Date of Publication
October 27, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

20 to 26 OCTOBER 2025

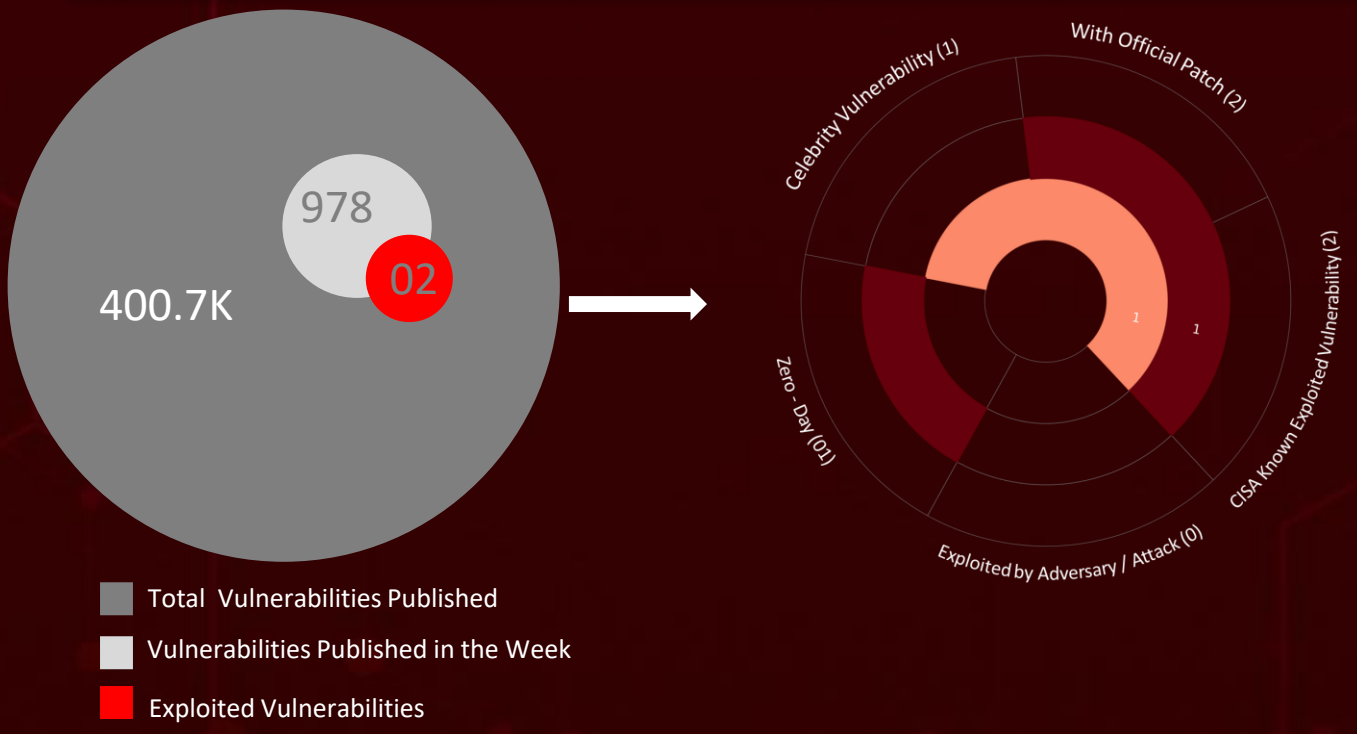
Table Of Contents

Summary

HiveForce Labs has observed a sharp spike in cyber threats, making it clear that attacks are becoming more frequent and more sophisticated. In just the past week, detected **five** major security incidents, tracked **two** active threat actor groups, and confirmed active exploitation of **two** vulnerabilities. The situation underscores how quickly the threat landscape continues to escalate, with attackers aggressively targeting exposed systems and misconfigurations to gain a foothold.

Two critical vulnerabilities are currently under active exploitation. **SessionReaper (CVE-2025-54236)** in Adobe Commerce and Magento Open Source enables unauthenticated attackers to hijack customer accounts and potentially execute malicious code on targeted systems. Meanwhile, **CVE-2025-61932** affects Motex's Lanscope Endpoint Manager (on-premises), allowing remote adversaries to run arbitrary commands on endpoints by sending specially crafted packets, a threat leveraged in real-world attacks since April 2025. Additionally, **Azure Blob Storage** has emerged as a major target, as attackers take advantage of misconfigurations, stolen credentials, or vulnerable automation triggers to steal or manipulate sensitive data, deploy ransomware, and maintain persistence in cloud environments.

