Singapore</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Rungan, Gamshen</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0005: Defense Evasion; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0006: Credential Access; TA0040: Impact; TA0011: Command and Control; TA0003: Persistence; TA0004: Privilege Escalation; T1112: Modify Registry; T1027.009: Embedded Payloads; T1059.003: Windows Command Shell; T1059.001: PowerShell; T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation; T1008: Fallback Channels; T1565: Data Manipulation; T1588.002: Tool; T1588: Obtain Capabilities; T1083: File and Directory Discovery; T1219: Remote Access Software; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1587: Develop Capabilities; T1587.001: Malware; T1608.006: SEO Poisoning; T1608: Stage Capabilities; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1134: Access Token Manipulation; T1608.001: Upload Malware; T1608.002: Upload Tool; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1588.003: Code Signing Certificates; T1190: Exploit Public-Facing Application; T1106: Native API; T1559: Inter-Process Communication; T1546: Event Triggered Execution</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
Storm-0940</td><td>China</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2023-50224
CVE-2025-9377</td><td>Quad 7 (7777) Botnet</td><td>TP-Link Multiple Routers</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; TA0040: Impact; T1078: Valid Accounts; T1110: Brute Force; T1110.003: Password Spraying; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1110: Brute Force; T1087: Account Discovery; T1046: Network Service Discovery; T1090: Proxy; T1090.003: Multi-hop Proxy; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1571: Non-Standard Port; T1496: Resource Hijacking</td></tr>
</table>

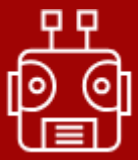
NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Hive0154 (aka Mustang Panda, Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, G0129)	China	Government, Defense	East Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	SnakeDisk, Yokai, Pubload, Toneshell	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1091: Replication Through Removable Media; T1574: Hijack Execution Flow; T1574.001: DLL; T1105: Ingress Tool Transfer; T1027: Obfuscated Files or Information; T1090: Proxy; T1071: Application Layer Protocol; T1059: Command and Scripting Interpreter; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1656: Impersonation; T1566: Phishing; T1070: Indicator Removal; T1053: Scheduled Task/Job; T1204: User Execution; T1036: Masquerading; T1140: Deobfuscate/Decode Files or Information; T1082: System Information Discovery; T1012: Query Registry

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
RevengeHotels (aka TA558)</td><td>-</td><td rowspan="2">Hotels</td><td rowspan="2">Brazil</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial crime</td><td rowspan="2">ASSOCIATED ATTACKS/RANSOM WARE</td><td rowspan="2">AFFECTED PRODUCT</td></tr>
<tr><td>TARGETED CVE</td></tr>
<tr><td>-</td><td>VenomRAT</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1059.001: PowerShell; T1027: Obfuscated Files or Information; T1059.005: Visual Basic; T1189: Drive-by Compromise; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1112: Modify Registry; T1057: Process Discovery; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1071: Application Layer Protocol; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Gamaredon (aka Primitive Bear, Winterflounder, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Shuckworm, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard)	Russia	Government, Defense, Diplomatic Entities	Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Kazuar backdoor, PteroOdd	-

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1583.007: Serverless; T1584: Compromise Infrastructure; T1584.003: Virtual Private Server; T1608: Stage Capabilities; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1574: Hijack Execution Flow; T1574.001: DLL; T1140: Deobfuscate/Decode Files or Information; T1480: Execution Guardrails; T1480.001: Environmental Keying; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1057: Process Discovery; T1012: Query Registry; T1082: System Information Discovery; T1083: File and Directory Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1102: Web Service

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
Turla (aka Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon)</td><td>Russia</td><td rowspan="3">Government, Defense, Diplomatic Entities</td><td rowspan="3">Ukraine</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>-</td><td>Kazuar backdoor, PteroOdd</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.004: Server; T1583.007: Serverless; T1584: Compromise Infrastructure; T1584.003: Virtual Private Server; T1608: Stage Capabilities; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1574: Hijack Execution Flow; T1574.001: DLL; T1140: Deobfuscate/Decode Files or Information; T1480: Execution Guardrails; T1480.001: Environmental Keying; T1036: Masquerading; T1036.005: Match Legitimate Resource Name or Location; T1057: Process Discovery; T1012: Query Registry; T1082: System Information Discovery; T1083: File and Directory Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1102: Web Service</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="3"> 
Subtle Snail (aka UNC1549, TA455, Smoke Sandstorm, Bohrium, DEV-0056, Yellow Dev 13)</td><td>Iran</td><td rowspan="3">Telecommunications, Aerospace, Defense</td><td rowspan="3">Canada, USA, UK, France, UAE</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td></td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td></td><td>-</td><td>MINIBIKE</td><td>-</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; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1589: Gather Victim Identity Information; T1591: Gather Victim Org Information; T1598: Phishing for Information; T1598.003: Spearphishing Link; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.003: Virtual Private Server; T1587: Develop Capabilities; T1587.001: Malware; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1585.002: Email Accounts; T1585.003: Cloud Accounts; T1588: Obtain Capabilities; T1588.003: Code Signing Certificates; T1566: Phishing; T1566.002: Spearphishing Link; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1016: System Network Configuration Discovery; T1070: Indicator Removal; T1574: Hijack Execution Flow; T1574.001: DLL; T1055: Process Injection; T1055.012: Process Hollowing; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1497: Virtualization/Sandbox Evasion; T1622: Debugger Evasion; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1036: Masquerading; T1036.003: Rename Legitimate Utilities; T1070.004: File Deletion; T1056: Input Capture; T1056.001: Keylogging; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1539: Steal Web Session Cookie; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1552.004: Private Keys; T1552.003: Bash History; T1555.005: Password Managers; T1087: Account Discovery; T1016: System Network Configuration Discovery; T1033: System Owner/User Discovery; T1082: System Information Discovery; T1069: Permission Groups Discovery; T1069.002: Domain Groups; T1083: File and Directory Discovery; T1057: Process Discovery; T1217: Browser Information Discovery; T1005: Data from Local System; T1119: Automated Collection; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1114: Email Collection; T1114.001: Local Email Collection; T1025: Data from Removable Media; T1039: Data from Network Shared Drive; T1115: Clipboard Data; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1020: Automated Exfiltration; T1041: Exfiltration Over C2 Channel; T1029: Scheduled Transfer</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 COLDRIVER (aka Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto, Star Blizzard, UNC4057, IRON FRONTIER, Grey Pro, Mythic Ursa, Gossamer Bear)	Russia	Civil Society	Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	BAITSWITCH, SIMPLEFIX	-

