Date of Publication
April 07, 2025

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

31 MARCH to 06 APRIL 2025

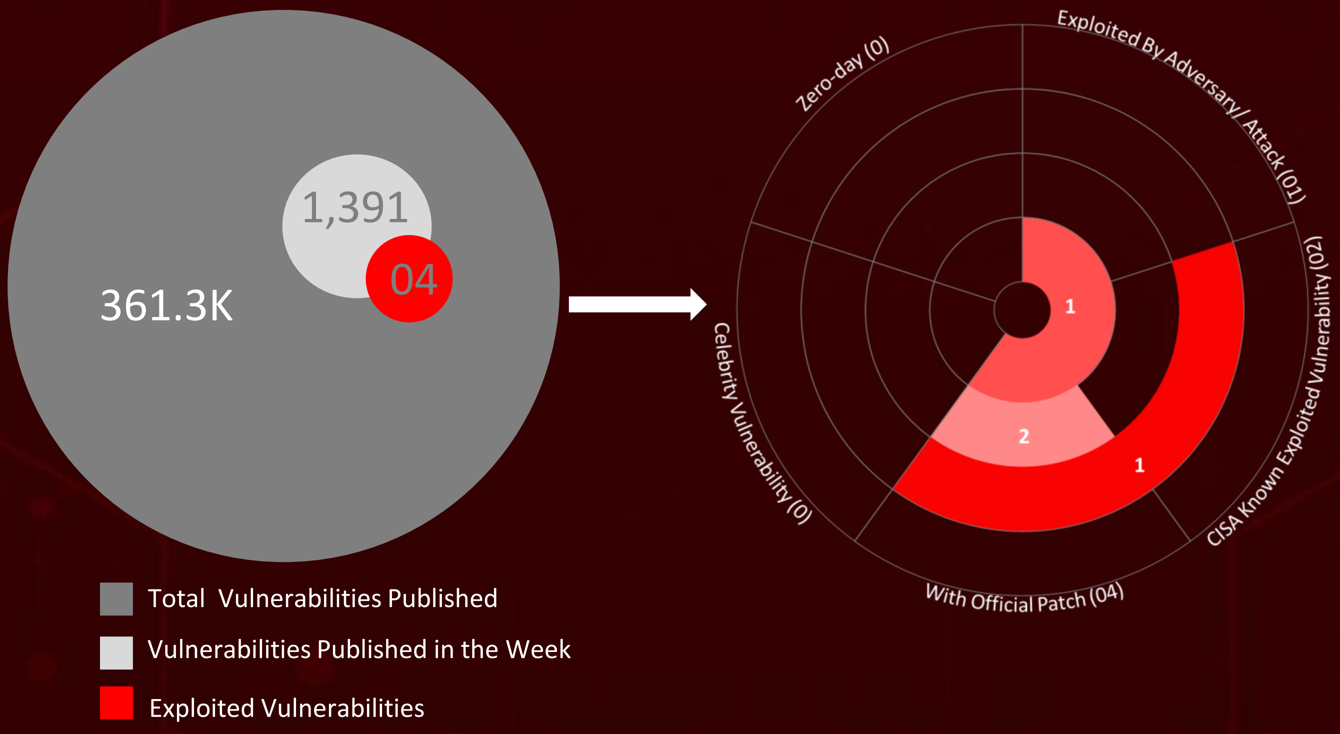
Table Of Contents

Summary

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

CrushFTP, a widely used file transfer server software, has come under intense scrutiny due to a newly discovered critical vulnerability **CVE-2025-31161**. What makes this threat particularly alarming is its active exploitation in the wild, with over **1,500** known instances still left unpatched and open to compromise. Meanwhile, the elusive China-linked APT group known as **Earth Alux** is stirring the cyberespionage landscape with almost undetectable intrusions. This group has set its sights on strategically vital sectors across the Asia-Pacific and Latin American regions.

Adding to the growing list of cyber threats, Ivanti has revealed a severe security flaw **CVE-2025-22457** that has been actively exploited since mid-March. Suspected Chinese threat actors have been leveraging this vulnerability to deliver custom-built malware strains, signaling a coordinated and persistent campaign. These escalating threats highlight the increasing sophistication of cyber adversaries and reinforce the urgent need for proactive, resilient cybersecurity measures to combat the rapidly evolving global threat landscape.