The week also brought attention to high-profile espionage campaigns. Iran-linked **MuddyWater** has been phishing government and critical infrastructure entities across the Middle East and North Africa, deploying the Phoenix backdoor for intelligence collection. Moreover, North Korea's **Lazarus** group continues to expand Operation DreamJob, shifting its focus toward European defense companies shaping next-generation drone technology. These developments reinforce a critical message for organizations everywhere: proactive defense, swift patching, and strong cyber hygiene are no longer optional; they are essential for survival in today's hostile digital world.



High Level Statistics

5
Attacks Executed

2
Vulnerabilities Exploited

2
Adversaries in Action

- Phoenix Backdoor v4
- FakeUpdate Loader
- Chromium_Stealer
- ScoringMathTea
- BinMergeLoader
- CVE-2025-54236
- CVE-2025-61932
- MuddyWater
- Lazarus

Insights

A wave of **1201** newly patched Linux flaws shows attackers continue to pressure even the most trusted open-source systems.

Azure Blob Storage has turned into a goldmine for attackers hunting misconfigurations and exposed data treasure.

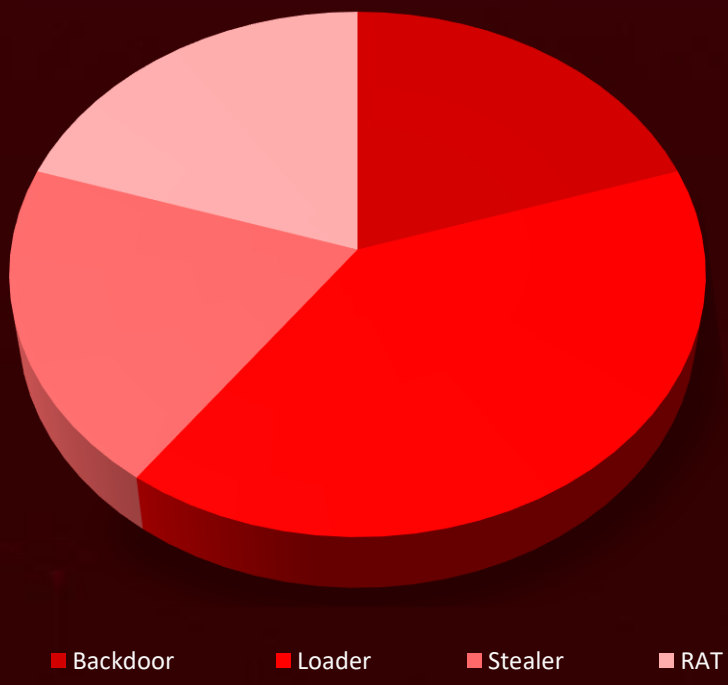
MuddyWater is striking government and critical infrastructure targets across MENA with phishing lures that deliver its Phoenix backdoor.

SessionReaper (**CVE-2025-54236**) is now being actively weaponized to hijack accounts and seize control of online stores.

