Date of Publication
November 10, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

03 to 09 NOVEMBER 2025

Table Of Contents

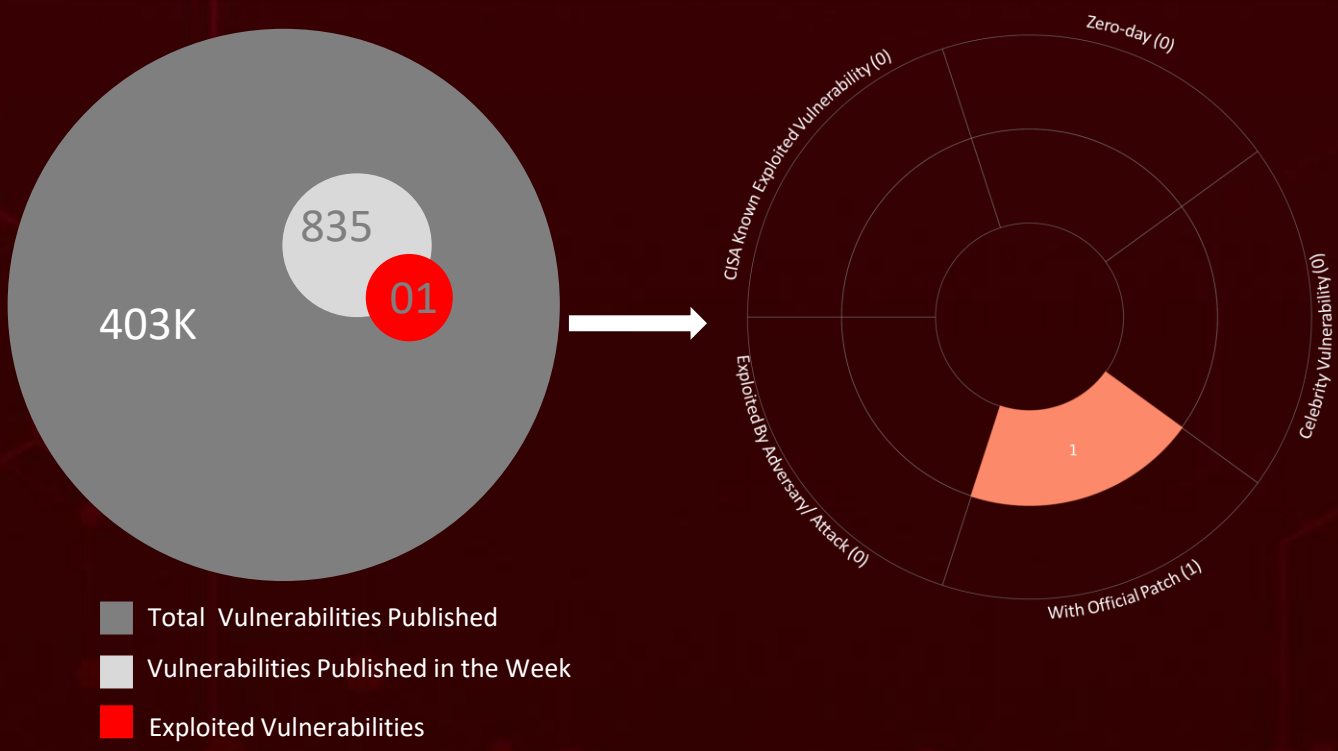
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **eight** major attacks were detected, **one** critical vulnerability was publicly disclosed, and **three** active threat actor groups were monitored, signaling a concerning escalation in malicious activity.

Silent Lynx is an advanced persistent threat (APT) group conducting sustained espionage operations across Central Asia. Their campaign, "**Peek-A-Baku**," employs custom implants such as **Silent Loader** and **LAPLAS**, underscoring a long-term effort to collect intelligence on regional geopolitical and economic developments.

A critical vulnerability (**CVE-2025-11833**) in the widely used Post SMTP WordPress plugin, affecting over 400,000 websites, enables unauthenticated attackers to gain full administrative control by exploiting a missing capability check. The flaw is already being weaponized, with more than 4,500 attacks reportedly blocked to date.

