Date of Publication
April 28, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

21 to 27 APRIL 2025

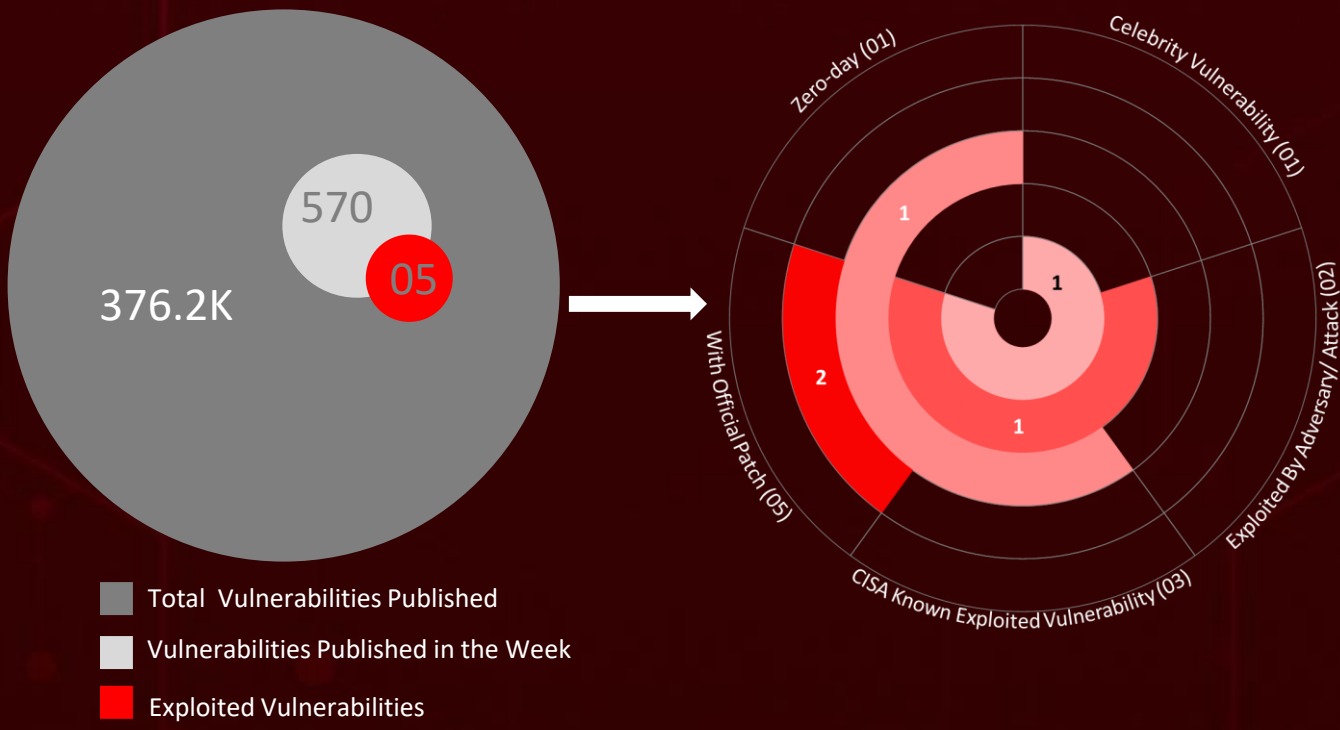
Table Of Contents

Summary

HiveForce Labs has observed a significant surge in cybersecurity threats, underscoring the growing complexity and frequency of cyber incidents. Over the past week, **fifteen** major attacks were detected, **five** critical vulnerabilities were actively exploited, and **four** threat actor groups were closely monitored, reflecting an alarming escalation in malicious activities.

A newly uncovered flaw, **CVE-2025-32433**, in the Erlang/OTP SSH server allows unauthenticated remote code execution, exposing systems to complete takeover. Meanwhile, North Korea-linked **Kimsuky** is targeting South Korea's critical sectors, leveraging old but effective vulnerabilities like **CVE-2017-11882** and **CVE-2019-0708** (**BlueKeep**) to breach networks.