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.006: Web Services; T1585: Establish Accounts; T1585.002: Email Accounts; T1585.003: Cloud Accounts; T1587: Develop Capabilities; T1587.001: Malware; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.003: Install Digital Certificate; T1608.005: Link Target; T1204: User Execution; T1204.004: Malicious Copy and Paste; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1037: Boot or Logon Initialization Scripts; T1037.001: Logon Script (Windows); T1112: Modify Registry; T1140: Deobfuscate/Decode Files or Information; T1564: Hide Artifacts; T1564.003: Hidden Window; T1218: System Binary Proxy Execution; T1218.011: Rundll32; T1205: Traffic Signaling; T1070: Indicator Removal; T1070.003: Clear Command History; T1027: Obfuscated Files or Information; T1027.011: Fileless Storage; T1027.013: Encrypted/Encoded File; T1033: System Owner/User Discovery; T1082: System Information Discovery; T1135: Network Share Discovery; T1016: System Network Configuration Discovery; T1016.001: Internet Connection Discovery; T1087: Account Discovery; T1087.001: Local Account; T1083: File and Directory Discovery; T1049: System Network Connections Discovery; T1057: Process Discovery; T1018: Remote System Discovery; T1046: Network Service Discovery; T1124: System Time Discovery; T1005: Data from Local System; T1530: Data from Cloud Storage; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1104: Multi-Stage Channels; T1001: Data Obfuscation; T1001.003: Protocol or Service Impersonation; T1105: Ingress Tool Transfer; T1132: Data Encoding; T1132.001: Standard Encoding; T1573: Encrypted Channel; T1573.002: Asymmetric Cryptography; T1566: Phishing; T1036: Masquerading; T1059.007: JavaScript; T1041: Exfiltration Over C2 Channel

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
UNC5221 (alias UTA0178, Red Dev 61)</td><td>China</td><td rowspan="3">Legal, Software-as-a-Service (SaaS) Providers, Business Process Outsourcers (BPOs), Technology</td><td rowspan="3">United States</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>-</td><td>BRICKSTORM</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1078: Valid Accounts; T1136: Create Account; T1543: Create or Modify System Process; T1027: Obfuscated Files or Information; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1555: Credentials from Password Stores; T1673: Virtual Machine Discovery; T1564: Hide Artifacts; T1564.006: Run Virtual Instance; T1114: Email Collection; T1114.002: Remote Email Collection; T1671: Cloud Application Integration; T1003: OS Credential Dumping; T1087: Account Discovery; T1059: Command and Scripting Interpreter; T1505.003: Web Shell; T1547: Boot or Logon Autostart Execution; T1021.004: SSH; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel; T1071.004: DNS; T1567: Exfiltration Over Web Service; T1071: Application Layer Protocol</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGION</th></tr>
<tr><td rowspan="4"> 
UAT4356 (aka Storm-1849)</td><td>China</td><td rowspan="3">Government, Critical Infrastructure, Telecommunication, Energy</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-20333
CVE-2025-20362</td><td>RayInitiator bootkit, Line Viper loader</td><td>Cisco ASA and FTD</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0005: Defense Evasion; T1190: Exploit Public-Facing Application; T1543: Create or Modify System Process; T1068; TA0002: Execution; TA0040: Impact; T1078: Valid Accounts; T1562; TA0003: Persistence; TA0004: Privilege Escalation; TA0042: Resource Development; T1529: System Shutdown/Reboot; T1542.001: System Firmware; T1070: Impair Defenses; T1068: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter; T1588.006: Vulnerabilities; T1588.005: Exploits; T1542: Pre-OS Boot; T1542.003: Bootkit; T1588: Obtain Capabilities</td></tr>
</table>

MITRE ATT&CK TTPS

Tactic	Technique	Sub-technique
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	
	T1591: Gather Victim Org Information	
	T1598: Phishing for Information	
		T1598.002: Spearphishing Attachment
		T1598.003: Spearphishing Link
		T1590.002: DNS
TA0042: Resource Development	T1583: Acquire Infrastructure	
		T1583.001: Domains
		T1583.004: Server
		T1583.006: Web Services
		T1583.007 : Serverless
	T1584: Compromise Infrastructure	
		T1584.001: Domains
		T1584.003: Virtual Private Server
	T1585: Establish Accounts	
		T1585.002: Email Accounts
	T1586: Compromise Accounts	
		T1586.001: Social Media Accounts
		T1586.002: Email Accounts
	T1587: Develop Capabilities	
		T1587.001: Malware
	T1588: Obtain Capabilities	
		T1588.002: Tool
		T1588.003: Code Signing Certificates
		T1588.005: Exploits
		T1588.006: Vulnerabilities
	T1608: Stage Capabilities	
		T1608.001: Upload Malware
		T1608.002: Upload Tool
		T1608.003: Install Digital Certificate
		T1608.005: Link Target
		T1608.006: SEO Poisoning
TA0001: Initial Access	T1078: Valid Accounts	
		T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1091: Replication Through Removable Media	
	T1133: External Remote Services	
	T1189: Drive-by Compromise	
	T1190: Exploit Public-Facing Application	

