

Date of Publication
September 22, 2026



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities, and Actors

14 to 20 SEPTEMBER 2026

Table Of Contents

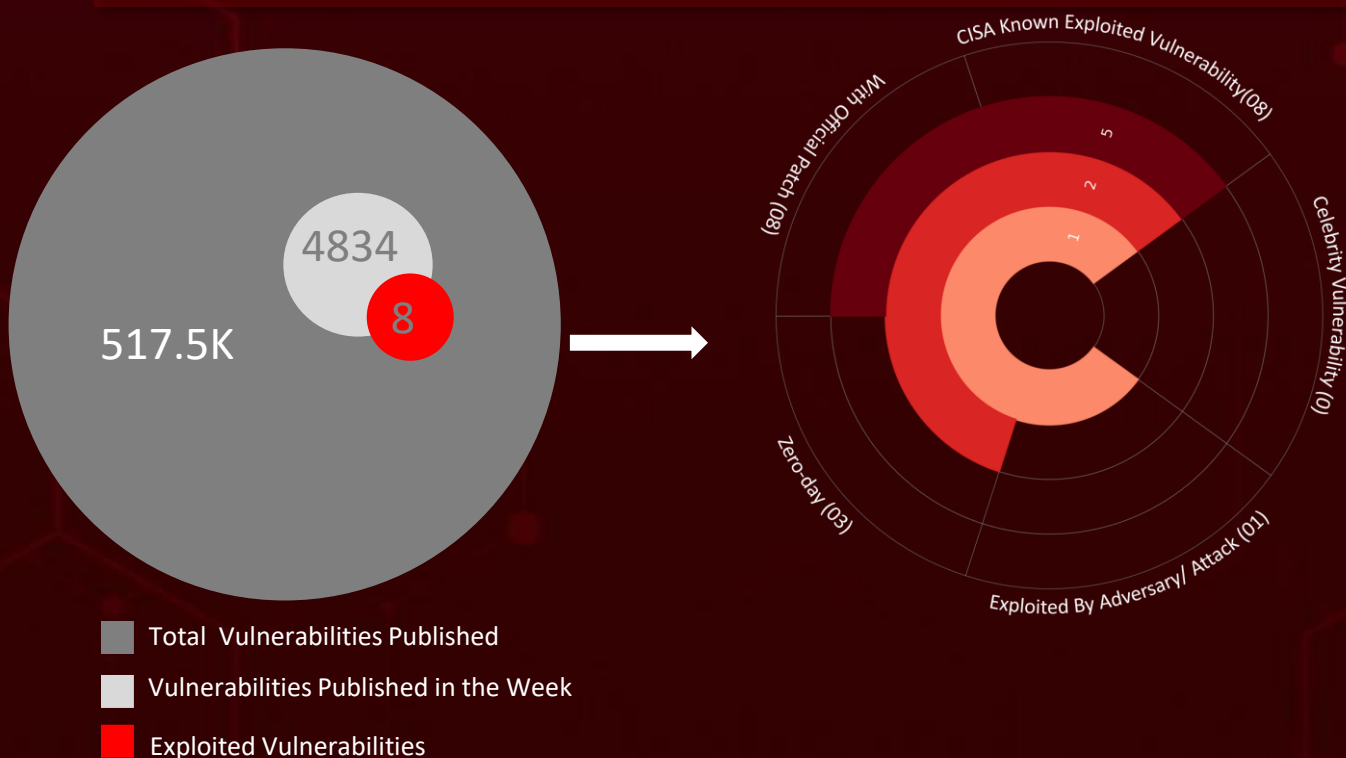
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	18
<u>Adversaries in Action</u>	26
<u>Recommendations</u>	29
<u>Threat Advisories</u>	30
<u>Appendix</u>	31
<u>What Next?</u>	34

Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **ten** major attacks were detected, **eight** vulnerabilities were actively exploited, and **two** threat actor groups were closely monitored, signaling a concerning escalation in malicious activity worldwide.

Among the most significant developments, Cisco has confirmed zero-day exploitation of **CVE-2026-76460**, a maximum-severity (CVSS 10.0) authentication bypass in Identity Services Engine that grants unauthenticated attackers root-level command execution, alongside **CVE-2026-76461** (CVSS 9.8), where a single crafted email compromises Secure Email Gateway with root privileges. In parallel, GitLab patched **CVE-2026-85706**, a maximum-severity path traversal in self-managed CE and EE that enables unauthenticated arbitrary file read, with scanning escalating to theft of configuration and SSH files within days.