Adding to the growing list of cyber threats, an active exploit, **CVE-2025-42599**, affecting Active! mail by QUALITIA CO., LTD., puts educational and enterprise email servers at serious risk. China-based **Billbug** is ramping up cyber espionage campaigns against Southeast Asian government and infrastructure systems. These developments spotlight the rising sophistication of cyber adversaries and reinforce the urgent need for agile, proactive cybersecurity defenses to navigate an increasingly hostile digital landscape.



High Level Statistics

15
Attacks Executed

5
Vulnerabilities Exploited

4
Adversaries in Action

- MySpy
- RandomQuery
- KimaLogger
- Sagerunex
- ChromeKatz
- CredentialKatz
- ThreatNeedle
- wAgent
- SIGNBT
- COPPERHEDGE
- Agamemnon
- LPEClient
- CrazyHunter
- LAGTOY
- Cactus

- CVE-2025-32433
- CVE-2019-0708
- CVE-2017-11882
- CVE-2025-42599
- CVE-2025-32965

- Kimsuky
- Billbug
- Lazarus
- ToyMaker

Insights

CVE-2025-42599: Active! mail Vulnerability Opens the Door for Remote Attacks

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

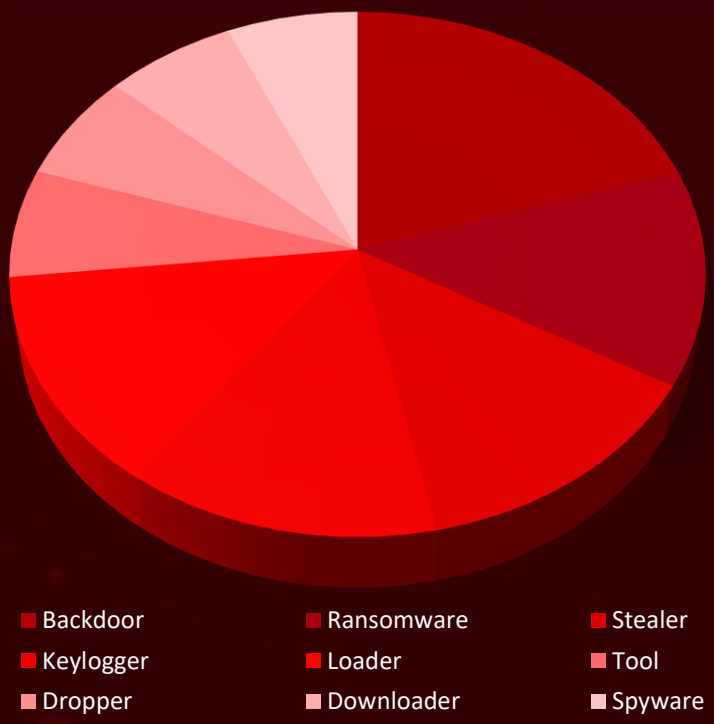
Billbug Cyber Group Expands Its Southeast Asian Espionage Network