Meanwhile, **Gootloader** resurfaced in October 2025, launching a wave of rapid intrusions that compromised domain controllers within hours of infection. This renewed campaign appears to involve coordinated activity between **Storm-0494** and the **Rhysida** ransomware group, reflecting an increasingly organized and sophisticated threat ecosystem. This highlights the increasing importance of proactive security updates and robust monitoring in defending against sophisticated, rapidly evolving attacks.



High Level Statistics

8
Attacks Executed

1
Vulnerabilities Exploited

3
Adversaries in Action

- SleepyDuck
- Silent Loader
- LAPLAS
- SilentSweeper
- Airstalk
- Gootloader
- Supper backdoor
- Rhysida

- CVE-2025-11833

- Silent Lynx
- Storm-0494
- Vanilla Tempest

Insights

SkyCloak: Decoy-Driven Compromise of High-Value Targets

Operation Peek-A-Baku: Silent Lynx's Multi-Stage Intrusion Chain

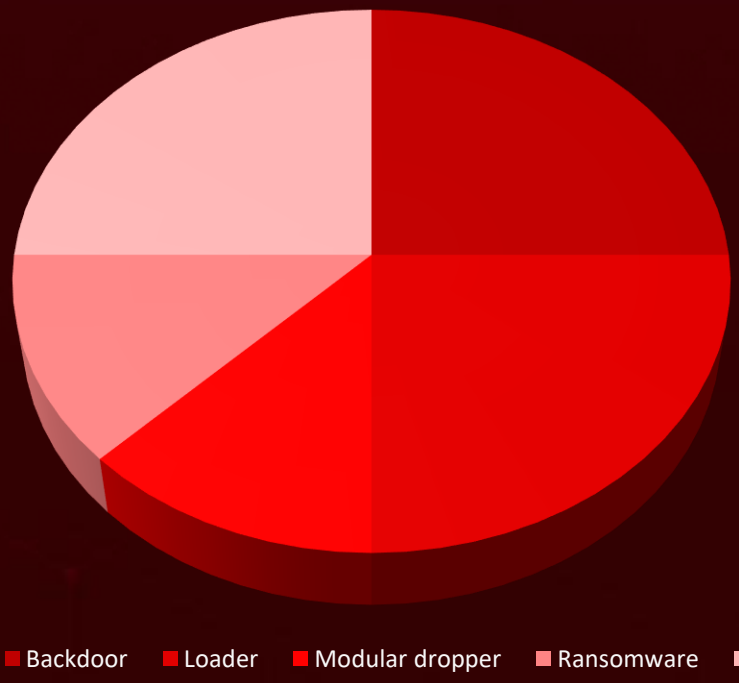
SleepyDuck: The Supply Chain's Quiet Intruder

400K Sites Exposed: **CVE-2025-11833** Post SMTP Bug Enables Complete Site Takeover