Elsewhere, **Kimsuky**, the North Korean espionage group, expanded its arsenal with AI-generated lures, weaponized QR codes harvesting Microsoft 365 and Okta credentials, and Operation GitPower, which routes payloads and exfiltration through GitHub, Pastebin, Dropbox, and Slack. Separately, **Stormous**, the Arabic-speaking extortion group active since 2021, announced the termination of its operations and took all leak-site mirrors offline, though a rebrand cannot be ruled out. Together, these incidents reinforce a landscape in which rapidly weaponised edge-facing vulnerabilities and patient, evasion-heavy espionage operations advance side by side, underscoring the need for prompt patching of internet-facing systems and continuous monitoring for post-exploitation activity.



High Level Statistics

10

Attacks
Executed

- [AppleSeed \(KGH SPY\)](#)
- [HappyDoor](#)
- [HelloDoor](#)
- [httpMalice](#)
- [httpTroy](#)
- [MemLoad](#)
- [HTTPSpy](#)
- [AsyncRAT](#)
- [StormousX](#)
- [XMRig](#)

8

Vulnerabilities
Exploited

- [CVE-2026-85706](#)
- [CVE-2026-76461](#)
- [CVE-2026-87886](#)
- [CVE-2026-84869](#)
- [CVE-2026-76460](#)
- [CVE-2026-42016](#)
- [CVE-2026-42018](#)
- [CVE-2026-82329](#)

2

Adversaries in
Action

- [Kimsuky](#)
- [Stormous](#)



Insights

CVE-2026-76460

is a Cisco ISE authentication bypass under active zero-day exploitation, granting unauthenticated attackers root command execution.

JFrog Artifactory flaws were chained to forge persistent admin tokens on internet-facing repositories, peaking at 406,000 attempts in a day, and the minted tokens survive patching.

CVE-2026-85706

is a GitLab path traversal allowing unauthenticated file read on self-managed servers, exploited within a day to steal SSH and configuration secrets.

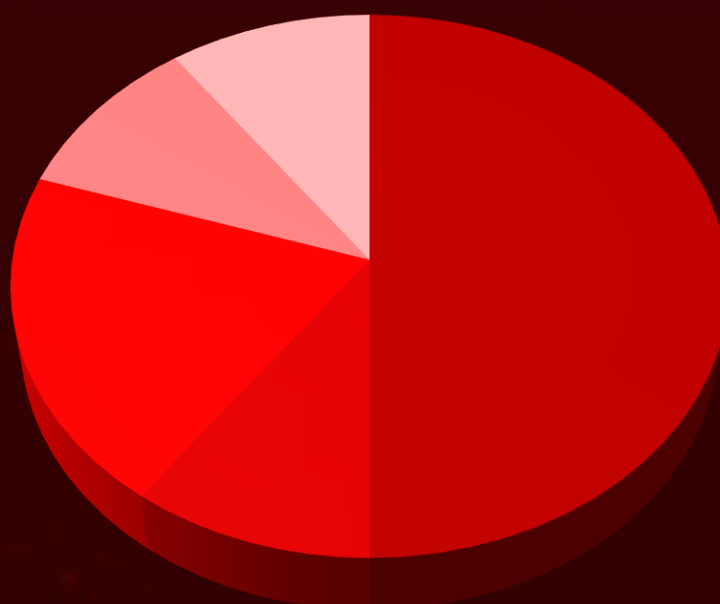
Kimsuky, the North Korean espionage group, expanded its arsenal with AI-generated lures, weaponized QR codes, and Operation GitPower, routing payloads and stolen data through GitHub, Pastebin, Dropbox, and Slack.

Stormous, the Arabic-speaking extortion group with up to 240 claimed victims, announced its shutdown and took all leak-site mirrors offline, though a rebrand cannot be ruled out.

CVE-2026-76461

lets a single crafted email seize root on Cisco Secure Email Gateway, with no login, password, or user interaction required.