Operation SyncHole: Lazarus Turns Familiar Tools into Silent Threats

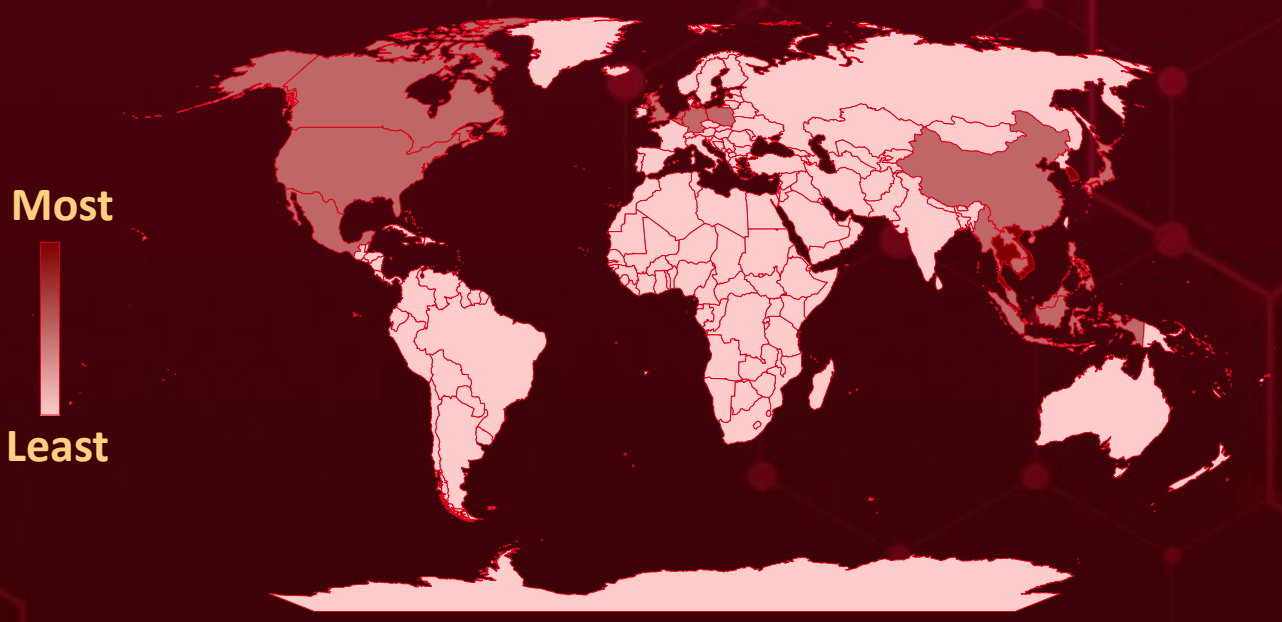
80% Open-Source, 100% Dangerous: CrazyHunter Ransomware Emerges

ToyMaker Brokers Access, **Cactus** Delivers the Blow in Coordinated Ransomware Hit

