Date of Publication
January 27, 2025

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

20 to 26 January 2025

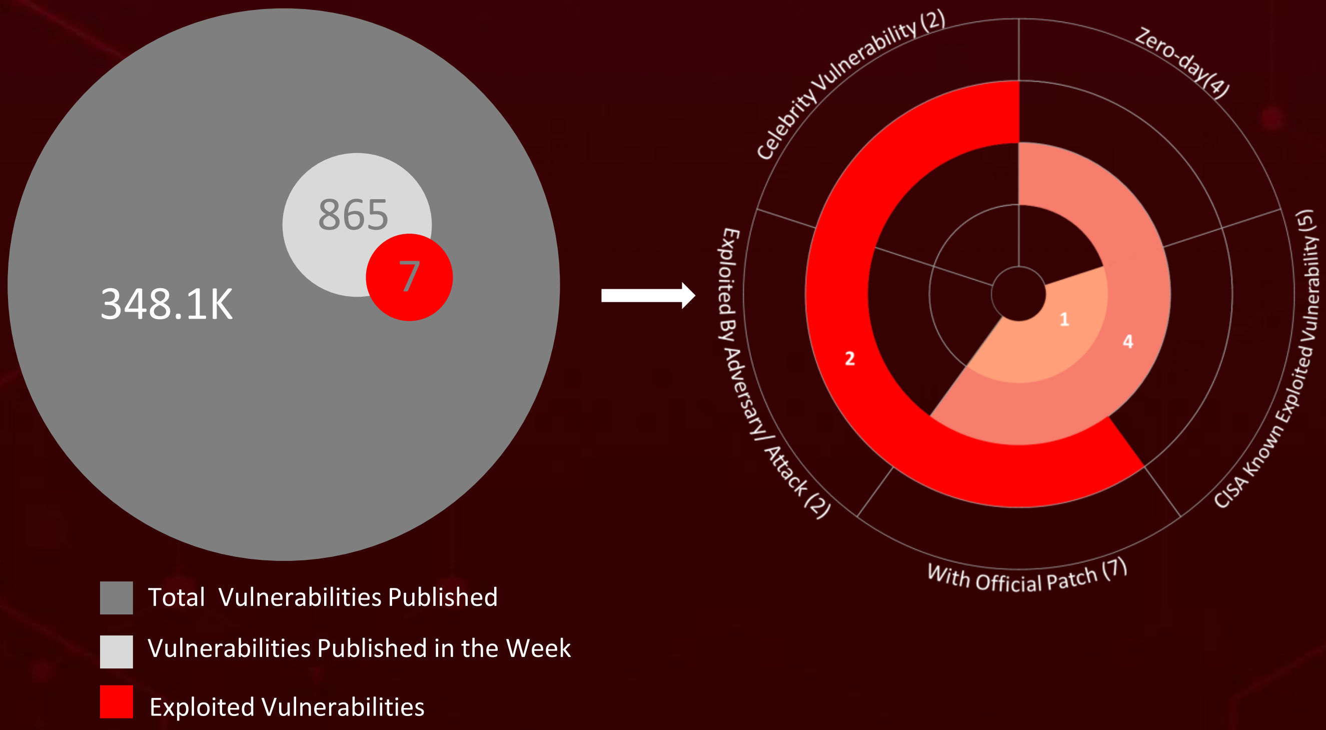
Table Of Contents

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, detected **three** attacks, reported **seven** vulnerabilities, and identified **five** active adversaries. These findings underscore the relentless and escalating danger of cyber intrusions.

Additionally, the Russian threat actor **Star Blizzard** has launched a new spear-phishing campaign, using WhatsApp group invitations as lures to compromise accounts, marking a shift in their tactics. **CVE-2024-55591**, a **zero-day** in FortiOS and FortiProxy, allows attackers to bypass authentication and gain super-admin access.