Tactic	Technique	Sub-technique
TA0001: Initial Access	T1195: Supply Chain Compromise	
		T1195.001: Compromise Software Dependencies and Development Tools
		T1195.002: Compromise Software Supply Chain
	T1566: Phishing	
		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
		T1059.007: JavaScript
	T1072: Software Deployment Tools	
	T1106: Native API	
	T1203: Exploitation for Client Execution	
	T1204: User Execution	
		T1204.001: Malicious Link
		T1204.002: Malicious File
	T1559: Inter-Process Communication	
	T1569: System Services	
		T1569.002: Service Execution
TA0003: Persistence	T1037: Boot or Logon Initialization Scripts	
		T1037.001: Logon Script (Windows)
	T1053: Scheduled Task/Job	
		T1053.005: Scheduled Task
	T1078: Valid Accounts	
		T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	
	T1133: External Remote Services	
	T1136: Create Account	
	T1205: Traffic Signaling	
	T1505: Server Software Component	
		T1505.003: Web Shell
		T1505.004: IIS Components
	T1542: Pre-OS Boot	
		T1542.001: System Firmware
		T1542.003: Bootkit

Tactic	Technique	Sub-technique
TA0003: Persistence	T1543: Create or Modify System Process	
		T1543.002: Systemd Service
		T1543.003: Windows Service
	T1546: Event Triggered Execution	
	T1547: Boot or Logon Autostart Execution	
		T1547.001: Registry Run Keys / Startup Folder
		T1547.009: Shortcut Modification
	T1574: Hijack Execution Flow	
		T1574.002: DLL Side-Loading
TA0004: Privilege Escalation	T1037: Boot or Logon Initialization Scripts	
		T1037.001: Logon Script (Windows)
	T1053: Scheduled Task/Job	
		T1053.005: Scheduled Task
	T1055: Process Injection	
		T1055.001: Dynamic-link Library Injection
		T1055.009: Proc Memory
		T1055.012: Process Hollowing
	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	
		T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1098: Account Manipulation	
	T1134: Access Token Manipulation	
	T1484: Domain or Tenant Policy Modification	
		T1484.001: Group Policy Modification
	T1543: Create or Modify System Process	
		T1543.002: Systemd Service
		T1543.003: Windows Service
	T1546: Event Triggered Execution	
	T1547: Boot or Logon Autostart Execution	
		T1547.001: Registry Run Keys / Startup Folder
		T1547.009: Shortcut Modification
	T1548: Abuse Elevation Control Mechanism	
		T1548.002: Bypass User Account Control
	T1574: Hijack Execution Flow	
		T1574.002: DLL Side-Loading

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1014: Rootkit	
	T1027: Obfuscated Files or Information	
		T1027.002: Software Packing
		T1027.003: Steganography
		T1027.007: Dynamic API Resolution
		T1027.009: Embedded Payloads
		T1027.011: Fileless Storage
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	
		T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
	T1055: Process Injection	
		T1055.001: Dynamic-link Library Injection
		T1055.009: Proc Memory
		T1055.012: Process Hollowing
	T1070: Indicator Removal	
		T1070.001: Clear Windows Event Logs
		T1070.003: Clear Command History
		T1070.004: File Deletion
	T1078: Valid Accounts	
		T1078.002: Domain Accounts
		T1078.004: Cloud Accounts
	T1112: Modify Registry	
	T1134: Access Token Manipulation	
	T1140: Deobfuscate/Decode Files or Information	
	T1205: Traffic Signaling	
	T1218: System Binary Proxy Execution	
		T1218.005: Mshta
		T1218.011: Rundll32
	T1480: Execution Guardrails	
		T1480.001: Environmental Keying
	T1484: Domain or Tenant Policy Modification	
		T1484.001: Group Policy Modification
	T1497: Virtualization/Sandbox Evasion	
	T1542: Pre-OS Boot	
		T1542.001: System Firmware
		T1542.003: Bootkit
	T1548: Abuse Elevation Control Mechanism	
		T1548.002: Bypass User Account Control
	T1550: Use Alternate Authentication Material	
		T1550.001: Application Access Token

Tactic	Technique	Sub-technique
TA0005: Defense Evasion	T1562: Impair Defenses	
		T1562.001: Disable or Modify Tools
		T1562.002: Disable Windows Event Logging
		T1562.007: Disable or Modify Cloud Firewall
	T1564: Hide Artifacts	
		T1564.001: Hidden Files and Directories
		T1564.003: Hidden Window
		T1564.006: Run Virtual Instance
	T1574: Hijack Execution Flow	
		T1574.002: DLL Side-Loading
	T1620: Reflective Code Loading	
	T1622: Debugger Evasion	
	T1656: Impersonation	
TA0006: Credential Access	T1003: OS Credential Dumping	
		T1003.001: LSASS Memory
	T1056: Input Capture	
		T1056.001: Keylogging
		T1056.002: GUI Input Capture
		T1056.003: Web Portal Capture
	T1110: Brute Force	
		T1110.003: Password Spraying
	T1528: Steal Application Access Token	
	T1539: Steal Web Session Cookie	
	T1552: Unsecured Credentials	
		T1552.001: Credentials In Files
		T1552.003: Bash History
		T1552.004: Private Keys
		T1552.007: Container API
	T1555: Credentials from Password Stores	
		T1555.003: Credentials from Web Browsers
		T1555.005: Password Managers
	T1606: Forge Web Credentials	
		T1606.001: Web Cookies
TA0007: Discovery	T1010: Application Window Discovery	
	T1012: Query Registry	
	T1016: System Network Configuration Discovery	
		T1016.001: Internet Connection Discovery
	T1018: Remote System Discovery	
	T1033: System Owner/User Discovery	
	T1046: Network Service Discovery	
	T1049: System Network Connections Discovery	