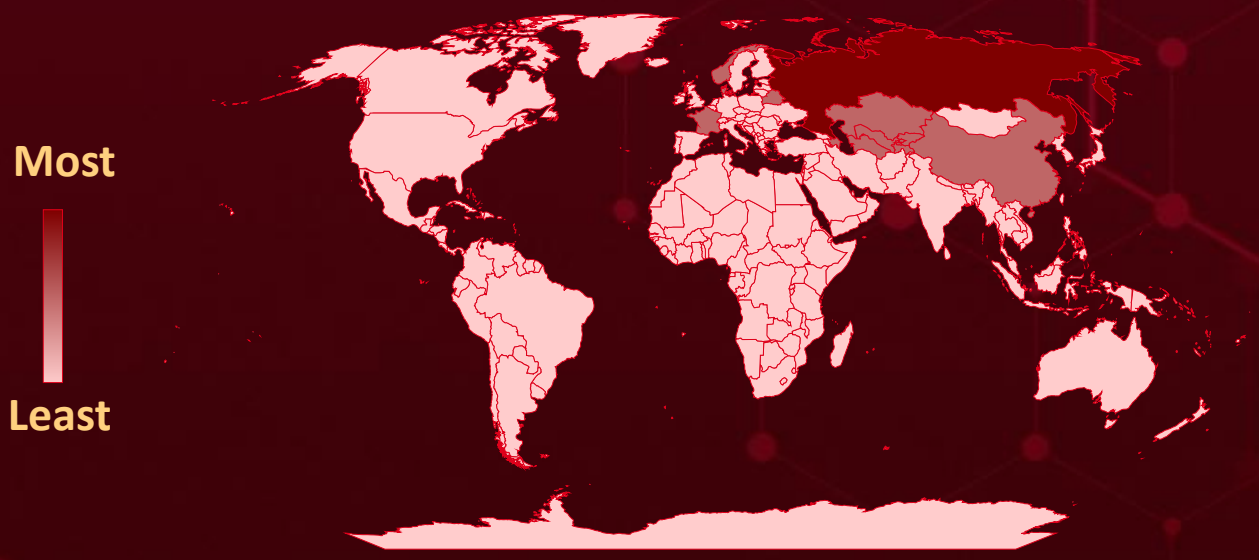
Gootloader Reloaded: SEO Poisoning as a Gateway to Ransomware

Airstalk: Nation-State Espionage Through Supply Chain Compromise

Threat Distribution



Targeted Countries



Countries
Russia
Tajikistan
Kazakhstan
Uzbekistan
Belarus
Azerbaijan
Norway
China
Turkmenistan
Denmark
France
Kyrgyzstan
Monaco
Sri Lanka
Pitcairn Islands
Armenia
Liechtenstein
Aruba
Australia
Saudi Arabia
Austria
Turkey
Afghanistan
Mali
Bahamas
Nauru
Bahrain
Pakistan

Countries
Bangladesh
Rwanda
Barbados
Slovenia
Akrotiri and Dhekelia
Anguilla
Belgium
United Arab Emirates
Belize
Madagascar
Benin
Mauritius
Bermuda
Morocco
Bhutan
New Zealand
Bolivia
Northern Cyprus
Bonaire
Papua New Guinea
Bosnia and Herzegovina
Qatar
Botswana
Saint Martin
Bouvet Island

Countries
Sierra Leone
Brazil
South Africa
British Virgin Islands
Sweden
Brunei
Tonga
Bulgaria
Burkina Faso
Antigua and Barbuda
Burundi
Luxembourg
Cambodia
Malaysia
Cameroon
Marshall Islands
Canada
Micronesia
Cayman Islands
Montenegro
Central African Republic
Myanmar
Chad
Netherlands
Chile

Countries
North Korea
Andorra
Colombia
Palestine
Comoros
Peru
Portugal
Romania
Croatia
Cuba
Serbia
Cyprus
Czech Republic
Somalia
Albania
Syria
Thailand
Uganda
Ecuador
United States
Egypt
Vatican City
El Salvador
Lithuania
Equatorial Guinea
Macau
Ethiopia

Targeted Industries

TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1053** Scheduled Task/Job	**T1071** Application Layer Protocol	**T1059.001** PowerShell	**T1027** Obfuscated Files or Information
T1036 Masquerading	**T1053.005** Scheduled Task	**T1090** Proxy	**T1204** User Execution	**T1547** Boot or Logon Autostart Execution
T1106 Native API	**T1204.002** Malicious File	**T1195** Supply Chain Compromise	**T1059.007** JavaScript	**T1095** Non-Application Layer Protocol
T1497 Virtualization/ Sandbox Evasion	**T1190** Exploit Public-Facing Application	**T1555** Credentials from Password Stores	**T1041** Exfiltration Over C2 Channel	**T1027.013** Encrypted/Encoded File