Furthermore, this week, Ransomware gangs **STAC5143** and **STAC5777** combine email bombing with Microsoft Teams impersonation, posing as IT support to exploit default settings, gain remote access, and deploy malware and ransomware. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

3
Attacks Executed

7
Vulnerabilities Exploited

5
Adversaries in Action

- Silver
- Resocks Toolkit
- SlowStepper

- CVE-2024-49113
- CVE-2024-49112
- CVE-2024-55591
- CVE-2025-21333
- CVE-2025-21334
- CVE-2025-21335
- CVE-2025-23006

- Star Blizzard
- Silent Lynx APT
- STAC5143
- STAC5777
- PlushDaemon

Insights

A **supply chain attack** compromised over a dozen **Chrome extensions**, using phishing to target developers and harvest sensitive data

PlushDaemon China-aligned APT uses its advanced SlowStepper backdoor for stealthy supply-chain attacks, including a 2023 hit on a South Korean VPN provider.

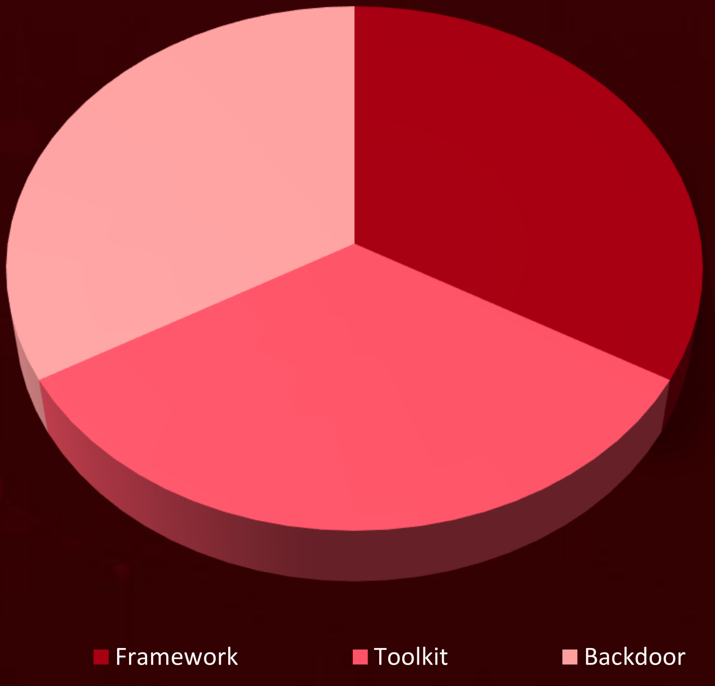
SonicWall fixed the critical **CVE-2025-23006** flaw in its SMA 1000 Series, allowing remote attackers to execute arbitrary commands.

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

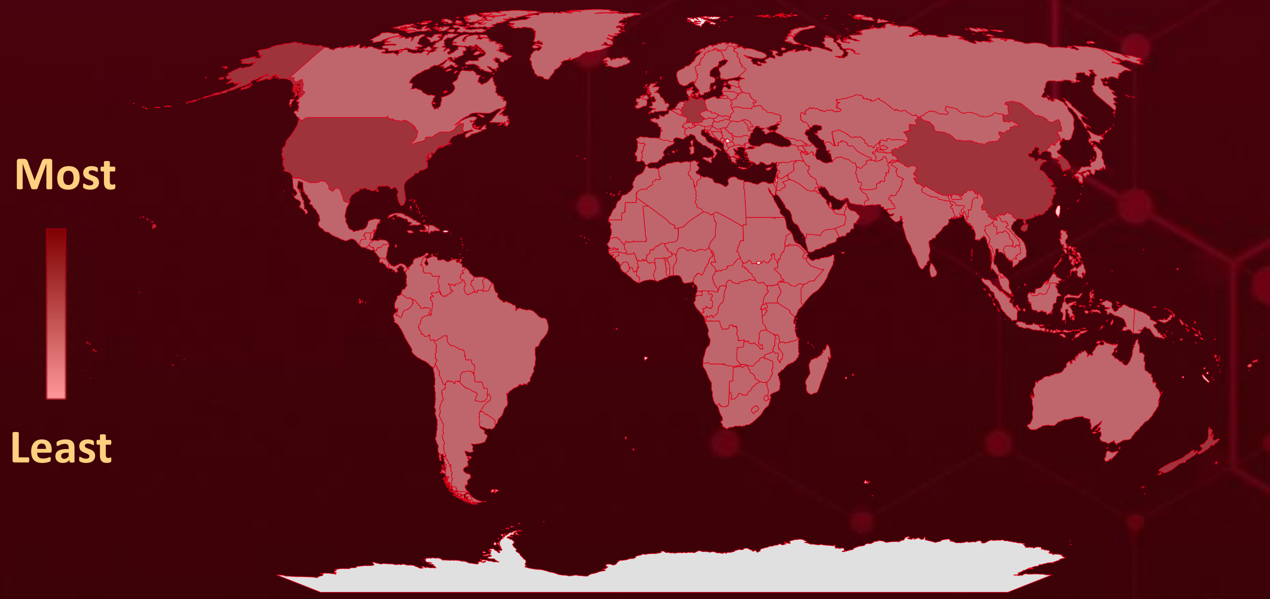
Silent Lynx APT targeted Kyrgyzstan's National Bank and Ministry of Finance with phishing campaigns, using malicious payloads and Telegram bots for espionage.