Tactic	Technique	Sub-technique
TA0007: Discovery	T1057: Process Discovery	
	T1069: Permission Groups Discovery	
		T1069.002: Domain Groups
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1087: Account Discovery	
		T1087.001: Local Account
		T1087.002: Domain Account
	T1124: System Time Discovery	
	T1135: Network Share Discovery	
	T1217: Browser Information Discovery	
	T1482: Domain Trust Discovery	
	T1497: Virtualization/Sandbox Evasion	
	T1518: Software Discovery	
		T1518.001: Security Software Discovery
	T1622: Debugger Evasion	
TA0008: Lateral Movement	T1021: Remote Services	
		T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
		T1021.004: SSH
	T1072: Software Deployment Tools	
	T1091: Replication Through Removable Media	
	T1210: Exploitation of Remote Services	
	T1534: Internal Spearphishing	
	T1550: Use Alternate Authentication Material	
		T1550.001: Application Access Token
TA0009: Collection	T1005: Data from Local System	
	T1025: Data from Removable Media	
	T1039: Data from Network Shared Drive	
	T1056: Input Capture	
		T1056.001: Keylogging
		T1056.002: GUI Input Capture
		T1056.003: Web Portal Capture
	T1074: Data Staged	
		T1074.001: Local Data Staging
	T1113: Screen Capture	
	T1114: Email Collection	
		T1114.001: Local Email Collection
		T1114.002: Remote Email Collection
	T1115: Clipboard Data	
	T1119: Automated Collection	
	T1123: Audio Capture	
	T1213: Data from Information Repositories	
	T1560: Archive Collected Data	
		T1560.001: Archive via Utility

Tactic	Technique	Sub-technique
TA0010: Exfiltration	T1020: Automated Exfiltration	
	T1029: Scheduled Transfer	
	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	
		T1048.001: Exfiltration Over Symmetric Encrypted Non-C2 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	
		T1090.003: Multi-hop Proxy
	T1102: Web Service	
		T1102.001: Dead Drop Resolver
		T1102.002: Bidirectional Communication
	T1104: Multi-Stage Channels	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	
		T1132.001: Standard Encoding
	T1205: Traffic Signaling	
	T1219: Remote Access Software	
	T1571: Non-Standard Port	
	T1573: Encrypted Channel	
		T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
TA0040: Impact	T1485: Data Destruction	
	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1491: Defacement	
		T1491.001: Internal Defacement
	T1496: Resource Hijacking	
	T1498: Network Denial of Service	
	T1499: Endpoint Denial of Service	
	T1529: System Shutdown/Reboot	
	T1561: Disk Wipe	
		T1561.001: Disk Content Wipe
	T1565: Data Manipulation	

Top 5 Takeaways

#1

In **September 2025**, **eight zero-day** vulnerabilities were identified in technologies associated with vendors such as **Citrix, Fortinet, Apple, Sitecore, Google Chrome,** and **Cisco**. Of the **14 exploitable**, **seven** were actively exploited by threat actors across multiple attack campaigns, demonstrating the growing sophistication of cyber adversaries.

#2

Several new malicious malware were detected in **September 2025,** including **NightSpire, PromptLock, Cephalus, The Gentlemen, HybridPetya, Yurei,** and **BlackNevas.** These fresh entries expand the ransomware and malware landscape, bringing diverse techniques and operational approaches that warrant close attention.

#3

Notably, **RokRAT, Warp Stealer, ValleyRAT, FatalRAT, VenomRAT, Atomic Stealer,** and **DarkCloud** staged significant rebounds this month, surfacing with upgraded variants. Enhanced capabilities in persistence, stealth, and evasion highlight the ongoing evolution of established threats in response to defensive improvements.

#4

In September 2025, cyber threat activity predominantly focused on the **United States, Japan, South Korea, Singapore,** and **Thailand**. These nations experienced heightened malicious campaigns spanning ransomware, botnets, and custom malware deployments.

#5

Key sectors under fire included **Technology, Healthcare, Legal, Education,** and **Manufacturing**. Attackers concentrated their efforts on disrupting essential services, accessing sensitive financial and medical data, and targeting crypto-related assets.

Recommendations

Security Teams

This digest can be used as a guide to help security teams prioritize the **14 significant vulnerabilities** and block the indicators related to the **11 active threat actors, 45 active malware,** and **229 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 **14 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
RokRAT	SHA256	3fa06c290c477c133ca58512c7852fc998632721f2dc3a0984f18fbe86451e18, 81fb0b9310ec3a4afb7fc107281d5c13f87fcf2b5cd151dd273f8f910a2cffc3, 8de48bd7eca096eb10a5023d245e5cb83e2fce7efdfde91cb86f89623b001535
NightSpire	SHA256	32e10dc9fe935d7c835530be214142041b6aa25ee32c62648dea124401137ea5
PromptLock	SHA256	2755e1ec1e4c3c0cd94ebe43bd66391f05282b6020b2177ee3b939fdd33216f6, 1612ab799df51a7f1169d3f47ea129356b42c8ad81286d05b0256f80c17d4089, b43e7d481c4fdc9217e17908f3a4efa351a1dab867ca902883205fe7d1aab5e7, 09bf891b7b35b2081d3ebca8de715da07a70151227ab55aec1da26eb769c006f, e24fe0dd0bf8d3943d9c4282f172746af6b0787539b371e6626bdb86605ccd70, 1458b6dc98a878f237bfb3c3f354ea6e12d76e340cefe55d6a1c9c7eb64c9aee
Rungan	SHA1	28140A5A29EBA098BC6215DDAC8E56EACBB29B69
Gamshen	SHA1	08AB5CC8618FA593D2DF91900067DB464DC72B3E, 871A4DF66A8BAC3E640B2D1C0AFC075BB3761954
	Domain	gobr.868id[.]com, brproxy.868id[.]com
Quad 7	SHA256	f8a78c33d4f37fd5b367f84536a738bc91d50a76a58d1b595c878f4c4d7f4dd1
WEEPSTEEL	SHA256	a566cceaf9a66332470a978a234a8a8e2bbdd4d6aa43c2c75c25a80b3b744307
	MD5	117305c6c8222162d7246f842c4bb014
EARTHWORM	IPv4:Port	130[.]33[.]156[.]194[:]443, 103[.]235[.]46[.]102[:]80
	SHA256	b3f83721f24f7ee5eb19f24747b7668ff96da7dfd9be947e6e24a688ecc0a52b
	MD5	a39696e95a34a017be1435db7ff139d5