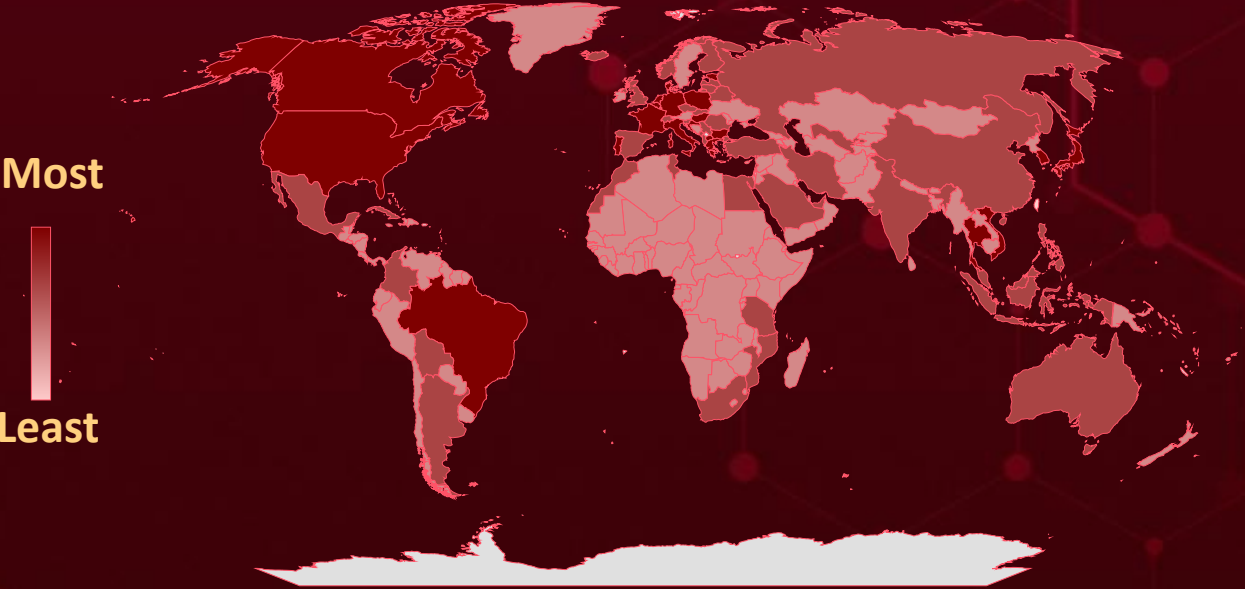
Threat Distribution



■ Backdoor ■ Loader ■ RAT ■ Ransomware ■ Cryptominer



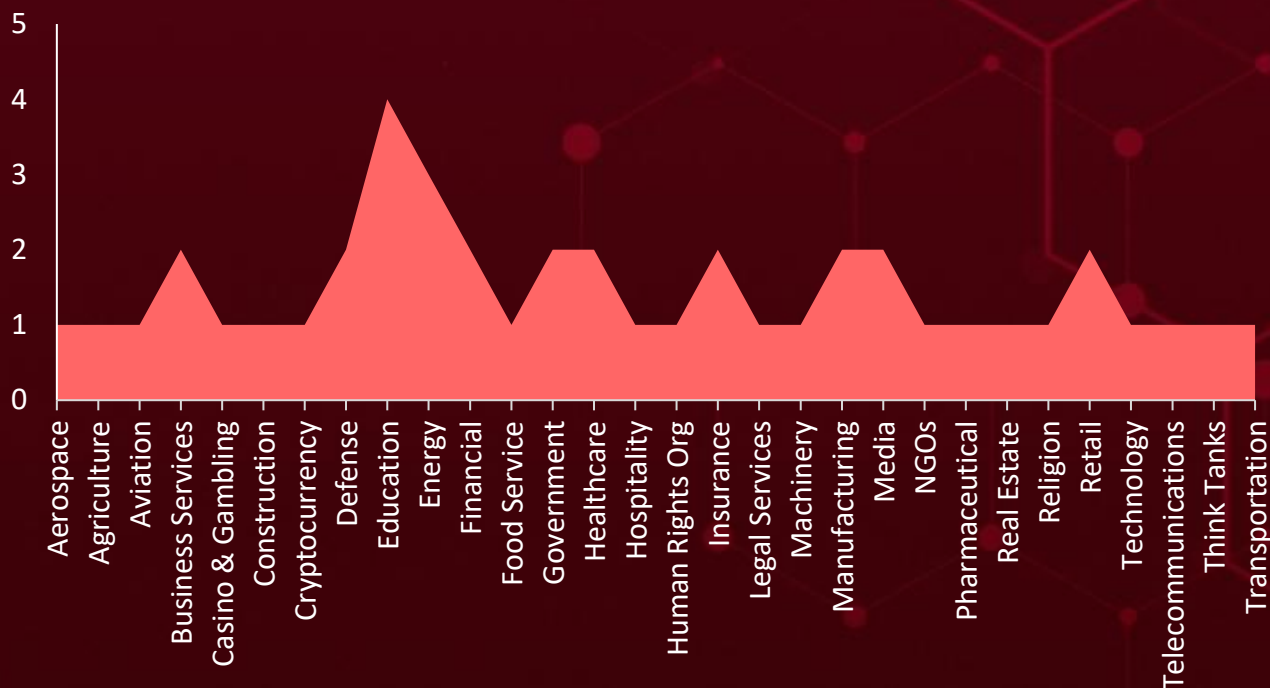
Targeted Countries



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

Countries	Countries	Countries	Countries
North Macedonia	Colombia	Tanzania	Peru
Hungary	Singapore	Mozambique	Guinea
Thailand	Iceland	Tunisia	Rwanda
Belgium	Australia	Czech Republic	Guinea-Bissau
Japan	India	United Arab Emirates	Dominica
Brazil	Egypt	Bolivia	Guyana
Portugal	Indonesia	Belarus	Antigua and Barbuda
Bulgaria	Saudi Arabia	Norway	Haiti
Greece	Iran	Philippines	Suriname
Canada	Slovenia	Lebanon	Holy See
Italy	Albania	Uruguay	Togo
Croatia	Switzerland	DR Congo	Honduras
Netherlands	Cuba	Qatar	Ukraine
Denmark	Turkey	Georgia	Botswana
Poland	Latvia	Tajikistan	Gambia
Estonia	China	Algeria	Armenia
South Korea	Uzbekistan	Palau	Oman
France	Argentina	Ghana	Brunei
United States	Lithuania	San Marino	Papua New Guinea
Germany	Russia	Bosnia and Herzegovina	Andorra
Vietnam	Luxembourg	Sri Lanka	Bangladesh
Finland	Serbia	Greenland	Burkina Faso
Romania	Malaysia	Fiji	Barbados
United Kingdom	Slovakia	Grenada	Iraq
	Mexico	Costa Rica	Saint Lucia
	Montenegro	Guatemala	Ireland
	Spain		
	Morocco		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1190

Exploit Public-Facing Application

T1588

Obtain Capabilities

T1588.006

Vulnerabilities

T1078

Valid Accounts

T1059

Command and Scripting Interpreter

T1657

Financial Theft

T1585

Establish Accounts

T1567

Exfiltration Over Web Service

T1583

Acquire Infrastructure

T1566

Phishing

T1005

Data from Local System

T1083

File and Directory Discovery

T1041

Exfiltration Over C2 Channel

T1098

Account Manipulation

T1589

Gather Victim Identity Information

T1053

Scheduled Task/Job

T1087

Account Discovery

T1105

Ingress Tool Transfer

T1068

Exploitation for Privilege Escalation

T1552

Unsecured Credentials

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AppleSeed (KGH_SPY)	AppleSeed is Kimsuky's flagship espionage implant, first seen in 2019 and still active through version 2.1, with the KGH_SPY suite tracked as a closely related modular toolset from the same actor. KGH_SPY as a modular spyware suite giving the operators reconnaissance, keylogging, information-stealing and backdoor functions. The AppleSeed family ships in two forms: a Dropper variant that pulls down further malware and runs C2 commands, and a Spy variant that harvests documents, screenshots, keystrokes and USB drive listings.	Spear-phishing emails	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent Access, Remote execution, Keystroke logging	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