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SleepyDuck	SleepyDuck, a remote access trojan (RAT), has surfaced in the Open VSX IDE extension marketplace, masquerading as a legitimate Solidity extension. SleepyDuck stands out for its advanced sandbox evasion techniques and its use of an Ethereum smart contract that allows it to dynamically update its command-and-control (C2) server address if the original is taken down, ensuring persistent control.	Supply Chain Compromise	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data exfiltration, Persistent remote control	Windows
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
IOC TYPE	**VALUE**		
Domain	sleepyduck[.]xyz		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Silent Loader	Silent Loader is simple in design and closely related to the C++-based loader. It uses PowerShell's iex to download the malicious file and constructs a command to download and execute the malicious PowerShell script.	Spear-phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Persistence, Command-and-control access	Windows
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
Silent Lynx			
IOC TYPE	**VALUE**		
SHA256	262f9c63c46a0c20d1feecbd0cad75dcb8f731aa5982fef47d2a87217ecda45b		

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
LAPLAS	Laplas is a C++ remote-access trojan that opens a connection to an attacker-controlled server. It can be started with a server address and port, or it falls back to a built-in address if none are provided. After a short pause, it attempts to connect, performs some internal data handling, and awaits commands. A second version behaves the same but uses an encrypted (TLS) channel and a slightly different command-and-control infrastructure.	Spear-phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Remote control	Windows
Remote Access Trojan			
ASSOCIATED ACTOR			**PATCH LINK**
Silent Lynx			-
IOC TYPE	**VALUE**		
SHA256	82f55f828618106ecd9f1c44acde2f0eefd566d50edcddb1f5782d1af84846c0, b90c565fb5fa3040dfae1345217f0b39af3657fcd766d3d0c5783d781c58f85e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SilentSweeper	SilentSweeper is a .NET malware that accepts command-line, extracts an embedded PowerShell script to disk. It loads an embedded script, decodes an encoded payload, then downloads and executes a second script that gives attackers remote control of the system.	Spear-phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Persistence enablement, Remote control	Windows
Modular dropper			
ASSOCIATED ACTOR			**PATCH LINK**
Silent Lynx			-
IOC TYPE	**VALUE**		
SHA256	2c8efe6eb9f02bf003d489e846111ef3c6cab32168e6f02af7396e93938118dd		

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
Airstalk	Airstalk is a stealthy Windows malware family, present in PowerShell and .NET variants, that exploits Workspace ONE's API for covert command-and-control communication and exfiltrates browser data, screenshots, and activity logs.	-	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data exfiltration, Operational disruption	Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
CL-STA-1009			-
IOC TYPE	VALUE		
SHA256	dfdc27d81a6a21384d6dba7dcdc4c7f9348cf1bdc6df7521b886108b71b41533, b6d37334034cd699a53df3e0bcac5bbdf32d52b4fa4944e44488bd2024ad719b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Gootloader	Gootloader is an advanced JavaScript-based loader frequently employed by threat actors to establish initial access. It has re-emerged, now employing bespoke WOFF2 fonts and glyph-substitution techniques to conceal filenames.	Compromised Website	-
		IMPACT	AFFECTED PLATFORM
TYPE		Downstream Payloads	Windows
Loader			
ASSOCIATED ACTOR			PATCH LINK
Storm-0494, Vanilla Tempest			-
IOC TYPE	VALUE		
SHA256	2f056ce0657542da3e7e43fb815a8973c354624043f19ef134dff271db1741b3, b9a61652dffd2ab3ec3b7e95829759fc43665c27e9642d4b2d4d2f7287254034		
URLs	hxxps[:]//spirits-station.fr/, hxxps[:]//www.us.registration.fcaministers.com/		

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
Supper backdoor	The Supper SOCKS5 backdoor enables remote control of compromised hosts and supports network traffic tunneling. It employs an 'API hammering' technique, issuing numerous rapid and repetitive API calls to hinder analysis tools and researchers. This flood of benign calls overwhelms disassemblers and debuggers, significantly slowing the manual analysis process.	-	-
		IMPACT	AFFECTED PLATFORM
TYPE		Remote Access and Control, Evasion	Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Vanilla Tempest			-
IOC TYPE	VALUE		
SHA256	cf44aa11a17b3dad61cae715f4ea27c0cbf80732a1a7a1c530a5c9d3d183482a		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Rhysida	Rhysida, a ransomware-as-a-service (RaaS) operation, emerged in May 2023 alongside the launch of its victim support portal on the TOR network. It is frequently observed following Gootloader intrusions.	-	-
		IMPACT	AFFECTED PLATFORM
TYPE		Financial Loss	Windows
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
Vanilla Tempest			-
IOC TYPE	VALUE		
SHA256	8220a20a98173ddf2330fe08f84e603ce05bcb686b9caed134ac084a4c63d77a, 9e88ac415d6823b48a2de3adf41979ffba16dbfaded7aa8a071ed0a36a211c64		