Sliver malware targets German organizations, using fake LNK files and DLL techniques for hidden access.

Threat Distribution



Targeted Countries



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

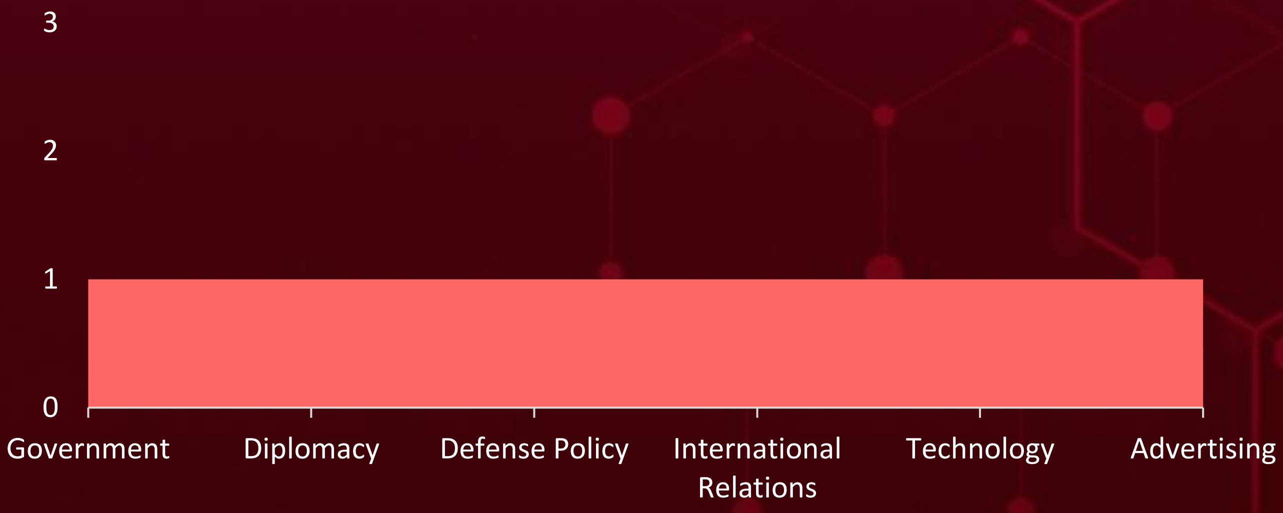
Countries
New Zealand
Germany
South Korea
China
United States
Pakistan
Lithuania
Spain
Argentina
Montenegro
Armenia
Samoa
Australia
Tunisia
Austria
Marshall Islands
Azerbaijan
Andorra
Bahamas
Portugal
Bahrain
Singapore
Bangladesh
Syria
Barbados
Vietnam
Equatorial Guinea

Countries
Belarus
Malaysia
Belgium
Micronesia
Belize
Namibia
Benin
North Korea
Bhutan
Paraguay
Bolivia
Russia
Bosnia and Herzegovina
Senegal
Botswana
Somalia
Brazil
Sudan
Brunei
Timor-Leste
Bulgaria
Uganda
Burkina Faso
Afghanistan
Guinea-Bissau
Burundi