SHA256	0845f218a588f7619169787c4db69ce9de0c84143b100400b6476d7289a1c493, 2c796053053a571e9f913fd5bae3bb45e27a9f510eace944af4b331e802a4ba0		

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
HappyDoor	HappyDoor is a backdoor, with the name taken from the "happy" string found in its export DLL name and debug data. It is a DLL that stores its configuration, including C2 addresses and encryption keys, in registry paths designed to look like legitimate software, and it communicates using a custom fixed-length packet structure with several authentication fields.	Spear-phishing emails	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent Access, Remote execution, Screen capture, File exfiltration	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
SHA256	4ac02dc231f2546ce64335729145db672b5ab01d8943df8a550cc77fc436df14		

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
HelloDoor	HelloDoor is a DLL-based backdoor and is Kimsuky's first known malware written in Rust, a language the group rarely uses. Its C2 is hosted on TryCloudflare, a temporary Cloudflare tunneling service that requires no account or setup, which makes the infrastructure behind it hard to trace. On execution it fingerprints the host using the MAC address, computer name and a fixed string, hashes that into a unique ID, and binds to local port 5555 or 5554 depending on whether its token is elevated.	Spear-phishing emails	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Autorun tampering, Host fingerprinting, Local port-binding, Process termination	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
SHA256	db284cc9b6536ab6f956a45ce9e5905716c7547f5e8dc572dc07aa125d27819e, 62aac86f38f26700cf534c0a316d31882ffb74488bd1d87a3caeef604fc3a124		

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
httpMalice	httpMalice is a backdoor, surfacing no later than December 2025. It profiles the host with Windows commands run under code page 949, indicating Korean-language (EUC-KR) targets, and its command set covers file transfer, directory archiving and upload, screen capture, in-memory payload loading, hibernation and self-removal.	Spear-phishing emails	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Persistent backdoor, Service creation, Remote execution	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
SHA256	23420100260cc80055fbf02f4464212278c0e71a4387537771f3fb50f2f891e5		