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

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-11833</td><td>  </td><td rowspan="2">Post SMTP WordPress Plugin Affected all versions up to, and including 3.6.0</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">WordPress Plugin Post SMTP Missing Authorization Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-862</td><td>T1059: Command and Scripting Interpreter, T1005: Data from Local System, T1078: Valid Accounts</td><td>https://wordpress.org/plugins/post-smtp/#developers</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
	-	Government, Diplomats, Think-tanks, Finance, Mining, Transport & Communications	Tajikistan, Kazakhstan, Kyrgyzstan, Turkmenistan, Uzbekistan, Russia, Azerbaijan, China
	MOTIVE		
	Information theft and espionage		
Silent Lynx (alias YoroTrooper, Sturgeon Phisher, Cavalry Werewolf, ShadowSilk)	**TARGETED CVE**	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	Silent Loader, LAPLAS, SilentSweeper	Windows

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0010: Exfiltration; TA0005: Defense Evasion; TA0004: Privilege Escalation; TA0011: Command and Control; T1053: Scheduled Task/Job; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1027: Obfuscated Files or Information; T1059: Command and Scripting Interpreter; T1027.013: Encrypted/Encoded File ; T1204.002: Malicious File; T1204.001: Malicious Link; T1106: Native API; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1059.001: PowerShell; T1036: Masquerading; T1095: Non-Application Layer Protocol; T1090: Proxy; T1041: Exfiltration Over C2 Channel; T1059.005: Visual Basic; T1547.009: Shortcut Modification; T1547: Boot or Logon Autostart Execution; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1572: Protocol Tunneling; T1567: Exfiltration Over Web Service

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Storm-0494</td><td>-</td><td rowspan="2">All</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Gootloader, Supper backdoor, Rhysida ransomware</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0007: Discovery; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0009: Collection; TA0006: Credential Access; TA0008: Lateral Movement; TA0011: Command and Control; TA0043: Reconnaissance; T1490: Inhibit System Recovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1027.013: Encrypted/Encoded File; T1105: Ingress Tool Transfer; T1090: Proxy; T1021.006: Windows Remote Management; T1584: Compromise Infrastructure; T1190: Exploit Public-Facing Application; T1204: User Execution; T1027: Obfuscated Files or Information; T1059.001: PowerShell; T1021: Remote Services; T1113: Screen Capture; T1608: Stage Capabilities; T1608.006: SEO Poisoning; T1189: Drive-by Compromise; T1059.007: JavaScript; T1547.001: Registry Run Keys / Startup Folder; T1068: Exploitation for Privilege Escalation; T1547: Boot or Logon Autostart Execution; T1059: Command and Scripting Interpreter; T1140: Deobfuscate/Decode Files or Information; T1555: Credentials from Password Stores; T1036: Masquerading; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1055: Process Injection; T1584.001: Domains; T1552: Unsecured Credentials; T1558.003: Kerberoasting; T1558: Steal or Forge Kerberos Tickets; T1095: Non-Application Layer Protocol</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Vanilla Tempest (DEV-0832, Vice Society)</td><td>-</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial Gains</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Gootloader, Supper backdoor, Rhysida ransomware</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0007: Discovery; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0009: Collection; TA0006: Credential Access; TA0008: Lateral Movement; TA0011: Command and Control; TA0043: Reconnaissance; T1490: Inhibit System Recovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1027.013: Encrypted/Encoded File; T1105: Ingress Tool Transfer; T1090: Proxy; T1021.006: Windows Remote Management; T1584: Compromise Infrastructure; T1190: Exploit Public-Facing Application; T1204: User Execution; T1027: Obfuscated Files or Information; T1059.001: PowerShell; T1021: Remote Services; T1113: Screen Capture; T1608: Stage Capabilities; T1608.006: SEO Poisoning; T1189: Drive-by Compromise; T1059.007: JavaScript; T1547.001: Registry Run Keys / Startup Folder; T1068: Exploitation for Privilege Escalation; T1547: Boot or Logon Autostart Execution; T1059: Command and Scripting Interpreter; T1140: Deobfuscate/Decode Files or Information; T1555: Credentials from Password Stores; T1036: Masquerading; T1053.005: Scheduled Task; T1053: Scheduled Task/Job; T1055: Process Injection; T1584.001: Domains; T1552: Unsecured Credentials; T1558.003: Kerberoasting; T1558: Steal or Forge Kerberos Tickets; T1095: Non-Application Layer Protocol</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **one exploitable vulnerability** and block the indicators related to the threat actors **Silent Lynx, Storm-0494, Vanilla Tempest,** and malware **SleepyDuck, Silent Loader, LAPLAS, SilentSweeper, Airstalk, Gootloader, Supper backdoor,** and **Rhysida.**