Threat Distribution

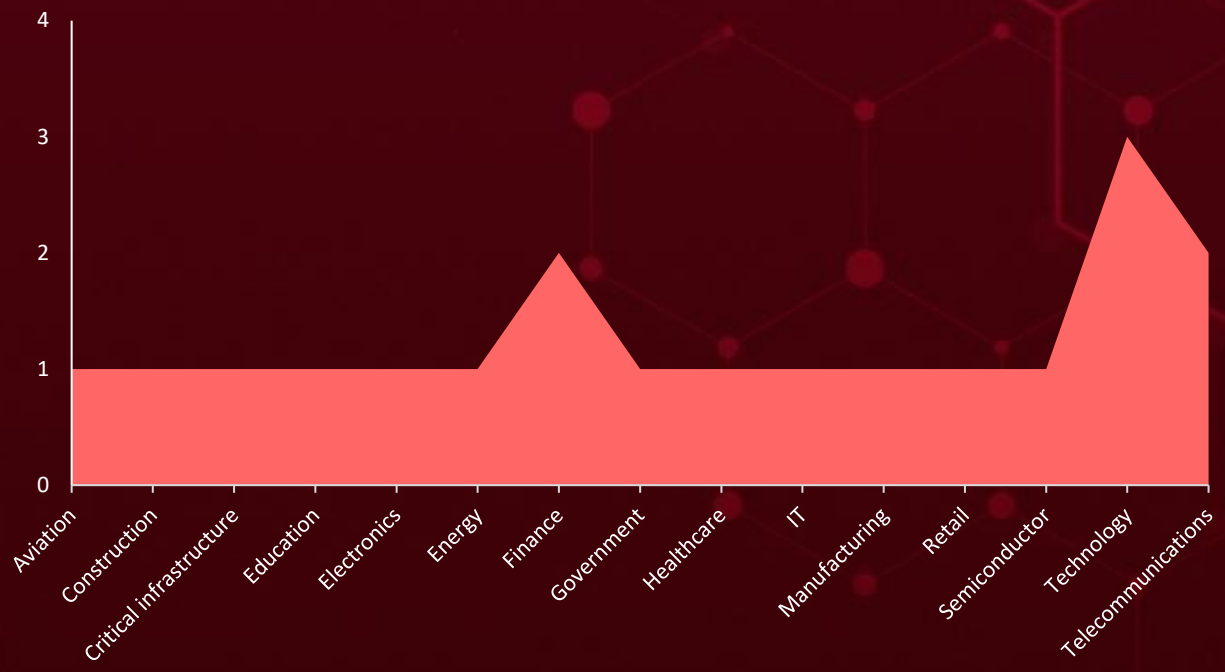


Targeted Countries



Countries	Countries	Countries	Countries
Thailand	Maldives	Armenia	Senegal
South Korea	Brazil	Taiwan	East Timor
Singapore	Nauru	Colombia	Africa
Vietnam	Brunei	Tunisia	Ecuador
Poland	Peru	Comoros	Somalia
Mexico	Brunei	Malawi	Egypt
United States	Seychelles	Congo	South Sudan
Belgium	Bulgaria	Malta	El Salvador
Netherlands	Suriname	Costa Rica	State of Palestine
Cambodia	Burkina Faso	Barbados	Equatorial Guinea
Laos	Uganda	Côte d'Ivoire	Switzerland
Canada	Burundi	Mongolia	Eritrea
Malaysia	Mauritania	Croatia	Tanzania
China	Cabo Verde	Belarus	Estonia
Myanmar	Morocco	Cuba	Tonga
Germany	Antigua and Barbuda	Angola	Eswatini
Philippines		Cyprus	Turkmenistan
Indonesia	Nicaragua	Nigeria	Ethiopia
Japan	Cameroon	Czechia	Bhutan
United Kingdom	Palau	Oman	Fiji
Saint Kitts & Nevis	Argentina	Denmark	Bangladesh
Moldova	Qatar	Papua New Guinea	Finland
Timor-Leste	Central African Republic	Djibouti	Mali
Bolivia		Benin	France
North Macedonia	Sao Tome & Principe	Dominica	Marshall Islands
Bosnia and Herzegovina	Chad	Russia	Gabon
	Slovenia	Dominican Republic	Mauritius
South Africa	Chile	Samoa	Gambia
Botswana	Sri Lanka	DR Congo	Micronesia

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1082** System Information Discovery
T1021 Remote Services	**T1027** Obfuscated Files or Information	**T1078** Valid Accounts	**T1560** Archive Collected Data	**T1068** Exploitation for Privilege Escalation
T1071.001 Web Protocols	**T1105** Ingress Tool Transfer	**T1566.001** Spearphishing Attachment	**T1071** Application Layer Protocol	**T1036** Masquerading
T1041 Exfiltration Over C2 Channel	**T1562.001** Disable or Modify Tools	**T1078.001** Default Accounts	**T1574** Hijack Execution Flow	**T1021.004** SSH

Attacks Executed

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

IOC TYPE	VALUE
SHA256	16bb4855a7412ce2bd63b2bcc0de3add1e7ca8c0f22acf8172e760931ef3e7da