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
httpTroy	httpTroy is the final-stage backdoor in a Kimsuky three-part chain. Its role is long-term access and data exfiltration. It marks infected hosts by writing eight random bytes to an Alternate Data Stream, depending on whether it holds an elevated token. It is heavily obfuscated: API calls are hidden behind custom hashing and strings are scrambled with XOR and SIMD operations, with both reconstructed at runtime rather than reused, which frustrates static analysis.	Spear-phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Backdoor		Remote execution, Reverse shell, File transfer, Persistent Access	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
MD5	7e0825019d0de0c1c4a1673f94043ddb		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>MemLoad</u>	MemLoad is a loader; its purpose is twofold: to keep the real backdoor off disk to evade detection and vet the target before committing the payload, using anti-VM checks and basic reconnaissance.	Spear-phishing attachment	-
TYPE		IMPACT	AFFECTED PLATFORM
Loader		Payload delivery, Memory injection, Scheduled-task persistence, Privilege check	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
SHA256	2d597c3a726970927b302bf015cec4e37cdc974959cb846dbcb23cdb46386a6c		

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
HTTPSpy	HttpSpy is a remote access trojan seen in use around April 2026 against South Korean military and enterprise targets. The newer variant abandons the old single-binary design for a three-stage chain with the final RAT decrypted and executed entirely in memory. Its command set covers shell execution, file upload in chunks and download, screen capture, secure file wiping, timestamping, DLL injection into a chosen process, execution in a specified terminal session, TCP connectivity testing, live config updates and full self-uninstall.	Spear-phishing attachments	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Remote execution, File exfiltration, File download	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
MD5	a581fdea0970f8a5b6cfec4853c802d7		

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
AsyncRAT	AsyncRAT is a widely available open-source .NET remote access trojan, not custom Kimsuky tooling; the group adopts it alongside other commodity RATs. In Kimsuky's hands, it appears most prominently in the campaign tracks as Operation GitPower, where encrypted AsyncRAT payloads are staged in Git repositories disguised as image files, with GitHub serving as both the distribution point and the C2 channel so traffic blends into trusted developer infrastructure.	Spear-phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
RAT		Remote control, Keystroke logging, Screen capture, Credential theft	Windows
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afcff20ef524		

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
StormousX	StormousX is the ransomware program the Stormous group has marketed under its own brand since 2023 and later offered alongside GhostLocker through the STMX_GhostLocker affiliate service. It is advertised as a file-encrypting payload supporting the group's double-extortion operations, with victims listed across multiple regions.	phishing	-
TYPE		IMPACT	AFFECTED PLATFORM
Ransomware		Data theft and public leak	-
ASSOCIATED ACTOR			PATCH LINK
Stormous			-
IOC TYPE	VALUE		
TOR Address	3slz4povugieoi3tw7sblxoowxhbxzeju427cfsst5fo2tizepwatid[.]onion, h3reihqb2y7woqdary2g3bmk3apgtxuyhx4j2ftovbhe3l5svev7bdyd[.]onion		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>XMRig</u>	XMRig is an open-source, cross-platform Monero (XMR) cryptocurrency miner that is legitimate software but is one of the most widely abused tools in illicit cryptojacking, as attackers embed it in malware chains to hijack victim CPU resources for mining.	social engineering	CVE-2026-84869
TYPE		IMPACT	AFFECTED PLATFORM
Cryptominer		Resource hijacking, persistent access	ConnectWise ScreenConnect
ASSOCIATED ACTOR			PATCH LINK
-			https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin
IOC TYPE	VALUE		
Filename	SearchIndex.exe		

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-85706</u>		GitLab CE/EE self-managed (18.7 before 19.1.8; 19.2 before 19.2.6; 19.3 before 19.3.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:**, cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:**	-
GitLab Community Edition and Enterprise Edition Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1005: Data from Local System	https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-87886</u>		Acronis Backup plugin for cPanel & WHM (Before 1.9.3.1021); Acronis Backup extension for Plesk (Before 1.8.11.638)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:acronis:backup_plugin_for_cpanel_and_whm:*:*:*:*:*:*:**, cpe:2.3:a:acronis:backup_extension_for_plesk:*:*:*:*:*:*:*	-
Acronis Backup Incorrect Default Permissions Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-276	T1068: Exploitation for Privilege Escalation	https://security-advisory.acronis.com/updates/UPD-2609-3d72-20a7 , https://security-advisory.acronis.com/updates/UPD-2609-efb0-50b2 , https://security-advisory.acronis.com/advisories/SEC-10986