Attack Name	TYPE	VALUE
SHARPHOUND	MD5	63d22ae0568b760b5e3aabb915313e44
	SHA256	61f897ed69646e0509f6802fb2d7c5e88c3e3b93c4ca86942e24d203aa878863
Cephalus	SHA256	b3e53168fc05aeedea828bd2042e2cc34bbf8193deadab9dd4aa507e5b9c045a, a34acd47127196ab867d572c2c6cf2fcccffa3a7a87e82d338a8efed898ca722, 91c459804dbf8739e2acbc6f13d8d324bceeed3f9a004f78d5475c717b04c8b5, cd28d8cc58d17521f68f04ce33ec23a3ccce95a6a4a94e8dd19697fb0bbf04b4
	Email	sadklajsdioqw[@]proton[.]me
	Tox ID	91C24CC1586713CA6060047297516AF534FE57EFA8C3EA2031B7DF8D116AC751B156869CB8838
	TOR Address	cephalus6oiypuwumqlwurvbmwsfglg424zjdmywfgqm4iehkqivsjyd[.]onion
GPUGate	SHA256	e4d63c9aefed1b16830fdfce831f27b8e5b904c58b9172496125ba9920c7405b, 3746217c25d96bb7efe790fa78a73c6a61d4a99a8e51ae4c613efbb5be18c7b4, ad07ffab86a42b4befaf7858318480a556a2e7c272604c3f1dcae0782339482e
Stealerium	SHA256	a00fda931ab1a591a73d1a24c1b270aee0f31d6e415dfa9ae2d0f126326df4bb
Warp Stealer	SHA256	65c886b3e4da2a71c6d381c64c2391c7b4bd780353960ceca13735eec93a3118
Phantom Stealer	URL	hxxps[:]//phantomsoftwares[.]site/home/
MostereRAT	SHA256	4e3cdeba19e5749aa88329bc3ac67acd777ea7925ba0825a421cada083706a4e
The Gentlemen	SHA1	c12c4d58541cc4f75ae19b65295a52c559570054
ZynorRAT	SHA256	037e5fe028a60604523b840794d06c8f70a9c523a832a97ecaaccd9f419e364a, 47338da15a35c49bcd3989125df5b082eef64ba646bb7a2db1565bb413b69323, c890c6e6b7cc6984cd9d9061d285d814841e0b8136286e6fd943013260eb8461, 237a40e522f2f1e6c71415997766b4b23f1526e2f141d68ff334de3ff5b0c89f,

Attack Name	TYPE	VALUE
ZynorRAT	SHA256	48c2a8453feea72f8d9bfb9c2731d811e7c300f3e1935bddd7188324aab7d30d, 4cd270b49c8d5c31560ef94dc0bee2c7927d6f3e77173f660e2f3106ae7131c3, a6c450f9abff8a22445ba539c21b24508dd326522df525977e14ec17e11f7d65, bceccc566fe3ae3675f7e20100f979eaf2053d9a4f3a3619a550a496a4268ef5, 8b09ba6e006718371486b3655588b438ade953beecf221af38160cbe6fedd40a, f9eb2a54e500b3ce42950fb75af30955180360c978c00d081ea561c86e54262d
kkRAT	SHA256	f557a90c1873eeb7f269ae802432f72cc18d5272e13f86784fdc3c38cbaca019
	IPv4:Port	154[.]44[.]30[.]27[:]8250
ValleyRAT	IPv4:Port	156[.]238[.]238[.]111[:]8111
FatalRAT	IPv4:Port	103[.]199[.]101[.]3[:]8081
EvilAI	SHA256	8ecd3c8c126be7128bf654456d171284f03e4f212c27e1b33f875b8907a7bc65
HybridPetya ransomware	Filenames	bootmgfw.efi, core.dll, f20000.mbam _update.exe, improved_not petyanew.exe, notpetya _new.exe, notpetyanew.exe, notpetyanew_improved_final.exe, bootmgfw.efi, cloak.dat
	SHA1	BD35908D5A5E9F7E41A61B7AB598AB9A88DB723D, 9DF922D00171AA3C31B75446D700EE567F8D787B, 9B0EE05FFFDA0B16CF9DAAC587CB92BB06D3981B, CDC8CB3D211589202B49A48618B0D90C4D8F86FD, D31F86BA572904192D7476CA376686E76E103D28, A6EBFA062270A321241439E8DF72664CD54EA1BC, C8E3F1BF0B67C83D2A6D9E594DE8067F0378E6C5, C7C270F9D3AE80EC5E8926A3CD1FB5C9D208F1DC, 3393A8C258239D6802553FD1CCE397E18FA285A1, 98C3E659A903E74D2EE398464D3A5109E92BD9A9, D0BD283133A80B47137562F2AAAB740FA15E6441
SnakeDisk	SHA256	dd694aaf44731da313e4594d6ca34a6b8e0fcce505e39f8273b9242fdf6220e0