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

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
KimaLogger	KimaLogger is a stealthy keylogger used to monitor user activity, capture credentials, and exfiltrate sensitive data to attacker-controlled C2 servers.	Exploited the RDP vulnerability	CVE-2019-0708 CVE-2017-11882
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Credential Theft, Data Exfiltration	Windows Server, Microsoft Office
Keylogger			
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708, https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882
IOC TYPE	**VALUE**		
SHA256	68c648a75976911609713dfa33957bf4399cc074b986ec88c85d0ec15e75d640		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Sagerunex	Sagerunex backdoor variants employ obfuscation to evade detection and use both traditional C2 infrastructure and legitimate platforms like Dropbox, Twitter, and Zimbra for stealthy communication and data exfiltration.	Exploiting vulnerabilities in public-facing applications, spear-phishing, or credential abuse.	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Exfiltration, Persistence and Control	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Billbug			-
IOC TYPE	**VALUE**		
SHA256	4b430e9e43611aa67263f03fd42207c8ad06267d9b971db876b6e62c19a0805e, 3fb81913c2daf36530c9ae011feebeb5bc61432969598e2dfaa52fc2ce839f20		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ChromeKatz	ChromeKatz stealer is capable of extracting both stored credentials and cookies from the Chrome browser.	Exploiting vulnerabilities in public-facing applications, spear-phishing, or credential abuse.	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Credential Theft, Session Hijacking	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Billbug			-
IOC TYPE	**VALUE**		
SHA256	2e1c25bf7e2ce2d554fca51291eaeb90c1b7c374410e7656a48af1c0afa34db4, 6efb16aa4fd785f80914e110a4e78d3d430b18cbdd6ebd5e81f904dd58baae61, ea87d504aff24f7daf026008fa1043cb38077eccec9c15bbe24919fc413ec7c7		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CredentialKatz	CredentialKatz is a stealer designed to extract credentials stored in the Chrome browser.	Exploiting vulnerabilities in public-facing applications, spear-phishing, or credential abuse.	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Stealer		Credential Theft, Privacy Violation	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Billbug			-
IOC TYPE	**VALUE**		
SHA256	e3869a6b82e4cf54cc25c46f2324c4bd2411222fd19054d114e7ebd32ca32cd1, 29d31cfc4746493730cda891cf88c84f4d2e5c630f61b861acc31f4904c5b16d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ThreatNeedle	The ThreatNeedle variant, a hallmark backdoor of Lazarus, was discovered running as a subprocess of Cross EX, a legitimate Korean software. It employed advanced encryption, generating Curve25519 key pairs for ChaCha20-encrypted communications with the C2. ThreatNeedle facilitated stealthy data exfiltration and persistence via system services like IKEEXT or SSP registration.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Stealthy Persistence, Facilitation of Further Malware Deployment	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-
IOC TYPE	**VALUE**		
SHA256	94868d8db5a22df0b841d282d5d408d00179224ec7031386fbd80f0473f486b3		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
wAgent	wAgent, a malicious loader documented in 2020, was disguised as liblzma.dll and executed via the command line. It can receive data in both form-data and JSON formats, depending on the C2 server it successfully connects to.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Covert Execution, Facilitation of Further Malware Deployment	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-
IOC TYPE	**VALUE**		
SHA256	922a2ffdbfbbc3998ff38111d20c6ed88bba0e09de7f0f66a28b06c0ee51f69c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SIGNBT	The latest version of SIGNBT has limited remote control capabilities, focusing primarily on executing additional payloads. The C2 server is hardcoded, without relying on configuration files. The malware receives an RSA public key from the C2, encrypts a randomly generated AES key, and uses it to encrypt all traffic.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Covert Communication, Potential for Lateral Movement	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-
IOC TYPE	**VALUE**		
SHA256	507929bd787b09db862543f203e6f9faa23409af534891bbbf145296c1697eed, 4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74, 507066f487ea037bde2e91158a63113585776fe0c13cfa7fe6252ae58e89a59a, 04bc903a0f44c31e976a2a090d8b846d68c3d87122293f8ce0c2d20a1978e37e		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
COPPERHEDGE	COPPERHEDGE, a dropper and variant of Manuscrypt, was used in the DeathNote cluster attacks. The latest version retrieves C2 configuration data from Alternate Data Streams (ADS) and communicates with the C2 via HTTP, using three to four randomly named parameters per request. Lazarus primarily deployed COPPERHEDGE for internal reconnaissance during the operation.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		Internal Reconnaissance, Facilitation of Further Malware Deployment	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-
IOC TYPE	**VALUE**		
SHA256	23ac99fb8de813172bb641baefff59fd8b84f1b39b362d7fd11736b5667bee56		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Agamemnon	The Agamemnon downloader is designed to fetch and execute additional payloads from its C2 server. It processes commands by parsing parameters delimited by ";;" received from the C2.	Compromised online media sites	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Payload Delivery, Command Execution	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-
IOC TYPE	**VALUE**		
SHA256	1174fd03271f80f5e2a6435c72bdd0272a6e3a37049f6190abf125b216a83471, 9c906c2f3bfb24883a8784a92515e6337e1767314816d5d9738f9ec182beaf44, e13888eed2466efaae729f16fc8e348fbabea8d7acd6db4e062f6c0930128f8f, c92c158d7c37fea795114fa6491fe5f145ad2f8c08776b18ae79db811e8e36a3, 17f1c3dc3ad9e0e87e6a131bd93d12c074b443f365eea2e720b9d9939f9ce22e, 75bf8feeac2b5b1690feab45155a6b97419d6d1b0d36083daccb061dc5dbdea8		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CrazyHunter	CrazyHunter is a Go-based ransomware first observed in January 2025, built on the open-source Prince encryptor. Notably, around 80% of the toolkit used in its attack chain consists of repurposed open-source tools—a strategic choice that lowers development costs and complicates attribution.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial Loss, Data Exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	f72c03d37db77e8c6959b293ce81d009bf1c85f7d3bdaa4f873d3241833c146b		