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-84869</u>		ConnectWise ScreenConnect client version before 26.6.5	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*	XMRig cryptominer
ConnectWise ScreenConnect Improper Privilege Management and Missing Authorization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269 CWE-862	T1068: Exploitation for Privilege Escalation, T1548: Abuse Elevation Control Mechanism	https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-42016</u>		JFrog Artifactory Self-Hosted Before 7.133.11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:jfrog:artifactory:*:*:*:*:self_hosted:*:*:*	-
JFrog Artifactory Incorrect Authorization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1583: Acquire Infrastructure, T1587: Develop Capabilities, T1528: Steal Application Access Token, T1190: Exploit Public-Facing Application	https://docs.jfrog.com/releases/docs/artifactory-self-managed-releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-42018</u>		JFrog Artifactory Self-Hosted Before: 7.111.20; 7.117.0 to 7.117.27; 7.125.0 to 7.125.19; 7.133.0 to 7.133.28; 7.146.0 to 7.146.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jfrog:artifactory:*:*:*:*: self_hosted:*:*:*	-
JFrog Artifactory Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application; T1562: Impair Defenses	https://docs.jfrog.com/releases/docs/artifactory-self-managed-releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
<u>CVE-2026-82329</u>		JFrog Artifactory Self-Hosted 7.111.4 to: 7.111.20; 7.117.0 to 7.117.27; 7.125.0 to 7.125.19; 7.133.0 to 7.133.28; 7.146.0 to 7.146.37; 7.161.0 to 7.161.19	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jfrog:artifactory:*:*:*:*:self_hosted:*:*:*	-
JFrog Artifactory Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application; T1562: Impair Defenses	https://docs.jfrog.com/releases/docs/artifactory-self-managed-releases



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Stormous	-	Technology, Business Services & Consulting, Manufacturing, Retail, Hospitality, Education, Healthcare, Telecommunications, Media, Government, Financial Services, Pharmaceutical, Energy, Transportation, Casino & Gambling, Aerospace and Defense, Food Service, Religion, Agriculture, Real Estate, Aviation, Insurance	United States, United Kingdom, Spain, France, Italy, Malaysia, United Arab Emirates, China, Brazil, India, Argentina, Turkey, Indonesia, Germany, Vietnam, Japan, Thailand, Uzbekistan, Iran, Lebanon, Colombia, Poland, South Africa, Taiwan, Tanzania, Tunisia, Bolivia, Canada, Cuba, Australia, Philippines, Denmark, Netherlands, Morocco, Portugal, Egypt, Croatia, Serbia, Belarus, Singapore, Mexico, Hungary, Bulgaria, South Korea, North Macedonia, Belgium, Greece, Switzerland, Saudi Arabia, Estonia, Mozambique
	MOTIVE		
	Financial gain		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	StormousX	-
TTPs			
TA0042: Resource Development, TA0001: Initial Access, TA0009: Collection, TA0010: Exfiltration, TA0040: Impact, T1583: Acquire Infrastructure, T1583.001: Domains, T1583.006: Web Services, T1585: Establish Accounts, T1585.001: Social Media Accounts, T1587: Develop Capabilities, T1587.001: Malware, T1078: Valid Accounts, T1566: Phishing, T1005: Data from Local System, T1213: Data from Information Repositories, T1114: Email Collection, T1567: Exfiltration Over Web Service, T1567.002: Exfiltration to Cloud Storage, T1486: Data Encrypted for Impact, T1657: Financial Theft			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 <u>Kimsuky (aka</u> <u>APT43, Thallium,</u> <u>THALLIUM,</u> <u>Velvet Chollima,</u> <u>Black</u> <u>Banshee,</u> <u>Emerald Sleet,</u> <u>Ruby Sleet,</u> <u>Sparkling Pisces,</u> <u>Springtail,</u> <u>TA427, TA406,</u> <u>Earth</u> <u>Kumiho,</u> <u>PatheticSlug,</u> <u>ARCHIPELAGO,</u> <u>SharpTongue,</u> <u>ITG16,</u> <u>Greendinosa,</u> <u>RGB-D5,</u> <u>Cerium)</u>	North Korea	Government, Public Administration, Defense, Think Tanks, Policy Research Institutes, Academia, Universities, NGOs, Human Rights Organizations, Media, Healthcare, Machinery, Energy, Nuclear Power Operations, Manufacturing, Business Services, Legal Services, Construction, Financial, Insurance, Retail, Cryptocurrency	South Korea, United States, Japan, Vietnam, Thailand, Brazil, Germany, Russia, Canada, and broader Europe including Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, and Albania
	MOTIVE		
	Espionage, Financial Gains		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	CVE-2017-11882 CVE-2018-0802 CVE-2019-0708 CVE-2019-1405 CVE-2020-0787 CVE-2024-1709 CVE-2025-48703	AppleSeed (KGH_SPY), AlphaSeed, HappyDoor, PebbleDash, HelloDoor, httpMalice, httpTroy, MemLoad, HTTPSpy, AsyncRAT, BabyShark, GoldDragon, KLogEXE, Troll Stealer, Gomir, NavRAT, NikiHTTP, NikiTeaR, ComeBacker, DRATzarus, FastFire, FastSpy, FlowerPower, RandomQuery, Yorekey, Grease, TRANSLATEXT, QuasarRAT, Gh0st RAT, KimJongRAT, CSPY Downloader, BITTERSWEET, VENOMBITE, xRAT, MailFetch.py, Reger Dropper, Pidoc Dropper	GitHub, Pastebin, Dropbox, Slack, Cloudflare Quick Tunnels, Visual Studio, Microsoft 365, Okta