Attack Name	TYPE	VALUE
Yokai	SHA256	35bec1d8699d29c27b66e5646e58d25ce85ea1e41481d048bcea89ea94f8fb4b
	URL	hxxp[:]//118[.]174[.]183[.]89/kptinfo/import/index[.]php
Pubload	IPv4	188[.]208[.]141[.]196
Toneshell	SHA256	bdbc936ddc9234385317c4ee83bda087e389235c4a182736fc597565042f7644, f0fec3b271b83e23ed7965198f3b00eece45bd836bf10c038e9910675bafefb1, e7b29611c789a6225aebbc9fee3710a57b51537693cb2ec16e2177c22392b546, 9ca5b2cbc3677a5967c448d9d21eb56956898ccd08c06b372c6471fb68d37d7d, 318a1ebc0692d1d012d20d306d6634b196cc387b1f4bc38f97dd437f117c7e20
	IPv4	146[.]70[.]29[.]229, 123[.]253[.]34[.]44
	Domain	www[.]slickvpn[.]com
StealC	SHA256	70ae293eb1c023d40a8a48d6109a1bf792e1877a72433bcc89613461cffc7b61
Yurei Ransomware	TOR Address	fewcriet5rhoy66k6c4cyvb2pqrblxtx4mekj3s5l4jjt4t4kn4vheyd[.]onion
	SHA256	49c720758b8a87e42829ffb38a0d7fe2a8c36dc3007abfabbea76155185d2902, 4f88d3977a24fb160fc3ba69821287a197ae9b04493d705dc2fe939442ba6461, 1ea37e077e6b2463b8440065d5110377e2b4b4283ce9849ac5efad6d664a8e9e, 10700ee5caad40e74809921e11b7e3f2330521266c822ca4d21e14b22ef08e1d, 89a54d3a38d2364784368a40ab228403f1f1c1926892fe8355aa29d00eb36819, f5e122b60390bdcc1a17a24cce0cbca68475ad5abee6b211b5be2dea966c2634, 0303f89829763e734b1f9d4f46671e59bfaa1be5d8ec84d35a203efbfcb9bb15, 53397d36cab0a32695a50d179f289fa61fc946591bd97355ee98d350f7652079, 84d68ba901462bb0918a852a01df885f986661954c14d9c4e8e40338df2a1cb8, 754865527bc33305d8dc89a88ffada71fa0180fe778e2106d5faa8e7a8801220

Attack Name	TYPE	VALUE
BlackNevas ransomware	TOR Address	Hxxp[://]ctyfftrjgtwdjzlgqh4avbd35sqrs6tde4oyam2ufbjch6oqpqtkdtid[.]onion
	Email	amsomar[@]consultant[.]com, avalonsupp[@]consultant[.]com, biosannetsuabvg[@]mail[.]com, black4over[@]newlookst[.]com, compsupp[@]techie[.]com, corubete[@]dr[.]com, milford[@]usa[.]com, murrock[@]consultant[.]com, ovtaitonine[@]usa[.]com, suppcarter[@]uymail[.]com, toxicavalon[@]toke[.]com, varentsujikyuke[@]mail[.]com, widemoucerpco[@]mail[.]com, paymeuk[@]consultant[.]com, Serina5Murrock[@]email[.]com
	SHA1	203f81cbe35c64071f52f34afbbbfc7d61b3e702, 2a79c999e20c5d8102e0b728733cc8eba2b4d8ac, 3226ebfc23dbe1a6cc44c3255d1a0e12f0dd153c, 3ff7aedacf36f96fef42391aaadb2c63820bef7f, 49551cb0bbc2da3f6d36523a005af5ee1f5ad1a8, 499cd23b37a00b9a8ad212f879501705baad1781, 4d5605008bd0619a5980c4633889d7c253093360, 4db3b2876ef5c8e5ea977d8ffedef428b93408a4, 61c56c25f5ca4bee336aa30e89123eb2daf5166a, 646533556a16a9d17bd7ad2265873bc8f1ccb4f4, 67750b2b0b90572ade6ef760bcded1ef5fc09982, 781a8e52c2399c07ca4853def924d79be5182b32, 7b3cbd60020c1d155b12271881d69c968fcde04f, 7bf79cc58fb8f3d0ec774cb8b9e8ce311cbc27d2, 7c4f10d85607e65386fb504446b45419901c5276, 812d65b67ce28905f5e07ac1f82b827ebd36470a, 88aee839de69ce1602ef2bb401a6cabb6b376e19, 8cbbcbe187ff66c44908a205236d4230931f7d73, 923be026c79e7b5b5d29461420887fe2e8875b01, 92b0ce569d838cd9b773cc13b6b6ea5609e85fd7, B00897AE5B116680CCDD2E43A3A9599D8C3E166E, b8c85fa5a81b3d70a21835fbea394e0611461bf8, c1c9008b4be855583df0f04204443262a3fbc8ab, cd2f25a8ab74bdc17d7c8170f2c4135537ece3c4, cdb07718787743ceb488b5bd184d9a4939c12dbf, d026954e6f646b84943f8514be606650be8c18bb, dc6d4f0a88ea0458926ff8f57dbd8239ed140824, ebf63e7a27c91f96d84b66d7ba435ddc3a153b71, 2d8e9ea39b9853d5676957a51f09f14d3703d1bd,