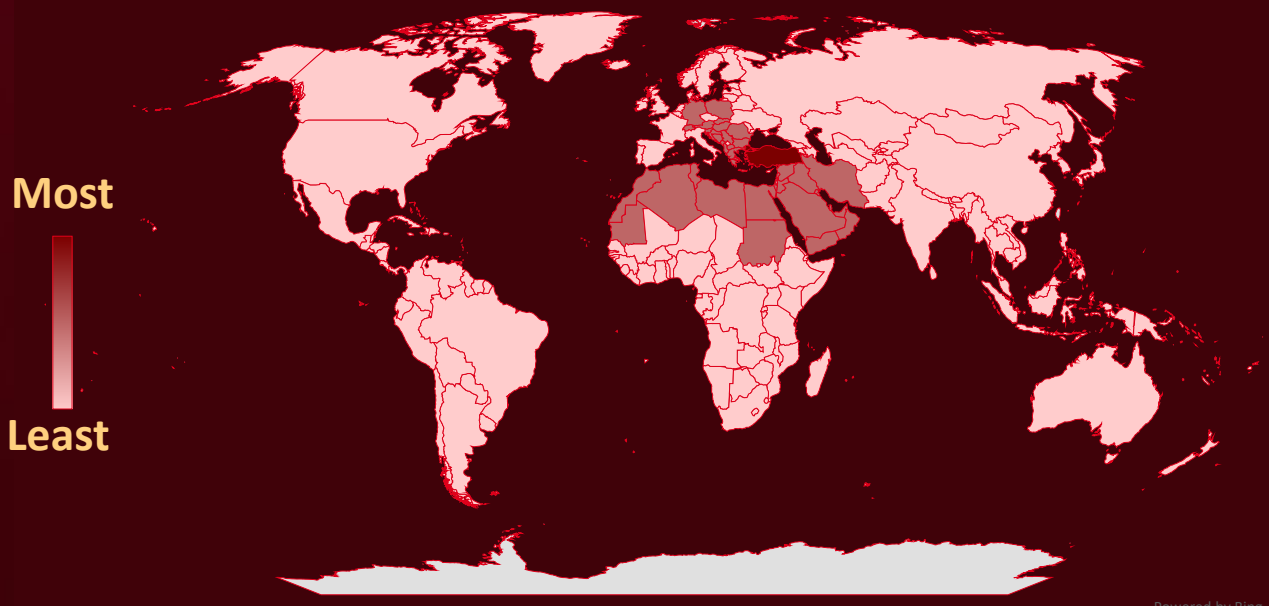
CVE-2025-61932 enables remote attackers to run arbitrary code on Lanscope endpoints through crafted network packets.

Lazarus is expanding **Operation DreamJob** to infiltrate Europe's defense innovators shaping next-gen drone tech.