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
LAGTOY	LAGTOY is a custom backdoor designed to extract credentials from targeted enterprises. It enables the creation of reverse shells and the execution of commands on compromised endpoints. LAGTOY employs a time-based logic to determine whether to execute commands or remain dormant for a specified duration.	Exploiting Internet-Facing Vulnerabilities	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Remote Command Execution, Targeted Exploitation	Windows
ASSOCIATED ACTOR			**PATCH LINK**
ToyMaker			-
IOC TYPE	**VALUE**		
SHA256	fdf977f0c20e7f42dd620db42d20c561208f85684d3c9efd12499a3549be3826		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cactus	Cactus employed various remote administration tools, such as eHorus, RMS, and AnyDesk, across different endpoints to sustain long-term access. They conducted extensive network reconnaissance, deployed remote management tools, executed a ransomware payload, exfiltrated sensitive data, and deleted shadow volume copies to hinder data recovery.	Exploiting Internet-Facing Vulnerabilities	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Exfiltration, Financial Loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
ToyMaker			-
IOC TYPE	**VALUE**		
SHA256	670586ea97fcd63f4375a976cc5ddaede00f2e4e5651ede2fa8b61b929563d31, d3d0bd2f72d0e23650ef47ff3c5297c1a201270a71fee78e8badfa816d455e13, 55a4e88be5f80260e3366b6adc1c2d1c6b0673105b509371ff7f3525d2f1c3ec		

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

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

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

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

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

Adversaries in Action

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

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

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

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

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

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

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actors **Kimsuky, Billbug, Lazarus, ToyMaker,** and malware **MySpy, RandomQuery, KimaLogger, Sagerunex, ChromeKatz, CredentialKatz, ThreatNeedle, wAgent, SIGNBT, COPPERHEDGE, Agamemnon, LPEClient, CrazyHunter, LAGTOY, Cactus.**

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 **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Kimsuky, Billbug, Lazarus, ToyMaker,** and malware **KimaLogger, Sagerunex, CrazyHunter** in Breach and Attack Simulation(BAS).

Threat Advisories

Erlang/OTP SSH Flaw Lets Hackers Bypass Login and Run Code

Kimsuky's Stealthy RDP Espionage Campaign

Active! Mail Under Attack via CVE-2025-42599

Billbug Cyberespionage Campaign Targets Southeast Asia

XRP at Risk: Malicious xrpl.js Update Steals Wallet Keys

April 2025 Linux Patch Roundup

Operation SyncHole: Lazarus Escalates Cyberattacks Against South Korean Industries