High Level Statistics

11
Attacks Executed

- GODZILLA
- VARGEIT
- RAILLOAD
- MASQLOADER
- GolangGhost
- FrostyFerret
- TRAILBLAZE
- BRUSHFIRE
- SPAWNSNARE
- SPAWNWAVE
- SPAWNSLOTH

4
Vulnerabilities Exploited

- CVE-2025-31161
- CVE-2025-22457
- CVE-2024-20439
- CVE-2024-20440

3
Adversaries in Action

- Earth Alux
- Lazarus
- UNC5221

Insights

CrushFTP Under Siege: Critical Flaw Exposes **1,500+** Servers

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

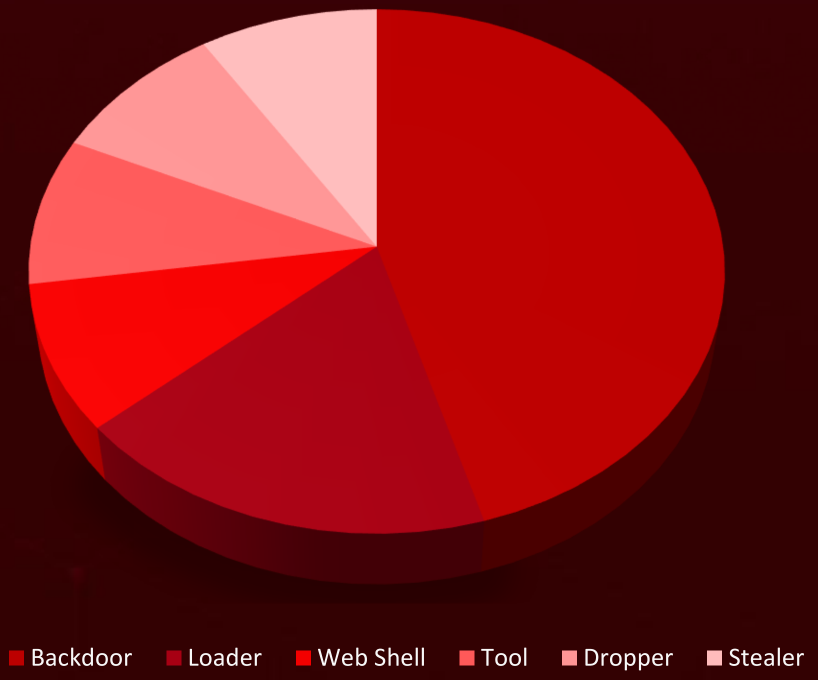
From APAC to Latin America: Earth Alux's Espionage Trail Expands

Malware Ops Intensify: Ivanti Products Used as Entry Points

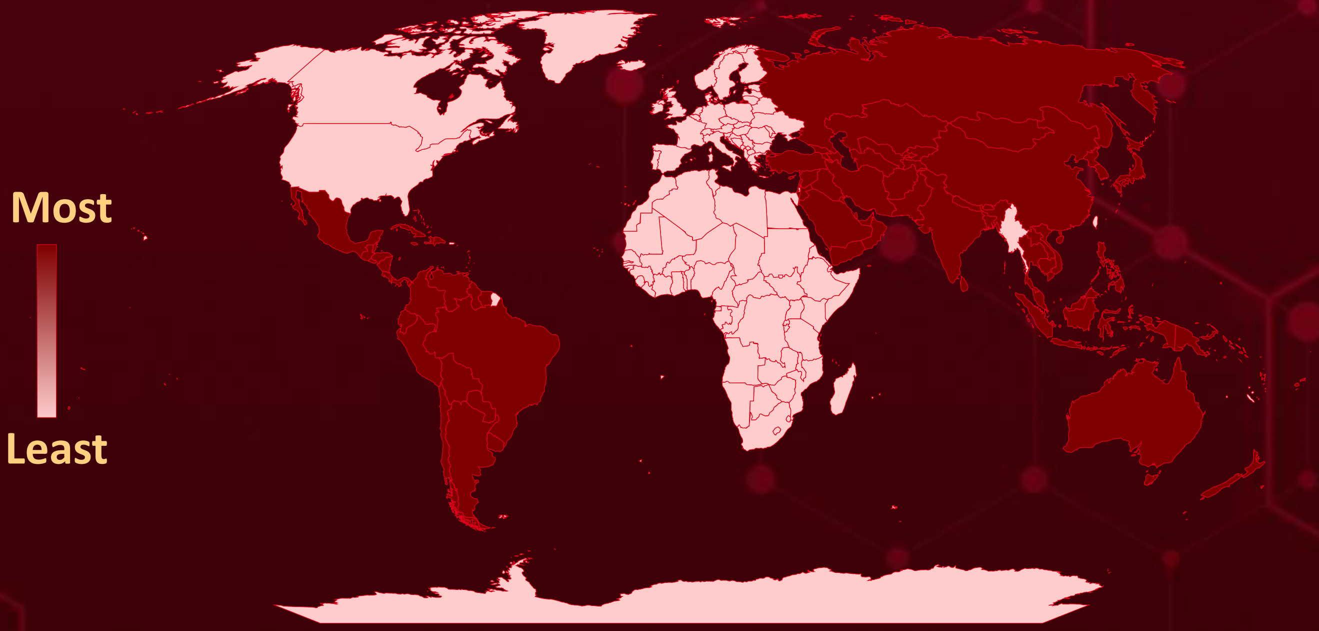
A Trojan in the Interview Room: ClickFix Campaign Targets Tech Professionals