Threat Distribution

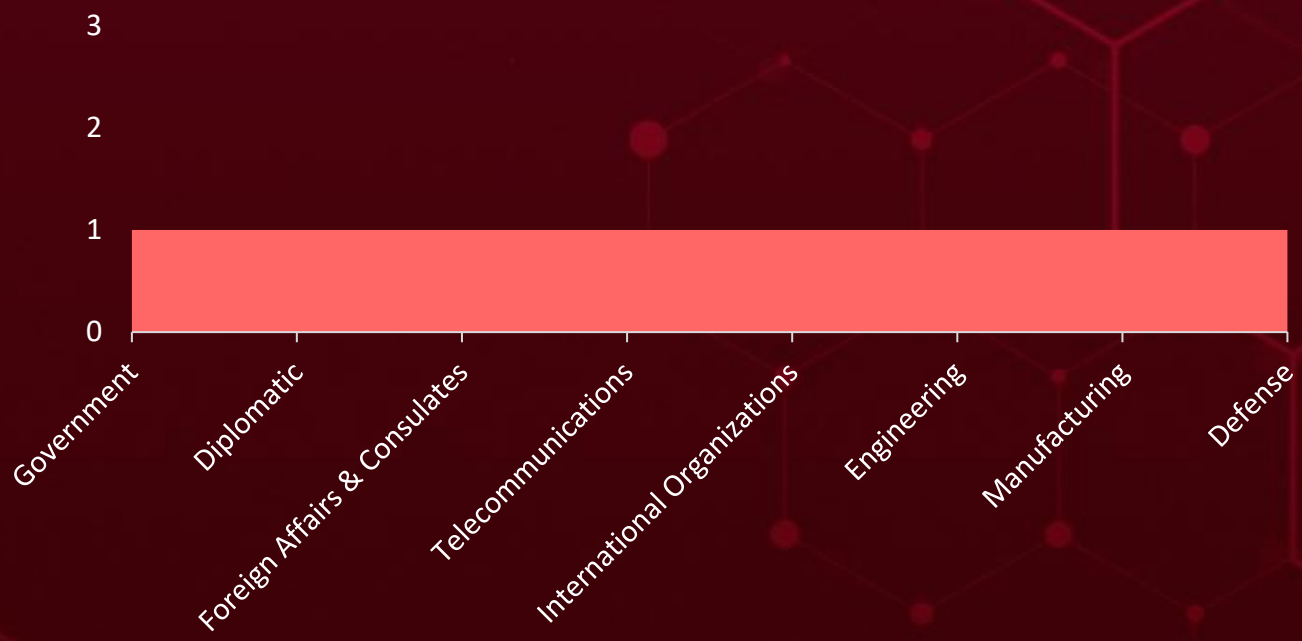


Targeted Countries



Countries	Countries	Countries	Countries
Turkey	Iran	Brunei	Myanmar
Mauritania	Serbia	Cyprus	India
Saudi Arabia	Iraq	Singapore	Nauru
Oman	Slovenia	Czech Republic	Indonesia
Algeria	Israel	Chad	Netherlands
Albania	Switzerland	Czech Republic (Czechia)	Angola
Sudan	Jordan	United States	Nicaragua
Austria	Tunisia	Denmark	Bangladesh
Morocco	Kuwait	Namibia	Nigeria
Bahrain	United Arab Emirates	Djibouti	Ireland
Qatar	Lebanon	North Korea	Botswana
Bosnia and Herzegovina	Liechtenstein	Dominica	Barbados
Slovakia	Libya	Papua New Guinea	Brazil
Bulgaria	Spain	Dominican Republic	Italy
Syria	Pakistan	Russia	Palau
Croatia	Zambia	DR Congo	Jamaica
Yemen	Costa Rica	Senegal	Panama
Egypt	Samoa	Ecuador	Japan
Montenegro	Côte d'Ivoire	Somalia	Paraguay
Germany	Chile	Australia	Belarus
North Macedonia	Armenia	Canada	Philippines
Greece	New Zealand	El Salvador	Kazakhstan
Poland	Cuba	Timor-Leste	Portugal
Hungary		Uganda	Kenya
Romania			Burkina Faso

Targeted Industries



TOP MITRE ATT&CK TTPs

T1071 Application Layer Protocol	**T1190** Exploit Public-Facing Application	**T1566** Phishing	**T1027** Obfuscated Files or Information	**T1059** Command and Scripting Interpreter
T1071.001 Web Protocols	**T1055** Process Injection	**T1565** Data Manipulation	**T1204** User Execution	**T1027.009** Embedded Payloads
T1140 Deobfuscate/ Decode Files or Information	**T1041** Exfiltration Over C2 Channel	**T1203** Exploitation for Client Execution	**T1566.001** Spearphishing Attachment	**T1204.002** Malicious File
T1082 System Information Discovery	**T1027.007** Dynamic API Resolution	**T1105** Ingress Tool Transfer	**T1078.004** Cloud Accounts	**T1210** Exploitation of Remote Services

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Phoenix Backdoor v4	Phoenix is a compact, stealthy backdoor linked to MuddyWater that fingerprints infected Windows hosts, attempts to create a mutex named sysprocupdate.exe, and installs a copy to maintains persistence by altering the current user's registry autostart and reaches out to its operators over WinHTTP to fetch and execute commands. This observed v4 sample also contains an embedded Portable Executable inside the binary that was not dropped or run during normal operation, implying a dormant capability the operator could enable later.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		System Compromise	Windows
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-
IOC TYPE	**VALUE**		
SHA256	668dd5b6fb06fe30a98dd59dd802258b45394ccd7cd610f0aaab43d801bf1a1e, 5ec5a2adaa82a983fcc42ed9f720f4e894652bd7bd1f366826a16ac98bb91839		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
FakeUpdate Loader	FakeUpdate is an injector-style loader that uses AES at runtime to decrypt an embedded second-stage payload and then injects the decrypted code into its own process for execution. It operates as a covert bootstrap, remaining quiet on disk and exposing the payload only after in-memory decryption and self-injection.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Loader		Loads Malware	Windows
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

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
Chromium_Stealer	Chromium_Stealer is a custom credential-harvesting tool that masquerades as a harmless calculator-style app to evade detection. Its primary purpose is to locate browser profiles, extract the browser master key, and then read the profile's Login Data databases to retrieve stored credentials. To ensure it can access locked files, it will terminate running browser processes, decrypt stored passwords in memory using the recovered master key, and write the results into a local staging file. The credentials in that file are stored in an encrypted form. After harvesting, the malware attempts to restart the browser from its previous state to reduce user suspicion.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	Windows
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ScoringMathTea	ScoringMathTea is a remote-access trojan first observed in late 2022 that gives operators near-complete control of infected hosts. It was quickly adopted by Lazarus during Operation DreamJob and has remained their go-to post-compromise payload for about three years, reappearing across multiple campaigns. The RAT talks to command-and-control infrastructure hosted on compromised servers; investigators often find the server-side components concealed inside WordPress sites, typically buried in theme or plugin directories to hide in plain sight. Its combination of reliable remote-control features and a stealthy C2 hosting approach makes it well-suited for long-term access and follow-up operations.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	-
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-