Attack Name	TYPE	VALUE
BlackNevas ransomware	SHA1	d6e1a47a0cf9bc94a816149f6e1f1a04c53f99d1, 1b14a60d50622a7c846f9e81d9668b4962fc356b, 70e9b61e0a8e708e8512c54f96b90b32bac38984, a35b2be3167b72c73b2f8f9ac058576cf080f752, 1c0620a81f8cfb3c2a8b073b7e5a5c2329b511a5, f7d2d8fd75a62a9ce4533196b13f9ba55e985b62, 3b8185e491bbfe4ba0583f3a5810674aeaff26ad, 1ad51a365293269da14fd6914c3014fb3556f69f, a61aaf88253bfb4bd80e0ca7bbaf4a78e6bb2591, 67a078a7d703308e3c0eb2af7ea0c288453cd705, 80ad69638820c264552e5f73ed696f88614fa3bd, cbe2b0cfa599fe7477ebbe92feaadb54b5b25deb, ad63f0652ce21b0dac5284158cf301410f57d0f9, f7ac2604e6e186a647318544c36ba5758cdcb85a, 97fa0c24f75164940717672f22643ba31161c638, f18b501eca2a7390705967a24f67b808b43d2212, 8dfd14d230d93ff6eea3dd09934ebf9c9e860a0f, 93ba61e1b7d12277e0bcee27ec7f37a74d8f1c97, 119388459d68d2781b843e1db71be8f5e01e965a, 0a33ed85842cf189f96ae9ea804a2e0789200430, 3bcf26bb616c57330da226f5db4e89bb609147e8, 827c01503a92b1e202939ae5a0e3e4d5ff02f4ae, 2e2046d5e8fb4ccc18f7fdf1a4dd076bf2333417, 18af0b641e456ed5df3908f2e2fc16ea01fef0f2, 1881f7bd1867e7d625e2ef2f0dc856437a376112, 1b87e342d2fdd5cf5db3a8280bac92f90f099516, 6b22150c7eeafd74dca41b749bf33f391401d094, a7da9e83c69a9deb6aa4de1fb0ec7d0badb4a426, 67c0338c0a58493befc6c77c9f7fb16d753eb155, 0b02e7c36714e9af519fd24bca893172afd2562d, aa10da9d601482262b87cb1e0748acca7a91c2a5
	MD5	2374998cffb71f3714da2075461a884b, 4a1864a95643b0211fa7ad81b676fe2e, 9f877949b8cbbb3adfe07fd4411b9f26, f2547a80dd64dcd5cba164fe4558c2b6
	SHA256	23642a78addcffd124db133a2dd2fcd2d1bdb060dd1e41da33cb18eec7a88867, 2b9fe8a2629727470be1c928f7c9be7e2ea6cc22fb12f971902bf9cea8b16afb, 360758c296310ba428d0d52c90e31c05fc43d5889282fa840283cf468f2378e8, 3d09e930305cb3aa4ca54a39b0e3749f083d432f202606c8adac8455014b47fc, 43f145fccec00f1e100ec3377eaf0ab60df3b9c5291b8011e05141cc04704be1,

Attack Name	TYPE	VALUE
BlackNevas ransomware	SHA256	49fcbd606ff10d4661e222b8910ab7829d1668e3c97f1bab7eb51e8ec7d799a5, 501821a19ccf59830789849beff94238736adb4b213870a511890c5c8efab2a6, 623f3e98908962669e48edd414dbb67e9d4e204f677998fdcc9c2d790816a67f, 713392f009bc133f24b3271379a4ac147e1a7782b6a1ac957c1fda69d676b550, 840b1c580bfd15ca3eb1cc94cf479f63b93285d2599bc2e3cd361e3f5a340f19, 8a2d6d27ffcc66400a640d3c9c9e6becb90c04c5bab452cac56f999c48a04d63, 910cc03d64bf09f53cdf3b83068cc46368c23a061c2e1ed5df0e3a35d6c9e084, 95e744ddcc2e8f89f6c6e25503eff2eb5e70e98f6989bb4a4e93f17b09448e78, 9d9c146910f294b3e2a755f76e8066cd2edfac057ff54f00f405e2f9e8b9e51a, a0630e2a81775e8334ea9f8cac73cebf1b9a70507ea3347c0c2eba82c80219a6, a331504acf589be5d11202232a7a93eeb4fe6b053beea231d9a0a661bcaf3fd6, b0dfaf509de38749c49afcb3cd34d27126044bb77cc16896b02ebced6f95db02, b2353fce403b079735a606294c4ffc20a71f1c6b16ec15e94f554beafcddd1ea, bad3c2f72ef2be522a554a9615dc93027416a3d4048f77519fca5104fabba1f9, bf4adad2eb1163369c133ae61c181a3f91ef8640a457e9c4e72d77a60fbfa7ab, c08a752138a6f0b332dfec981f20ec414ad367b7384389e0c59466b8e10655ec, c0fc61631a20c373ce17e939e09cfb4f5179c9e0788e80079b4ee8986afe89bd, d953bce4d87f5837ce318481e3a1b6617cf64af976043d3b4b4866475bb31972, def75a41435dc28430097a7e116b2d17526ce2b0172995618f2749b0d732f7ea, E7706a633f24679c7550a31b96088dda8f772c98f64daee7cfbf0dc17a4a8338, eb8cbc4a0eae33bfdc4ecb99d033c81224b005e55588ceb86346f2b2d3fd790f, F25f76a85ded0d4d285d9ae5482d8fe07dade3e241853d00b17642d7873733e8

Attack Name	TYPE	VALUE
VenomRAT	SHA256	a5d1e69076fd9f52d8a804202a21852fe2b76fb4534f48455def652e84cceaab
Shai-Hulud	SHA256	46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09, b74caeaa75e077c99f7d44f46daaf9796a3be43ecf24f2a1fd381844669da777, dc67467a39b70d1cd4c1f7f7a459b35058163592f4a9e8fb4dffcbba98ef210c, 4b2399646573bb737c4969563303d8ee2e9ddbd1b271f1ca9e35ea78062538db, de0e25a3e6c1e1e5998b306b7141b3dc4c0088da9d7bb47c1c00c91e6e4f85d6, 81d2a004a1bca6ef87a1caf7d0e0b355ad1764238e40ff6d1b1cb77ad4f595c3, 83a650ce44b2a9854802a7fb4c202877815274c129af49e6c2d1d5d5d55c501e
SilentSync	MD5	3918cace55342909c8309ec37d0207fd
	SHA256	bbe8f3e78ca09b8deb0d476d45bedc2aa1401916e5de20819d9e745e2b7d3ab0
Kazuar	SHA256	3ecb09e659bcb500f9f40d022579a09acb11aec3a92c03e7d3fd2e56982d9eea
	SHA1	da7d5b9ab578ef6487473180b975a4b2701fda9e, d7df1325f66e029f4b77e211a238aa060d7217ed, a7acee41d66b537d900403f0e6a26ab6a1290a32, 54f2245e0d3adec566e4d822274623bf835e170c, 371ab9eb2a3da44099b2b7716de0916600450cfd, 4a58365eb8f928ec3cd62ff59e59645c2d8c0ba5, 214dc22fa25314f9c0dda54f669ede72000c85a4
PteroOdd	SHA1	7db790f75829d3e6207d8ec1cbcd3c133f596d67, 2610a899fe73b8f018d19b50be55d66a6c78b2af, 3a24520566bbe2e262a2911e38fd8130469ba830
MINIBIKE	MD5	b40533e67e70b7ff7bb53d34a4b9170e, 67e09818d1aa650896a432b1de54d376
	SHA256	0e4ff052250ade1edaab87de194e87a9afeff903695799bcbc3571918b131100