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 **one exploitable vulnerability.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Silent Lynx, Storm-0494, Vanilla Tempest,** and malware **Silent Loader, SilentSweeper,** and **Airstalk Malware** in Breach and Attack Simulation(BAS).

Threat Advisories

Operation SkyCloak: Covert Cyber Strikes on Russian and Belarusian Military Personnel

SleepyDuck: Trojan Nesting in the Open VSX Marketplace

Silent Lynx APT: Espionage Operations Targeting Central Asia's Critical Infrastructure

WordPress Plugin Bug CVE-2025-11833 Hands Hackers the Admin Throne

Unmasking Airstalk's Covert Supply Chain Intrusion

Return of Gootloader: Blending Technical Evasion with Operational Discipline

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
SleepyDuck	Domain	sleepyduck[.]xyz
Silent Loader	SHA256	262f9c63c46a0c20d1feecbd0cad75dcb8f731aa5982fef47d2a87217ecda45b
LAPLAS	SHa256	82f55f828618106ecd9f1c44acde2f0eefd566d50edcddb1f5782d1af84846c0, b90c565fb5fa3040dfae1345217f0b39af3657fcd766d3d0c5783d781c58f85e, a6b21c396a5e0875875732d93d048176cf9ad78e34e8a08615590bcd90714c96, 876b86d89ce3aea4cbdc8fd1014420db685aa77d1fd0bb2ed31daa4c1f394d40, 2c63c61e0adaaf669c9c674edfc9081d415c05b834611944a682f120ab9559d8, 876b86d89ce3aea4cbdc8fd1014420db685aa77d1fd0bb2ed31daa4c1f394d40
SilentSweeper	SHA256	2c8efe6eb9f02bf003d489e846111ef3c6cab32168e6f02af7396e93938118dd
Airstalk	SHA256	dfdc27d81a6a21384d6dba7dcdc4c7f9348cf1bdc6df7521b886108b71b41533, b6d37334034cd699a53df3e0bcac5bbdf32d52b4fa4944e44488bd2024ad719b, 4e4cbaed015dfbda3c368ca4442cd77a0a2d5e65999cd6886798495f2c29fcd5, 3a48ea6857f1b6ae28bd1f4a07990a080d854269b1c1563c9b2e330686eb23b5, 0c444624af1c9cce6532a6f88786840ebce6ed3df9ed570ac75e07e30b0c0bde