IOC TYPE	VALUE
SHA1	71D0DDB7C6CAC4BA2BDE679941FA92A31FBEC1FF, E670C4275EC24D403E0D4DE7135CBCF1D54FF09C
IPv4	23[.]111[.]133[.]162, 104[.]21[.]80[.]1

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 rowspan="2">BinMergeLoader</td><td rowspan="5">BinMergeLoader is a lightweight loader in the same family as MISTPEN that abuses legitimate Microsoft cloud tooling to blend in. It authenticates with Microsoft API tokens and uses the Microsoft Graph API as its command-and-control and delivery channel, giving operators a stealthy, high-privilege pathway into Microsoft 365 resources and endpoints.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td rowspan="2">IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Loads Malware</td><td rowspan="2">-</td></tr>
<tr><td>Loader</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Lazarus</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA1</td><td colspan="3">26AA2643B07C48CB6943150ADE541580279E8E0E</td></tr>
</table>

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-2025-54236	✓	Adobe Commerce Versions: 2.4.9- alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6- p12, 2.4.5-p14, 2.4.4-p15 and earlier Adobe Commerce B2B Versions: 1.5.3-alpha2, 1.5.2-p2, 1.4.2-p7, 1.3.4-p14, 1.3.3-p15 and earlier Magento Open Source Versions: 2.4.9-alpha2, 2.4.8-p2, 2.4.7 p7, 2.4.6-p12, 2.4.5-p14 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:commerce:-:*:*:*:*:*:*:* cpe:2.3:a:adobe:commerce_b2b:-:*:*:*:*:*:*:* cpe:2.3:a:adobe:magento:-:*:*:open_source:*:*:*	-
SessionReaper (Adobe Commerce and Magento Improper Input Validation Vulnerability)	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1539: Steal Web Session Cookie	https://helpx.adobe.com/security/products/magento/apsb25-88.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-61932	✗	LANSCOPE Endpoint Manager On-Premise Version 9.4.7.1 and earlier Client Program (MR) Detection Agent (DA)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:motex:lanscope_endpoint_manager:*:*:*:*:on-premise:*:*:*	-
Motex LANSCOPE Endpoint Manager Improper Verification of Source of a Communication Channel Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-940	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1210: Exploitation of Remote Services; T1068: Exploitation for Privilege Escalation; T1203: Exploitation for Client Execution	https://www.motex.co.jp/news/notice/2025/release251020/

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix)	Iran	Government, Diplomatic, Foreign Affairs Ministries and Consulates, Telecommunications, International Organizations	Middle East and North Africa (MENA)
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Phoenix Backdoor v4, FakeUpdate Loader, Chromium_Stealer	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0007: Discovery; TA0005: Defense Evasion; TA0040: Impact; TA0010: Exfiltration; TA0009: Collection; TA0006: Credential Access; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1059.003: Windows Command Shell; T1059: Command and Scripting Interpreter; T1547.001: Registry Run Keys / Startup Folder; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1219: Remote Access Software; T1027: Obfuscated Files or Information; T1586: Compromise Accounts; T1564.001: Hidden Files and Directories; T1564: Hide Artifacts; T1555: Credentials from Password Stores; T1082: System Information Discovery; T1071.001: Web Protocols; T1071: Application Layer Protocol; T1555.003: Credentials from Web Browsers; T1090.002: External Proxy; T1090: Proxy; T1041: Exfiltration Over C2 Channel; T1565: Data Manipulation; T1059.005: Visual Basic; T1059.001: PowerShell; T1547.004: Winlogon Helper DLL; T1546.015: Component Object Model Hijacking; T1546: Event Triggered Execution; T1055: Process Injection; T1055.002: Portable Executable Injection; T1140: Deobfuscate/Decode Files or Information; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1112: Modify Registry; T1027.002: Software Packing; T1105: Ingress Tool Transfer