Unauthenticated Attackers Could Strike: Cisco Vulnerabilities Go Live

Threat Distribution



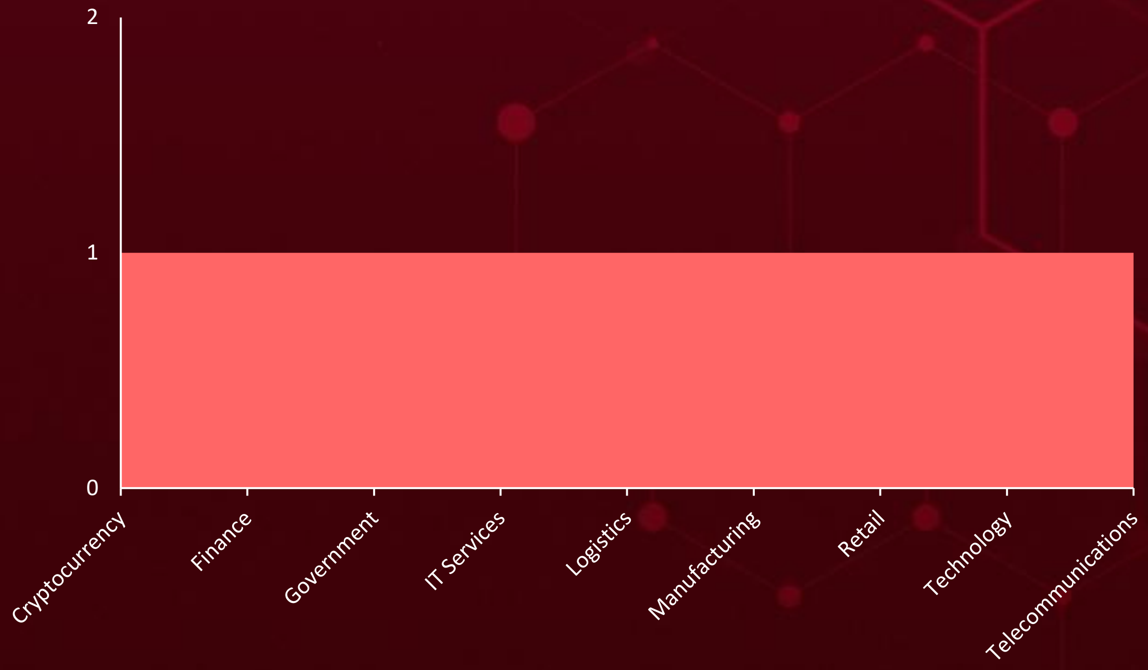
Targeted Countries



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

	Countries		Countries		Countries		Countries
🟥	Panama	🟥	Brazil	🟥	Nicaragua	🟥	Uruguay
🟥	Vietnam	🟥	Pakistan	🟥	Grenada	🟥	Kuwait
🟥	Tajikistan	🟥	Brunei	🟥	Oman	🟥	Vanuatu
🟥	Antigua and Barbuda	🟥	Paraguay	🟥	Guatemala	🟥	Kyrgyzstan
🟥	Nauru	🟥	Cambodia	🟥	Palau	🟥	Laos
🟥	Argentina	🟥	Russia	🟥	Guyana	🟥	Yemen
🟥	Samoa	🟥	Chile	🟥	Papua New Guinea	⬜	Rwanda
🟥	Armenia	🟥	Singapore	🟥	Haiti	⬜	Hungary
🟥	United Arab Emirates	🟥	China	🟥	Peru	⬜	Kenya
🟥	Australia	🟥	Suriname	🟥	Honduras	⬜	Congo
🟥	Marshall Islands	🟥	Colombia	🟥	Qatar	⬜	Croatia
🟥	Azerbaijan	🟥	Timor-Leste	🟥	India	⬜	Sudan
🟥	North Korea	🟥	Costa Rica	🟥	Saint Lucia	⬜	Angola
🟥	Bahamas	🟥	Turkmenistan	🟥	Indonesia	⬜	Ireland
🟥	Philippines	🟥	Cuba	🟥	Saudi Arabia	⬜	Albania
🟥	Bahrain	🟥	Uzbekistan	🟥	Iran	⬜	Portugal
🟥	South Korea	🟥	Cyprus	🟥	Solomon Islands	⬜	Latvia
🟥	Bangladesh	🟥	Lebanon	🟥	Iraq	⬜	Czechia
🟥	Trinidad and Tobago	🟥	Dominica	🟥	Sri Lanka	⬜	Sierra Leone
🟥	Barbados	🟥	Afghanistan	🟥	Israel	⬜	Lesotho
🟥	Venezuela	🟥	Dominican Republic	🟥	Syria	⬜	South Sudan
🟥	Belize	🟥	Maldives	🟥	Jamaica	⬜	Liberia
🟥	Malaysia	🟥	Ecuador	🟥	Thailand	⬜	Canada
🟥	Bhutan	🟥	Mexico	🟥	Japan	⬜	Chad
🟥	Micronesia	🟥	El Salvador	🟥	Tonga	⬜	Zambia
🟥	Bolivia	🟥	Mongolia	🟥	Jordan	⬜	United Kingdom
🟥	New Zealand	🟥	Fiji	🟥	Turkey	⬜	Denmark
		🟥	Nepal	🟥	Kazakhstan	⬜	Germany
		🟥	Georgia	🟥	Tuvalu	⬜	Luxembourg

Targeted Industries



TOP MITRE ATT&CK TTPs

T1190
Exploit Public-Facing Application

T1588.005
Exploits

T1588
Obtain Capabilities

T1027
Obfuscated Files or Information

T1588.006
Vulnerabilities

T1082
System Information Discovery

T1059
Command and Scripting Interpreter

T1041
Exfiltration Over C2 Channel

T1070
Indicator Removal