Attack Name	TYPE	VALUE
Gootloader	File path	C:\Users\username\AppData\Roaming\ISIS Drivers\, C:\Users\username\AppData\Roaming\Nuance\ , C:\Users\username\AppData\Roaming\PFU\,C:\Users\username\AppData\Local\Oardwior\ , C:\Users\username\AppData\Roaming\myHUD,C:\Users\username\AppData\Roaming\Canon U.S.A.
	URLs	hxxps[:]//spirits-station.fr/, hxxps[:]//www.us.registration.fcaministers.com/, hxxps[:]//motoz.com.au/, hxxps[:]//routinelynomadic.com/, hxxps[:]//www.wagenbaugrabs.ch/, hxxps[:]//studentspoint.org/, hxxps[:]//dailykhabrain.com.pk/, hxxps[:]//myanimals.com/, hxxps[:]//www2.pelisyseries.net/, hxxps[:]//www.claritycontentservices.com/wp/, hxxps[:]//patriotillumination.com/, hxxps[:]//michaelcheney.com/, hxxps[:]//allreleases.ru/, hxxps[:]//cloudy.pk/, hxxps[:]//eliskavaea.cz/, hxxps[:]//r34porn.net/, hxxps[:]//leadoo.com/, hxxps[:]//ostmarketing.com/, hxxps[:]//egyptelite.com/, hxxps[:]//restaurantchezhenri.ca/, hxxps[:]//www1.zonewebmaster.eu/news/, hxxps[:]//campfosterymca.com/, hxxps[:]//idmpakistan.pk/, hxxps[:]//themasterscraft.com/, hxxps[:]//unica.md/, hxxps[:]//cargoboard.de/, hxxps[:]//www.supremesovietoflove.com/wp/, hxxps[:]//buildacampervan.com/, hxxps[:]//www.minklinkaps.com/, hxxps[:]//aradax.ir/, hxxps[:]//medicit-y.ch/, hxxps[:]//redronic.com/, hxxps[:]//www.ferienhausdehaanmieten.de/, hxxps[:]//gravityforms.ir/, hxxps[:]//apprater.net/, hxxps[:]//fotbalovavidea.cz/, hxxps[:]//usma.ru/, hxxps[:]//thetripschool.com/, hxxps[:]//cortinaspraga.com/, hxxp[:]//cookcountyjudges.org/, hxxps[:]//x.fybw.org/, hxxps[:]//jungutah.com/, hxxps[:]//influenceimmo.com/, hxxps[:]//tokyocheapo.com/, hxxps[:]//espressonisten.de/, hxxps[:]//tiresdoc.com/, hxxps[:]//hotporntv.net/, hxxps[:]//yourboxspring.nl/, hxxps[:]//filmcrewnepal.com/, hxxps[:]//yoga-penzberg.de/, hxxps[:]//sugarbeecrafts.com/, hxxps[:]//www.worldwealthbuilders.com/, hxxps[:]//lepolice.com/, hxxps[:]//www.lovestu.com/, hxxps[:]//bluehamham.com/, hxxps[:]//vps3nter.ir/, hxxps[:]//whiskymuseum.at/, hxxps[:]//latimp.eu/, hxxps[:]//solidegypt.net/, hxxps[:]//wessper.com/,