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, G0032)	North Korea	Engineering, Manufacturer of Aircraft Components, Defense Company	Southeastern and Central Europe
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	ScoringMathTea, BinMergeLoader	-

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1584: Compromise Infrastructure; T1584.004: Server; T1587: Develop Capabilities; T1587.001: Malware; T1106: Native API; T1129: Shared Modules; T1204: User Execution; T1204.002: Malicious File; T1574: Hijack Execution Flow; T1574.001: DLL; T1134: Access Token Manipulation; T1134.002: Create Process with Token; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1620: Reflective Code Loading; T1055: Process Injection; T1083: File and Directory Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1132: Data Encoding; T1132.001: Standard Encoding; T1041: Exfiltration Over C2 Channel; T1036: Masquerading; T1566: Phishing

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploited vulnerabilities** and block the indicators related to the threat actors **MuddyWater, Lazarus,** and malware **Phoenix Backdoor v4, FakeUpdate Loader, Chromium_Stealer, ScoringMathTea,** and **BinMergeLoader.**

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 **two exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **MuddyWater, Lazarus,** and malware **Phoenix Backdoor v4, ScoringMathTea,** in Breach and Attack Simulation(BAS).

Threat Advisories

Critical Cloud Threat: Azure Blob Storage Under Active Attack

MuddyWater Deploys Phoenix Backdoor in Targeted Espionage Campaign

Lazarus Targets Europe’s UAV Innovation

SessionReaper Flaw Enables Seamless Session Hijacking on Adobe Commerce

CVE-2025-61932: Critical Lanscope Endpoint Manager Flaw Actively Exploited

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
Phoenix Backdoor v4	SHA256	668dd5b6fb06fe30a98dd59dd802258b45394ccd7cd610f0aaab43d801bf1a1e, 5ec5a2adaa82a983fcc42ed9f720f4e894652bd7bd1f366826a16ac98bb91839, 1883db6de22d98ed00f8719b11de5bf1d02fc206b89fedd6dd0df0e8d40c4c56, 3ac8283916547c50501eed8e7c3a77f0ae8b009c7b72275be8726a5b6ae255e3, 76fa8dca768b64aefedd85f7d0a33c2693b94bdb55f40ced7830561e48e39c75, 3d6f69cc0330b302ddf4701bbc956b8fca683d1c1b3146768dcbce4a1a3932ca
ScoringMathTea	SHA256	c39ecc7d9f1e225a37304345731fffe72cdb95b21aeb06aa6022f6d338777012
	SHA1	71D0DDB7C6CAC4BA2BDE679941FA92A31FBEC1FF, E670C4275EC24D403E0D4DE7135CBCF1D54FF09C, AC16B1BAEDE349E4824335E0993533BF5FC116B3, 086816466D9D9C12FCADA1C872B8C0FF0A5FC611

Attack Name	TYPE	VALUE
ScoringMathTea	IPv4	23[.]111[.]133[.]162, 104[.]21[.]80[.]1, 70[.]32[.]24[.]131, 185[.]148[.]129[.]24, 66[.]29[.]144[.]75, 108[.]181[.]92[.]71, 104[.]247[.]162[.]67, 193[.]39[.]187[.]165, 172[.]67[.]193[.]139, 77[.]55[.]252[.]111, 45[.]148[.]29[.]122, 75[.]102[.]23[.]3, 152[.]42[.]239[.]211, 95[.]217[.]119[.]214
	Domains	coralsunmarine[.]com, kazitradebd[.]com, oldlinewoodwork[.]com, www[.]mnmathleague[.]org, pierregems[.]com, www[.]scgestor.com[.]br, galaterrace[.]com, ecudecode[.]mx, www[.]anvil.org[.]ph,partnerls[.]pl, trainingpharmacist[.]co[.]uk, mediostresbarbas[.]com[.]ar, www[.]bandarpowder[.]com, spaincaramoon[.]com
	URLs	hxxps[:]//coralsunmarine[.]com/wp-content/themes/flatsome/inc/functions/function-hand[.]php, hxxps[:]//kazitradebd[.]com/wp-content/themes/hello-elementor/includes/customizer/customizer-hand[.]php, hxxps[:]//oldlinewoodwork[.]com/wp-content/themes/zubin/inc/index[.]php, hxxps[:]//www[.]mnmathleague[.]org/ckeditor/adapters/index[.]php, hxxps[:]//pierregems[.]com/wp-content/themes/woodmart/inc/configs/js-hand[.]php, hxxps[:]//www[.]scgestor[.]com[.]br/wp-content/themes/vantage/inc/template-headers[.]php, hxxps[:]//galaterrace[.]com/wp-content/themes/hello-elementor/includes/functions[.]php, hxxps[:]//ecudecode[.]mx/redsocial/wp-content/themes/buddyx/inc/Customizer/usercomp[.]php, hxxps[:]//www[.]anvil[.]org[.]ph/list/images/index[.]php,