NAME	TTPs
 <u>Kimసుకు (aka APT43, Thallium, THALLIUM, Velvet Chollima, Black Banshee, Emerald Sleet, Ruby Sleet, Sparkling Pisces, Springtail, TA427, TA406, Earth Kumiho, PatheticSlug, ARCHIPELAGO, SharpTongue, ITG16, Greendinosa, RGB-D5, Cerium)</u>	TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0012: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1566: Phishing; T1657: Financial Theft; T1041: Exfiltration Over C2 Channel; T1204: User Execution; T1082: System Information Discovery; T1070: Indicator Removal; T1027: Obfuscated Files or Information; T1111: Multi-Factor Authentication Interception; T1056: Input Capture; T1102: Web Service; T1071: Application Layer Protocol; T1005: Data from Local System; T1001: Data Obfuscation; T1003: OS Credential Dumping; T1020: Automated Exfiltration; T1030: Data Transfer Size Limits; T1036: Masquerading; T1053: Scheduled Task/Job; T1055: Process Injection; T1057: Process Discovery; T1059: Command and Scripting Interpreter; T1074: Data Staged; T1078: Valid Accounts; T1083: File and Directory Discovery; T1087: Account Discovery; T1098: Account Manipulation; T1105: Ingress Tool Transfer; T1106: Native API; T1113: Screen Capture; T1115: Clipboard Data; T1123: Audio Capture; T1133: External Remote Services; T1140: Deobfuscate/Decode Files or Information; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution; T1218: System Binary Proxy Execution; T1219: Remote Access Software; T1497: Virtualization/Sandbox Evasion; T1518: Software Discovery; T1531: Account Access Removal; T1539: Steal Web Session Cookie; T1543: Create or Modify System Process; T1547: Boot or Logon Autostart Execution; T1553: Subvert Trust Controls; T1555: Credentials from Password Stores; T1557: Adversary-in-the-Middle; T1562: Impair Defenses; T1564: Hide Artifacts; T1567: Exfiltration Over Web Service; T1572: Protocol Tunneling; T1573: Encrypted Channel; T1583: Acquire Infrastructure; T1584: Compromise Infrastructure; T1585: Establish Accounts; T1586: Compromise Accounts; T1587: Develop Capabilities; T1588: Obtain Capabilities; T1589: Gather Victim Identity Information; T1592: Gather Victim Host Information; T1598: Phishing for Information; T1620: Reflective Code Loading; T1622: Debugger Evasion; T1682: Query Public AI Services; T1001.001: Junk Data; T1003.001: LSASS Memory; T1027.013: Encrypted/Encoded File; T1036.005: Match Legitimate Name or Location; T1053.005: Scheduled Task; T1055.001: Dynamic-link Library Injection; T1056.001: Keylogging; T1059.001: PowerShell; T1070.003: Clear Command History; T1070.004: File Deletion; T1071.001: Web Protocols; T1074.001: Local Data Staging; T1078.003: Local Accounts; T1087.004: Cloud Account; T1102.002: Bidirectional Communication; T1204.002: Malicious File; T1218.010: Regsvr32; T1497.001: System Checks; T1518.001: Security Software Discovery; T1543.003: Windows Service; T1547.001: Registry Run Keys / Startup Folder; T1553.002: Code Signing; T1555.003: Credentials from Web Browsers; T1562.004: Disable or Modify System Firewall; T1564.004: NTFS File Attributes; T1566.001: Spearphishing Attachment; T1567.002: Exfiltration to Cloud Storage; T1573.001: Symmetric Cryptography; T1583.001: Domains; T1584.004: Server; T1585.003: Cloud Accounts; T1586.002: Email Accounts; T1587.001: Malware; T1588.002: Tool; T1589.002: Email Addresses; T1598.003: Spearphishing Link; T1588.007: Artificial Intelligence; T1566.002: Spearphishing Link; T1059.003: Windows Command Shell; T1059.005: Visual Basic; T1059.007: JavaScript; T1027.001: Binary Padding; T1036.008: Masquerade File Type; T1070.006: Timestomp; T1218.011: Rundll32; T1564.003: Hidden Window; T1071.003: Mail Protocols; T1102.001: Dead Drop Resolver

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eight exploited vulnerabilities** and block the indicators related to the threat actors **Kimsuky**, **Stormous** and malware **AppleSeed (KGH_SPY)**, **HappyDoor**, **HelloDoor**, **httpMalice**, **httpTroy**, **MemLoad**, **HTTPSpy**, **AsyncRAT**, **StormousX**, and **XMRig**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Run a Scan to discover the assets impacted by the **eight exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Kimsuky**, and malware **StormousX** in Breach and Attack Simulation(BAS).