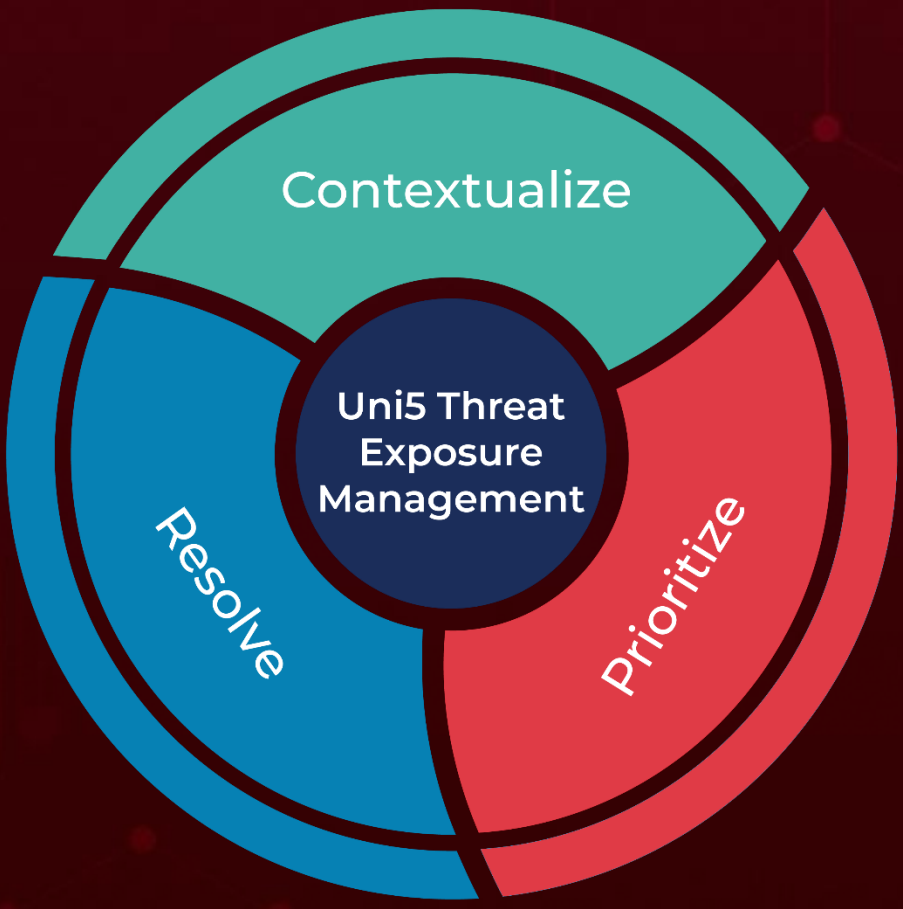
Attack Name	TYPE	VALUE
Gootloader	URLs	hxxps[:]//www.pathfindertravels.se/tickets/, hxxps[:]//www.smithcoinc.biz/, hxxps[:]//kollabmi.se/, hxxps[:]//xxxmorritas.com/, hxxps[:]//onsk.dk/, hxxps[:]//villasaze.ir/, hxxps[:]//blossomthemesdemo.com/, hxxps[:]//headedforspace.com/
	SHA256	2f056ce0657542da3e7e43fb815a8973c354624043f19ef134dff271db1741b3, b9a61652dffd2ab3ec3b7e95829759fc43665c27e9642d4b2d4d2f7287254034, 39d980851be1e111c035e4db2589fa3d5f59a5bef7b7b3e36bff5435c78f7049, c2326db8acae0cf9c5fc734e01d6f6c1cd78473b27044955c5761ec7fd479964, ad88076fd75d80e963d07f03d7ae35d4e55bd49634baf92743eece19ec901e94, 7557d5fed880ee1e292aba464ffdc12021f9acbe0ee3a2313519ecd7f94ec5c4, 5ec9e926d4fb4237cf297d0d920cf0e9a5409f0226ee555bd8c89b97a659f4b0, 87cbe9a5e9da0dba04dbd8046b90dbd8ee531e99fd6b351eae1ae5df5aa67439
Supper backdoor	IPv4	103[.]253[.]42[.]91 , 91[.]236[.]230[.]134 , 213[.]232[.]236[.]138 , 146[.]19[.]49[.]177
	SHA256	cf44aa11a17b3dad61cae715f4ea27c0cbf80732a1a7a1c530a5c9d3d183482a
Rhysida	SHA256	8220a20a98173ddf2330fe08f84e603ce05bcb686b9caed134ac084a4c63d77a, 9e88ac415d6823b48a2de3adf41979ffba16dbfaded7aa8a071ed0a36a211c64, cc1d720d5da2885c50cd93547ccf8163d7b4bb7511c7f5756e4798e449306c53, 86e75af22f702ba1aaa545708e04cb54468a388e899e259510af9c95b34d80cc, 8061bb999a0f5d3165742283001a7a68e7905718c928172343bf8456b69f268d, 57a2401758b5282090f145623041a6c3805663de137505a7095df9e0271b4602

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

November 10, 2025 . 7:45 AM

More at www.hivepro.com