Countries
Madagascar
Cabo Verde
Mali
Cambodia
Mauritius
Cameroon
Monaco
Canada
Mozambique
Central African Republic
Nepal
Chad
Niger
Chile
Norway
Albania
Panama
Colombia
Philippines
Comoros
Republic of the Congo
Congo
Saint Kitts & Nevis
Costa Rica
El Salvador
Malawi

Countries
Sao Tome & Principe
Côte d'Ivoire
Seychelles
Croatia
Slovenia
Cuba
Angola
Cyprus
St. Vincent & Grenadines
Czech Republic (Czechia)
Sweden
Denmark
Tanzania
Djibouti
Tonga
Dominica
Turkmenistan
Dominican Republic
United Arab Emirates
DR Congo
Zambia
Ecuador
Liechtenstein
Egypt
Luxembourg

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1195** Supply Chain Compromise	**T1566** Phishing	**T1204** User Execution	**T1588** Obtain Capabilities
T1566.001 Spearphishing Attachment	**T1588.006** Vulnerabilities	**T1190** Exploit Public-Facing Application	**T1204.002** Malicious File	**T1140** Deobfuscate/ Decode Files or Information
T1041 Exfiltration Over C2 Channel	**T1059.001** PowerShell	**T1204.001** Malicious Link	**T1036** Masquerading	**T1027** Obfuscated Files or Information
T1547 Boot or Logon Autostart Execution	**T1068** Exploitation for Privilege Escalation	**T1059.005** Visual Basic	**T1574** Hijack Execution Flow	**T1071.001** Web Protocols

Attacks Executed

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

IOC TYPE	VALUE
SHA256	f778825b254682ab5746d7b547df848406bb6357a74e2966b39a5fa5eae006c2, 83a70162ec391fde57a9943b5270c217d63d050aae94ae3efb75de45df5298be

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

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

IOC TYPE	VALUE
SHA256	297d1afa309cdf0c84f04994ffd59ee1e1175377c1a0a561eb25869909812c9c

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

IOC TYPE	VALUE
SHA256	40df05b4f04ad093b31c9ca07a559be56a700e49f6051b5cb7462db5f85be8c3
SHA1	068fd2d209c0bbb0c6fc14e88d63f92441163233
MD5	e2bc2361ead7c80eba86a5d1c492865d
Domains	7051[.]gsm[.]360safe[.]company, st[.]360safe[.]company

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

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

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

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21334	✗	Windows: 10 - 11 24H2 Windows Server 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21334

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21335	✗	Windows: 10 - 11 24H2 Windows Server 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Star Blizzard (aka Cold River, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto, UNC4057)	Russia	Government, Diplomacy, Defense Policy, International Relations	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs
TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0008: Lateral Movement; TA0010: Exfiltration; T1566: Phishing; T1566.002: Spearphishing Link; T1598: Phishing for Information; T1598.003: Spearphishing Link; T1036: Masquerading; T1589: Gather Victim Identity Information; T1534: Internal Spearphishing; T1078: Valid Accounts; T1585: Establish Accounts; T1585.001: Social Media Accounts; T1204: User Execution; T1204.001: Malicious Link; T1176: Browser Extensions; T1656: Impersonation

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Silent Lynx APT	Iran	Government banks, think tanks, embassies, legal entities	Central Asia and Special Programme for the Economies of Central Asia (SPECA) based nations
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Resocks Toolkit	Windows

TTPs

TA0043: Reconnaissance; TA0006: Credential Access; T1589.002: Email Addresses; T1078.002: Domain Accounts; T1547.001: Registry Run Keys / Startup Folder; T1552.001: Credentials In Files; T1046: Network Service Discovery; T1007; TA0003: Persistence; TA0007: Discovery; T1589: Gather Victim Identity Information; T1078: Valid Accounts; T1547: Boot or Logon Autostart Execution; T1552; TA0001: Initial Access; TA0009: Collection; T1204.002: Malicious File; T1059.001: PowerShell; TA0002: Execution; TA0010: Exfiltration; T1204: User Execution; T1059: Command and Scripting Interpreter; T1056.001: Keylogging; T1087: Unsecured Credentials; T1012: Query Registry; T1560.001: System Service Discovery Archive via Utility; T1567.002: Exfiltration to Cloud Storage Account Discovery; T1018: Remote System Discovery; T1560: Archive Collected Data; T1056: Input Capture; T1083: File and Directory Discovery; T1016: System Network Configuration Discovery; T1567: Exfiltration Over Web Service