Threat Advisories

[GitLab Path Traversal \(CVE-2026-85706\) Exploited to Steal Secrets](#)

[Root Delivered by Email: Cisco Secure Email Gateway Zero-Day](#)

[Kimsuky Blends AI-Generated Lures and Quishing into an Expanded Espionage Arsenal](#)

[Acronis Backup Plugin Flaw Exploited in the Wild](#)

[Stormous Extortion Group Announces Shutdown After Four Years of Leak-Site Activity](#)

[CVE-2026-84869: Critical ScreenConnect Client Flaw Under Active Exploitation](#)

[Cisco ISE Authentication Bypass Zero-Day Under Active Exploitation](#)

[JFrog Artifactory Flaws Chained for Administrative Takeover](#)

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

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>AppleSeed</u> (KGH_SPY)	SHA256	0845f218a588f7619169787c4db69ce9de0c84143b100400b6476d7289a1c493, 2c796053053a571e9f913fd5bae3bb45e27a9f510eace944af4b331e802a4ba0, 8c35eed98b295d2fc13cb7280e17dcbf232f6703ee74052a479196786ea9f333
<u>HappyDoor</u>	SHA256	4ac02dc231f2546ce64335729145db672b5ab01d8943df8a550cc77fc436df14
	Domains	cms[.]spaceyou[.]o-r[.]kr, erp[.]spaceme[.]p-e[.]kr
<u>HelloDoor</u>	SHA256	db284cc9b6536ab6f956a45ce9e5905716c7547f5e8dc572dc07aa125d27819e, 62aac86f38f26700cf534c0a316d31882ffb74488bd1d87a3caeef604fc3a124
	FileName	[별지 제8호서식] 개인정보(열람 정정삭제 처리정지) 요구서(개인 정보 보호법 시행규칙).hwp.jse

Attack Name	TYPE	VALUE
<u>httpMalice</u>	SHA256	23420100260cc80055fbf02f4464212278c0e71a4387537771f3fb50f2f891e5
	URL	hxxps[:]//www[.]pyrotech[.]co[.]kr/common/include/tech/default[.]php, hxxp[:]//newjo-imd[.]com/common/include/library/default[.]php
	MD5	08160acf08fccecd7b34090db18b321, 94faed9af49c98a89c8acc55e97276c9
<u>httpTroy</u>	MD5	7e0825019d0de0c1c4a1673f94043ddb
	Domains	file[.]bigcloud[.]n-e[.]kr, load[.]auraria[.]org
<u>MemLoad</u>	MD5	58ac2f65e335922be3f60e57099dc8a3, f73ba062116ea9f37d072aa41c7f5108
	SHA256	2d597c3a726970927b302bf015cec4e37cdc974959cb846dbcb23cdb46386a6c
	Domains	load[.]ssangyongcne[.]o-r[.]kr, load[.]yju[.]o-r[.]kr, attach[.]docucloud[.]o-r[.]kr, load[.]supershop[.]o-r[.]kr, load[.]erasecloud[.]n-e[.]kr
<u>HTTPSpy</u>	URLs	hxxps[:]//bigfile[.]jaycloudlab[.]com/download[.]php?id=745896, hxxps[:]//download[.]birdriver[.]org/download[.]php?id=393156
	MD5	a581fdea0970f8a5b6cfec4853c802d7
<u>AsyncRAT</u>	SHA256	601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455

Attack Name	TYPE	VALUE
<u>AsyncRAT</u>	SHA256	daac2fe0fe9a71f531d9b35c9ca269c0bdfbd1bbac5e8d73fc91afcff20ef524,7bb7c893fdf7f7ccd998610969d23993c50fc0b693e67930b6f98d8dbd003ee3
<u>StormousX</u>	TOR Address	3slz4povugieoi3tw7sblxoowxhbzxeju427cffsst5fo2tizepwatid[.]onion, h3reihqb2y7woqdary2g3bmk3apgtxuyhx4j2ftovbhe3l5svev7bdyd[.]onion, pdcizqzjitsgfcgqeyhuee5u6uki6zy5slzioinlhx6xjns25irdgqd[.]onion, 6sf5xa7eso3e3vk46i5tpcqhnlayczztj7zjktzaztlotyy75zs6j7qd[.]onion, zib7duoiglvzvpj5faly6bio4xhwiby2lupsnxrkjnx46gmwdfyrid[.]onion, ahb6hjhe4nomgfwxequu52hazigh4ty4gdcnrf3r7z5tiyhour5py2id[.]onion, stniiomyjliimcgkvdsvgen3eaa0z55hreqqx6o77yvmppwt7gklffqd[.]onion, 5pbckbo5ra36srfwmb2y6mqpqj7akx3e6ewanujsv7nnjndbbgsjsad[.]onion
<u>XM Rig</u>	Filename	SearchIndex.exe

What Next?

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

Book a demo of HivePro.

REPORT GENERATED ON

September 22, 2026 • 11:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com