T1036
Masquerading

T1070.004
File Deletion

T1068
Exploitation for Privilege Escalation

T1204
User Execution

T1574.002
DLL Side-Loading

T1556
Modify Authentication Process

T1547
Boot or Logon Autostart Execution

T1055
Process Injection

T1567
Exfiltration Over Web Service

T1057
Process Discovery

T1059.007
JavaScript

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GODZILLA	GODZILLA is a web shell that delivers first-stage backdoors, operating entirely in memory to evade traditional disk-based detection methods. It uses AES encryption for secure communication, making detection even more challenging.	Exploiting Vulnerabilities in Exposed Servers	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Evasion of Detection, Increased Risk of Further Attacks	Windows
Web Shell			
ASSOCIATED ACTOR			**PATCH LINK**
Earth Alux			-
IOC TYPE	**VALUE**		
SHA256	245fdb5e35b6f51b26d4cf3999a40dde13987240f9bf565fe03a1f6adb9da9b2		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
VARGEIT	VARGEIT is a primary backdoor executed via shellcode injection using a debugger script. It enables attackers to collect system and drive information, gather data on running processes, and interact with the Windows Defender Firewall. VARGEIT also allows for directory management, including creating, setting, searching, and deleting directories, as well as reading from and writing to files. Additionally, it can execute command lines and inject miscellaneous tools into controlled instances of mspaint or conhost.	GODZILLA facilitates the delivery	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Tool Injection into Controlled Processes, Unauthorized Directory Management	Windows
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
Earth Alux			-
IOC TYPE	**VALUE**		
SHA256	28517bff286ade02b81da52f9fcddcb9764023ae7035bc593d081fdd2a8c85d9		