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="6">STAC5143</td><td>Iran</td><td rowspan="3">-</td><td rowspan="3">Worldwide</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><th>TARGETED CVEs</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>-</td><td>Unknown Ransomware</td><td>Windows</td></tr>
<tr></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1090: Proxy; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1049: System Network Connections Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1018: Remote System Discovery; T1482: Domain Trust Discovery; T1656: Impersonation; T1036: Masquerading; T1566: Phishing; T1037: Boot or Logon Initialization Scripts; T1021: Remote Services; T1021.001: Remote Desktop Protocol; T1021.006: Windows Remote Management; T1005: Data from Local System; T1486: Data Encrypted for Impact; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder</td></tr>
</table>

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

TTPs

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

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5">PlushDaemon</td><td>China</td><td rowspan="3">-</td><td rowspan="3">South Korea, China, Taiwan, Hong Kong, United States, New Zealand</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><th>TARGETED CVEs</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>-</td><td>SlowStepper Backdoor</td><td>-</td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583.001: Domains; T1583.004: Server; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.002: Upload Tool; T1588: Obtain Capabilities; T1588.001: Malware; T1588.002: Tool; T1588.003: Code Signing Certificates; T1588.005: Exploits; T1659: Content Injection; T1190: Exploit Public-Facing Application; T1195: Supply Chain Compromise; T1195.002: Compromise Software Supply Chain; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1059.006: Python; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder; T1547.004: Winlogon Helper DLL; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1222: File and Directory Permissions Modification; T1222.001: Windows File and Directory Permissions Modification; T1070: Indicator Removal; T1070.004: File Deletion; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1112: Modify Registry; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1027.013: Encrypted/Encoded File; T1553: Subvert Trust Controls; T1553.002: Code Signing; T1217: Browser Bookmark Discovery; T1083: File and Directory Discovery; T1120: Peripheral Device Discovery; T1057: Process Discovery; T1012: Query Registry; T1518: Software Discovery; T1082: System Information Discovery; T1614: System Location Discovery; T1016: System Network Configuration Discovery; T1016.002: Wi-Fi Discovery; T1033: System Owner/User Discovery; T1560: Archive Collected Data; T1560.002: Archive via Library; T1123: Audio Capture; T1005: Data from Local System; T1074.001: Local Data Staging; T1113: Screen Capture; T1125: Video Capture; T1071.004: DNS; T1132.001: Standard Encoding; T1573.001: Symmetric Cryptography; T1008: Fallback Channels; T1105: Ingress Tool Transfer; T1104: Multi-Stage Channels; T1095: Non-Application Layer Protocol; T1090: Proxy; T1219: Remote Access Software; T1020: Automated Exfiltration; T1041: Exfiltration Over C2 Channel; T1583: Acquire Infrastructure</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seven exploited vulnerabilities** and block the indicators related to the threat actors **Star Blizzard, Silent Lynx APT, STAC5143, STAC5777, PlushDaem** and malware **Silver, Resocks Toolkit, SlowStepper.**

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

- Running a Scan to discover the assets impacted by the **seven exploited vulnerabilities.**

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Star Blizzard** and malware **Silver, Resocks Toolkit, SlowStepper** in Breach and Attack Simulation(BAS).

Threat Advisories

Fake LDAPNightmare Exploit on GitHub Spreads Infostealer Malware

Fortinet Firewalls Under Siege: Exploitation of Critical Zero-Day CVE-2024-55591

Microsoft’s January 2025 Patch Tuesday Fixes Active Zero-Day Exploits

Rsync Vulnerabilities Could Spell Disaster for Over 660,000 Servers

Star Blizzard Launches Spear-Phishing Campaign Targeting WhatsApp

German Entities Under Attack: Sliver Implant Delivered via Malicious LNK Files

Silent Lynx Campaigns Targeting Central Asian Governments

Exploiting Trust: Cybercriminals Abusing Teams Leading to Ransomware Deployment

SonicWall SMA 1000 Faces Active Exploitation of Critical Vulnerability

Supply-Chain-Attack-on-Chrome-Browser-Extensions

PlushDaemon’s Supply Chain Heist That Shook South Korea

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.