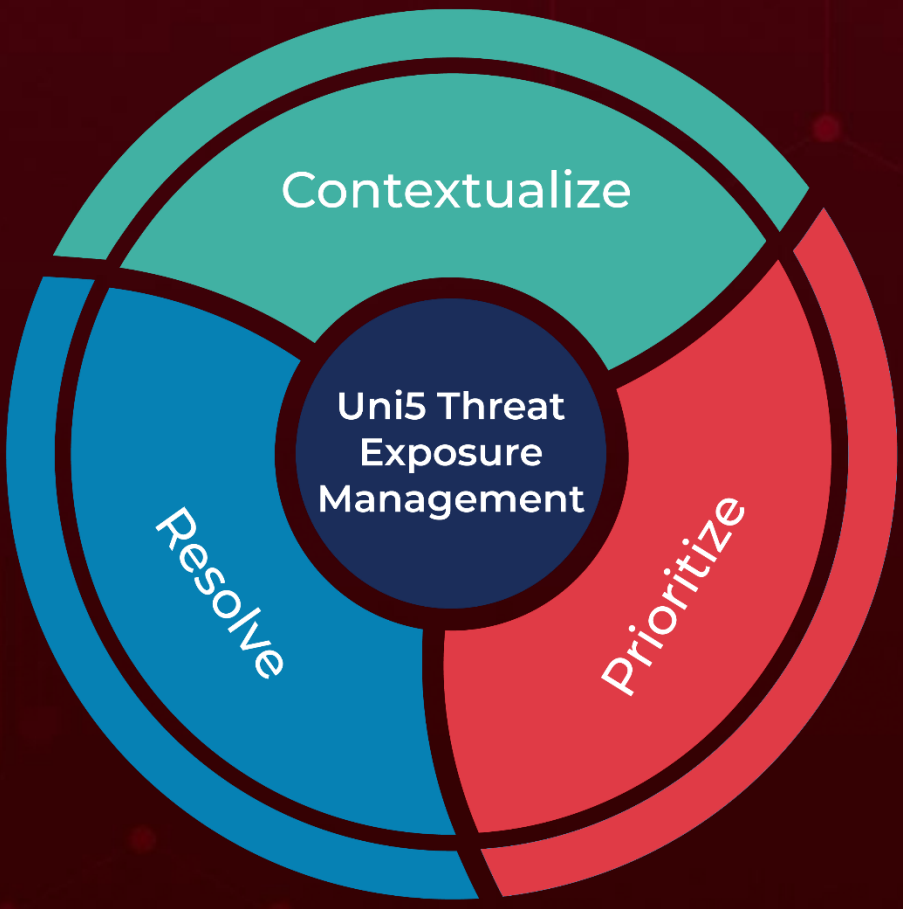
Attack Name	TYPE	VALUE
Atomic Stealer	SHA256	e52dd70113d1c6eb9a09eafa0a7e7bcf1da816849f47ebcdc66ec9671eb9b350
BadIIS	SHA256	01a616e25f1ac661a7a9c244fd31736188ceb5fce8c1a5738e807fdbef70fd60
DeerStealer	SHA256	b57c56e5f0d15eea013c39b5c169f3308ca3e8ffd0cf5b1ef001dba894beeef0, 24475ae7781189075f64a2de1a7d1fd69b341b7adee67f0bd2286cfbf1f0b7f9, eb17f8296482b0c096a2249844a62988b6abdd8ffe8cbbe3398f422968d46875, e34d753f2b992cf74c1b9db61bad4d6c6089ab8ef9fb942c865290b2dd64b4ad, 9163f9237ad869a74715f9b126f7c577bd1f12afb8eae37ba07c11f00a39fa3e, 4640d425d8d43a95e903d759183993a87bafcb9816850efe57ccfca4ace889ec, 569ac32f692253b8ab7f411fec83f31ed1f7be40ac5c4027f41a58073fef8d7d, 66282239297c60bad7eeae274e8a2916ce95afeb932d3be64bb615ea2be1e07a, a6f6175998e96fcecad5f9b3746db5ced144ae97c017ad98b2caa9d0be8a3cb5, b5ab21ddb7cb5bfbedee68296a3d98f687e9acd8ebcc4539f7fd234197de2227, d9db8cdef549e4ad0e33754d589a4c299e7082c3a0b5efdee1a0218a0a1bf1ee, e24c311a64f57fd16ffc98f339d5d537c16851dc54d7bb3db8778c26ccb5f2d1
BAITSWITCH	SHA256	87138f63974a8ccbbf5840c31165f1a4bf92a954bacccfbf1e7e5525d750aa48
SIMPLEFIX	SHA256	16a79e36d9b371d1557310cb28d412207827db2759d795f4d8e27d5f5afaf63f
BRICKSTORM	SHA256	90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035, 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df, aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878
DarkCloud	SHA256	e013fb82188cb7ea231183197e12c189b4637e7d92e277793d607405e16da1e2, 6a3b4e62a8262a0bf527ad8ea27eb19a0fcb48a76d6fc2868785362e40491432

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

October 1, 2025 . 10:30 AM

More at www.hivepro.com