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 rowspan="3">RAILLOAD</td><td rowspan="7">RAILLOAD is a loader component with a base64-encoded configuration. Its decryption process involves first decoding the base64 string, followed by AES-128 CBC mode decryption. In some variants, RAILLOAD includes execution guardrails to control its operation.</td><td>VARGEIT deploys via DLL side-loading</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td rowspan="5">Increased Attack Surface, Evasion of Detection</td><td rowspan="3">Windows</td></tr>
<tr><th>TYPE</th></tr>
<tr><td>Loader</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>Earth Alux</td><td>-</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">00a41c8272d405ba85ae9d0e435e3030033e8a032f3d762367d0a57d41524f3a,
0d3ec88b0bfa5530e45dec75dfbea7ae683bdea91105b5f90a787beaabd1ef27,
0f6fe5d0ee754d581d4a8d989e83272b121d0125bd3c77e57a6b14db23f425ab</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="3">MASQLOADER</td><td rowspan="7">MASQLOADER is a loader that, in recent versions, incorporates an anti-API hooking technique. It achieves this by overwriting the code section of ntdll.dll in memory with the original code from the file, effectively removing any API hooks inserted by security and monitoring tools. This method enables MASQLOADER and the injected payload to evade detection by circumventing monitoring tools that rely on intercepted API calls.</td><td>Side-loaded DLL or shellcode</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td rowspan="5">Bypasses Security Measures, Enabling Further Exploitation</td><td rowspan="3">Windows</td></tr>
<tr><th>TYPE</th></tr>
<tr><td>Loader</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>Earth Alux</td><td>-</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">8b0023248bc037631b26694f34d7bc8163e2d5f5919fe61f3dbc1354f87d6792</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 CVEs
GolangGhost	GolangGhost is an interpreted Go backdoor crafted for remote control and data exfiltration, specifically targeting Windows and macOS systems. It features the ability to steal data from Chrome browsers and, once the victim is registered with the command-and-control (C2) server, it can execute a range of commands.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Remote Control, Chrome Browser Data Theft	Windows, macOS
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus Group			-

IOC TYPE	VALUE
SHA256	0cbbf7b2b15b561d47e927c37f6e9339fe418badf49fa5f6fc5c49f0dc981100, ef9f49f14149bed09ca9f590d33e07f3a749e1971a31cb19a035da8d84f97aa0, 6e186ada6371f5b970b25c78f38511af8d10faaeaed61042271892a327099925

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

IOC TYPE	VALUE
SHA256	b7b9e7637a42b5db746f1876a2ecb19330403ecb4ec6f5575db4d94df8ec79e8

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>TRAILBLAZE</td><td rowspan="5">TRAILBLAZE is a minimal, in-memory-only dropper written in raw C, utilizing syscalls to ensure it remains compact enough to fit within a shell script as Base64.</td><td>Exploiting vulnerabilities</td><td>CVE-2025-22457</td></tr>
<tr><th>TYPE</th><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>Dropper</td><td rowspan="3">Evasion of Detection, System Compromise</td><td>Ivanti Connect Secure, Policy Secure, and ZTA Gateways</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>UNC5221</td><td>https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>MD5</td><td colspan="3">4628a501088c31f53b5c9ddf6788e835</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>BRUSHFIRE</td><td rowspan="5">BRUSHFIRE is a passive backdoor written in C that hooks into the SSL_read function. It first executes the original SSL_read, checks if the returned data starts with a specific string, and if so, XOR decrypts and runs the contained shellcode. If the shellcode returns a value, the backdoor sends it back using SSL_write.</td><td>Exploiting vulnerabilities</td><td>CVE-2025-22457</td></tr>
<tr><th>TYPE</th><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>Backdoor</td><td rowspan="3">Data Exfiltration, Remote Access</td><td>Ivanti Connect Secure, Policy Secure, and ZTA Gateways</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>UNC5221</td><td>https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>MD5</td><td colspan="3">e5192258c27e712c7acf80303e68980b</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
SPAWNSNARE	SPAWNSNARE is a C-based utility designed for Linux that extracts the uncompressed Linux kernel image and encrypts it using AES without requiring any command-line tools.	Exploiting vulnerabilities	CVE-2025-22457
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Tool		Exposure of sensitive system information	Ivanti Connect Secure, Policy Secure, and ZTA Gateways
ASSOCIATED ACTOR			**PATCH LINK**
UNC5221			https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457