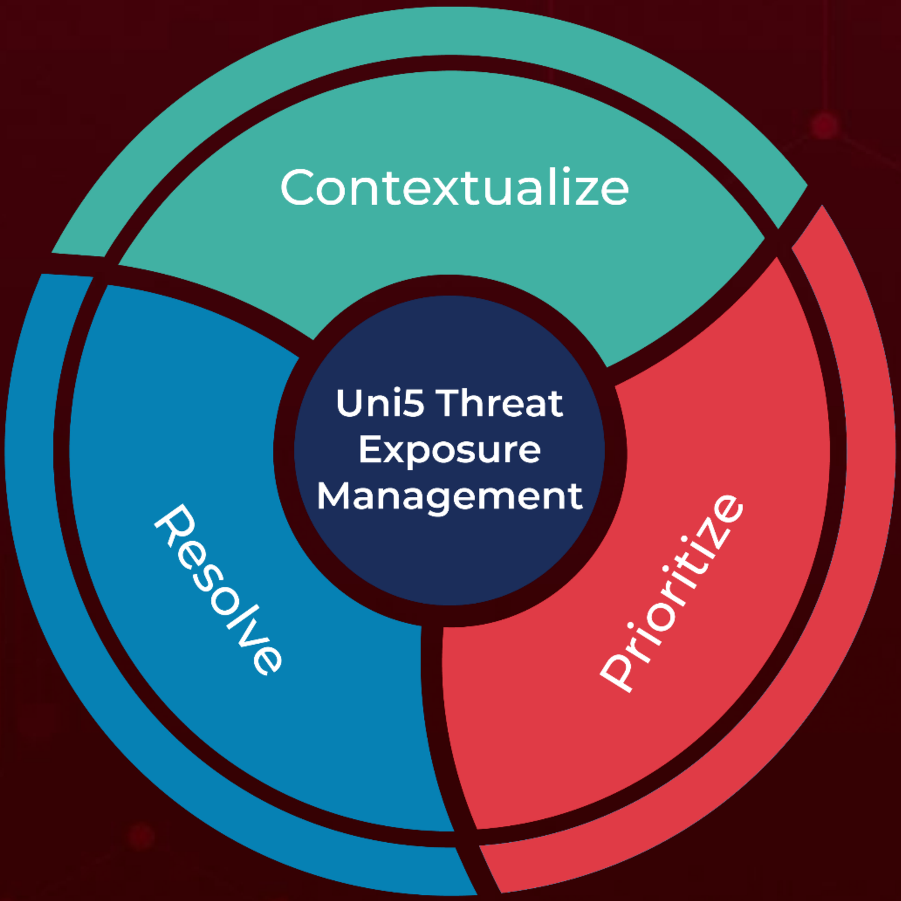
Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Silver	SHA256	f778825b254682ab5746d7b547df848406bb6357a74e2966b39a5fa5eae006c2, 83a70162ec391fde57a9943b5270c217d63d050aae94ae3efb75de45df5298be
Resocks Toolkit	SHA256	297d1afa309cdf0c84f04994ffd59ee1e1175377c1a0a561eb25869909812c9c
SlowStepper	SHA256	40df05b4f04ad093b31c9ca07a559be56a700e49f6051b5cb7462db5f85be8c3
	SHA1	068fd2d209c0bbb0c6fc14e88d63f92441163233
	MD5	e2bc2361ead7c80eba86a5d1c492865d
	Domains	7051[.]gsm[.]360safe[.]company, st[.]360safe[.]company
	IPv4	8[.]130[.]87[.]195 47[.]108[.]162[.]218 47[.]113[.]200[.]18, 202[.]105[.]1[.]187, 47[.]74[.]159[.]166, 47[.]104[.]138[.]190, 120[.]24[.]193[.]58, 202[.]189[.]8[.]87, 202[.]189[.]8[.]69, 202[.]189[.]8[.]193, 47[.]92[.]6[.]64

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

January 27, 2025 • 7:45 AM

More at www.hivepro.com