Go-Based CrazyHunter Ransomware Strikes Taiwan

ToyMaker: Unveiling the Role of Initial Access Brokers in Ransomware Attacks

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
MySpy	SHA256	16bb4855a7412ce2bd63b2bcc0de3add1e7ca8c0f22acf8172e760931ef3e7da
KimaLogger	SHA256	68c648a75976911609713dfa33957bf4399cc074b986ec88c85d0ec15e75d640
	MD5	184a4f3f00ca40d10790270a20019bb4
Sagerunex	SHA256	4b430e9e43611aa67263f03fd42207c8ad06267d9b971db876b6e62c19a0805e, 3fb81913c2daf36530c9ae011feebeb5bc61432969598e2dfaa52fc2ce839f20
ChromeKatz	SHA256	2e1c25bf7e2ce2d554fca51291eaeb90c1b7c374410e7656a48af1c0afa34db4, 6efb16aa4fd785f80914e110a4e78d3d430b18cbdd6ebd5e81f904dd58baae61, ea87d504aff24f7daf026008fa1043cb38077eccec9c15bbe24919fc413ec7c7
CredentialKatz	SHA256	e3869a6b82e4cf54cc25c46f2324c4bd2411222fd19054d114e7ebd32ca32cd1, 29d31cfc4746493730cda891cf88c84f4d2e5c630f61b861acc31f4904c5b16d
ThreatNeedle	SHA256	94868d8db5a22df0b841d282d5d408d00179224ec7031386fbd80f0473f486b3
	MD5	f1bcb4c5aa35220757d09fc5feea193b
wAgent	SHA256	922a2ffdbfbbc3998ff38111d20c6ed88bba0e09de7f0f66a28b06c0ee51f69c
	MD5	dc0e17879d66ea9409cdf679bfea388c

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

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

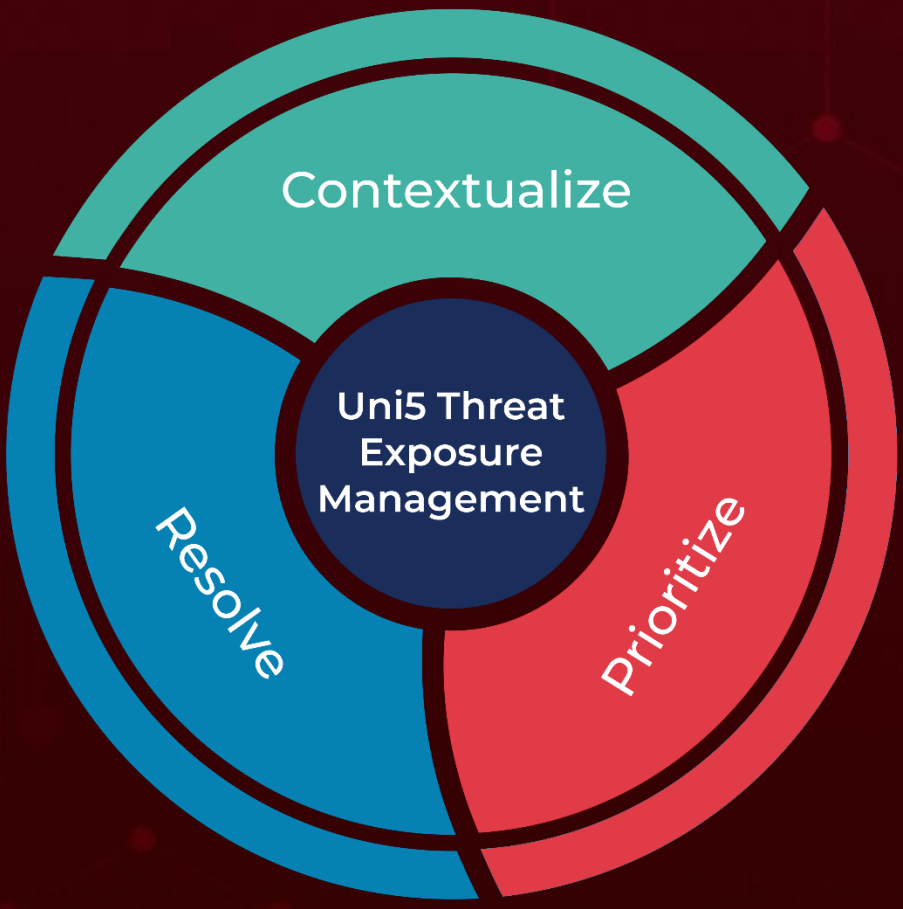
Attack Name	TYPE	VALUE
Cactus	SHA256	23d62b71af79a0e6aed11e378f810613b349361b09faf975dca9e2d202dd3b66, 6007ed278f1cb22cfae95dcc4684ae157435ea759ee7b972de3d5e039695b189, b705636ed4a0d5253e5f9a4e4712c080bfd22403672fc3bca000745022909c96

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

April 28, 2025 • 10:00 PM

More at www.hivepro.com