IOC TYPE	VALUE
MD5	6e01ef1367ea81994578526b3bd331d6

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

IOC TYPE	VALUE
MD5	ce2b6a554ae46b5eb7d79ca5e7f440da

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

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

IOC TYPE	VALUE
MD5	10659b392e7f5b30b375b94cae4fdca0

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-2025-31161	☒	CrushFTP versions 10.0.0 through 10.8.3 and 11.0.0 through 11.3.0	-
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:crushftp:crushftp:*:*:*:*:*:*:*	-
CrushFTP Authentication Bypass Vulnerability	☒		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-287	T1556: Modify Authentication Process	https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update, https://www.crushftp.com/download.html

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

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

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

Adversaries in Action

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

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

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

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1204: User Execution; T1204.001: Malicious Link; T1555: Credentials from Password Stores; T1555.001: Keychain; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1059.005: Visual Basic; T1059.004: Unix Shell; T1059.003: Windows Command Shell; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1217: Browser Information Discovery; T1071: Application Layer Protocol; T1036: Masquerading; T1027: Obfuscated Files or Information; T1560: Archive Collected Data; T1041: Exfiltration Over C2 Channel; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1082: System Information Discovery

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

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actors **Earth Alux, Lazarus, UNC5221,** and malware **GODZILLA, VARGEIT, RAILLOAD, MASQLOADER, GolangGhost, FrostyFerret, TRAILBLAZE, BRUSHFIRE, SPAWNSNARE, SPAWNWAVE, SPAWNSLOTH.**

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 **four exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Earth Alux, Lazarus, UNC5221,** and malware **MASQLOADER, GolangGhost** in Breach and Attack Simulation(BAS).

Threat Advisories

Patch Now: CrushFTP Authentication Bypass Actively Exploited

Earth Alux the Cyber Threat Hiding in Plain Sight

ClickFake Interview: Lazarus Group’s New Crypto Heist via Fake Job Offers

CVE-2025-22457: Hackers Actively Exploiting Ivanti’s Critical New Flaw

Cisco Smart Licensing Utility Vulnerabilities Exploited in the Wild

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
GODZILLA	SHA256	245fdb5e35b6f51b26d4cf3999a40dde13987240f9bf565fe03a1f6adb9da9b2
VARGEIT	SHA256	28517bff286ade02b81da52f9fcddcb9764023ae7035bc593d081fdd2a8c85d9, 43e5c3d6182ab6d9d71b5892c5087b4ef4b3093126bcdf4ebcef0b15e04e0c03, 4be6f5e76ea02ae348b26fc32a0dabe009d05b701e53270cf40ca50fa76197b0, a14e226a50c12e637e8b280ad688e5637db752c72d0f8b2bac5f2d3d487e1c21, a9804fa05845707f094fe91668a5c3792f2441d371816b46fbe636953fc5787d, b8e1a46146c09ef54b802a6989b485ef5982a86228a24ec0839ec5af7b42e648, b9fefe3946d0c9e000262a10b184090da45925f24b7dfc9d25abe63bc55ca7ed, d692c85da91bb5e5724f520ca392b68eee144a3719a7441c779c8ce73d3b25dc
RAILLOAD	SHA256	00a41c8272d405ba85ae9d0e435e3030033e8a032f3d762367d0a57d41524f3a, 0d3ec88b0bfa5530e45dec75dfbea7ae683bdea91105b5f90a787beaabd1ef27, 0f6fe5d0ee754d581d4a8d989e83272b121d0125bd3c77e57a6b14db23f425ab, 13e0aef0ab6d218e68c5c5b6008872eb73104f161c902511aec3df5bce89136e, 16509adf92b1ac3097452affd8dda640936c8a40272592b978db3698487df5fa,

Attack Name	TYPE	VALUE
RAILLOAD	SHA256	19bcca292814942f2fe8d142a679cc6a97fa6cbf77a0c98873146e918013bb5c, 1c8c14251710fbdef994d9ccf1d3507cf0ef5cd6c7d3495af2adfe7f97cc0dc2, 1c93ba375016bcb41b915b78eb4ab023ecf456e240823a1d6d2b5297b3523956, 281fc3aff361f202a41f4aff84a5f61e5728fd8ea0c1219a8bca540a959a4ee2, 2971a53769745c107a89eeb5f48e3b3e9680d371bf06b028c7769c961e6f9e55, 3129bfad321be526f231c64aac10d7d8f416dc14cab11c1bbc57252c75823959, 3b7c29489c1feaafc587eac0ffcca79964259c9687d86a5cce5ea70261f7439b, 3f0157cfb493df1cd051cc87364c7bdbe3719927335b76b7c567b369ab47b3be, 41410a8aa4a4fcd811ef67ba023e263f4cd6667039b01547d23a3eb758d97b96, 442446fbc012847a12448398b619837614498bb611968e64166f0e9040c311db, 455510fe663775e09a2d0bbfdc4c8ec2e26665e10f9599b05dc59ea460f06ac8, 47ea0392ec123e3949b9ae2638b9078cd5efd4da942e38f149ccfb74d8e70123, 529e691a9d60b8ae0c64de82402e76c112df3bc27be5f2e94ee58252a67804a1, 52c8eacbcc8906036894a3a11cb4181d454c3a4f685500a799263cdcf6c6d88e, 5502735d81accb96c58300d1e21765b8b53a4749aad68e513b2558ed79f83cc4, 5518b542afd9d456ee8dea4dec3e0e8a98a42982b33f8f629d3d8edeca0dbf4d, 55b4e3814a349c9de4c99237f62d42787a6fef64b809db9cf52cfe0602cac01e, 5872da9dfd5ed3c0b9e0a05466a56c6ac6966012b5b3e14ac43a1225ba5e6bb2, 5aaca0994795ba7da0f10cd393ac32cc1e78c9afd4e9d09bbbe430f168c0eebe, 5d358bcd0acb999fdec332f0a2d1fe51952542f0836b9618ab18f253597d244c, 5dcd5cb720a40692b7e49540a42f1d12e831aaab369d9fe31a66b0433b825264, 62d71b61af750ad3b763d98504a174a1949a359a4cb4f6ce2795b7b3240919eb, 67dddc4ce777df1baa19acb1c3535eb01a54f24516a85312bafe4cba11d74483, 681e9aab60b1c64dacbc7c8574d294333b9cd4494ec683b0c780866c3e1e7d40, 762525805afe6a0891275ebc2ae1f067e9aad8f310afc0b1ad800cc980ed8b55,

Attack Name	TYPE	VALUE
RAILLOAD	SHA256	7654e7f7076f07e76ae478c1df65f1711918ad4f36c45f520cc46cdcb1128cc2, 7ad44f7e1f78ee83f20da498584ec7138c2514580ddfe62698be7587ae2678e1, 83968575244ab2e44a5b94423bb1cacd10bb293ddcbbddbc2fc117f9335b6e78, 846be29c140850fd9524339acd67eac4b84bc59ed056544356d199226452ea88, 85f9bac9eefb5fbc1e51508ce12cda10a69d8bde82952891081b19d6833297ab, 86e2d56761fb4dc16c7b0cd8da241c9899af851f5df751ffc67a2d68062e71f4, 86f5f088cf997766e52860b57506ba0923454a63bee39e4e3de2fb98c4fee240, 8c89362d4bed8bd2f0fbffc450bca4e7666fc7a3e88ec56a5dd149593fd697ec, 91034c01e800b116095eecdb073a5262852fc2c788f9fcd09259d6c09ce88ac6, 9366ece5ff9082145184adb2e91053d5e0d68d4d9f9a9f054aad68b8e7368443, 9b5e6c2f287ea7931bb27f63111ef0035265bc27751f01bd6c7f3dd3395bbaf5, 9d9f40c6c2dc14118452f7f1b56346e60a8681fb83300e4292576e635b37f9c8, 9f94bb59bfc32958a15cd8e225f270802bd9e14929e5d0f4f488842710a361ea, a042157e7460f6c28c984a1c1f3803521a556c67e26411854e497685ef436325, a79679d8f9551810504ff316465fb289d1ac64dc52bcaabd70267217d33d603c, a845cb84ea11f0fa7a982407705e892f58d7cb407eadc5329416464cccdd6a23, ab6145f1ea6c8a682bea289cef06c0f27fa076b8f88a89a2631167541fc835e9, ac70d98af57d9e3da9ee485a4ab1badbb28e89d15c4ef2df521423881a147e43, afd83d598843f93f7cad02bbe8467da2f257b5344600090034bb795844f05bdc, b0a42d1c5a07bbe317a034e204c0eb64ae5d99e3dfbfbd9b3b098caea4b19f96, b32dd5d549bcf4b674b4e7cf5481064b38ea614c666b158afedc7084b715c1fa, b92452a6c2cd13193a6df88278c31c85008acf448655c18389c84b353026d15e, ba0105c8fa99b8f3a82c32d20e94031f22e277286b738db529e763955df248dc, bd0dbf799e98137238ae38f134c7af82d7ff673c0a418044add0220211d98a27, be01089ad2c2e7af32677ec0a7a9a541dee1cb149639d60fb7b7e9b641d2ccdb,

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

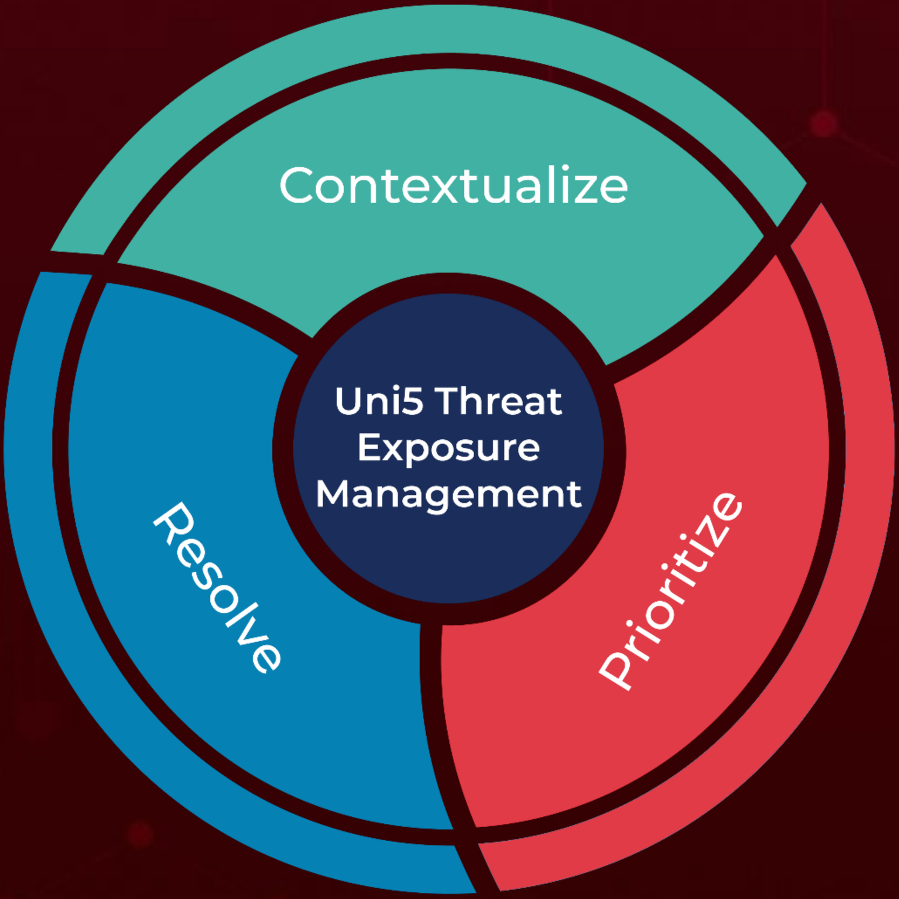
Attack Name	TYPE	VALUE
TRAILBLAZE	MD5	4628a501088c31f53b5c9ddf6788e835
	File Path	/tmp/.i
BRUSHFIRE	File Path	/tmp/.r
	MD5	e5192258c27e712c7acf80303e68980b
SPAWNSNARE	MD5	6e01ef1367ea81994578526b3bd331d6
	File Path	/bin/dsmain
SPAWNWAVE	MD5	ce2b6a554ae46b5eb7d79ca5e7f440da
	File Path	/lib/libdsupgrade.so
SPAWNSLOTH	File Path	/tmp/.liblogblock.so
	MD5	10659b392e7f5b30b375b94cae4fdca0

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 07, 2025 • 4:00 AM

More at www.hivepro.com