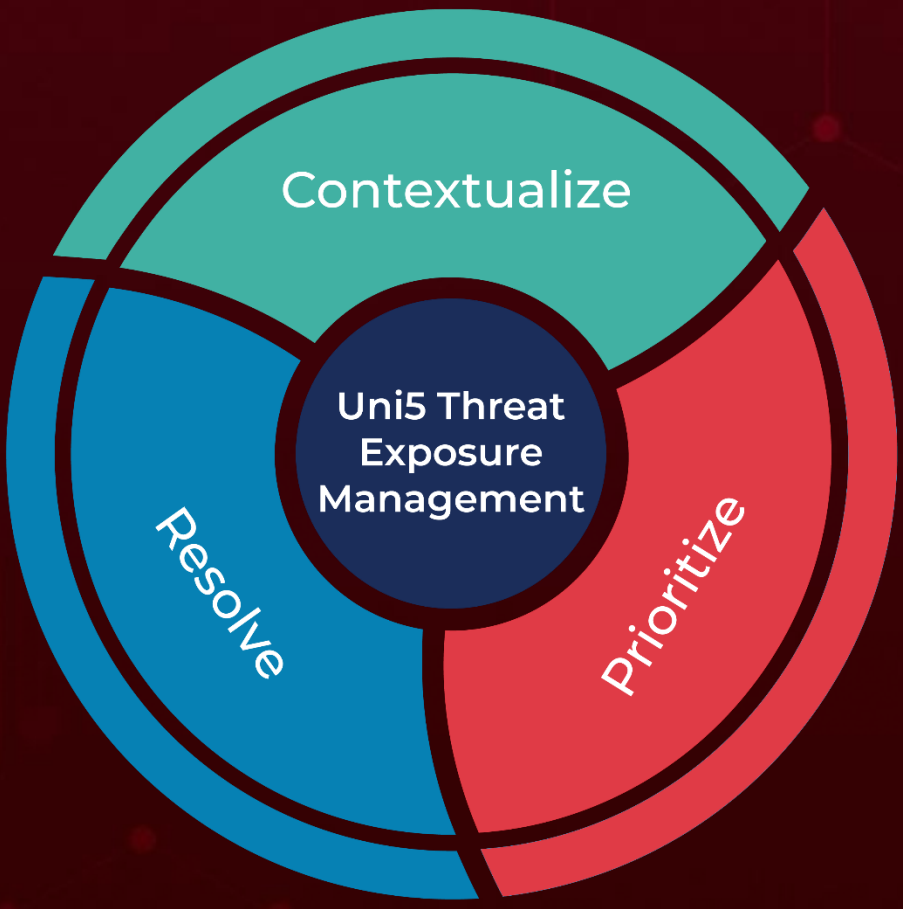
Attack Name	TYPE	VALUE
ScoringMathTea	URLs	hxxps[:]//partnerls[.]pl/wp-content/themes/public/index[.]php, hxxps[:]//trainingpharmacist[.]co[.]uk/bootstrap/bootstrap[.]php, hxxps[:]//mediostresbarbas[.]com[.]ar/php_scrip/banahosting/index[.]php, hxxps[:]//www[.]bandarpowder[.]com/public/assets/buttons/bootstrap[.]php, hxxps[:]//spaincaramoon[.]com/realestate/wp-content/plugins/gravityforms/forward[.]php
BinMergeLoader	SHA1	26AA2643B07C48CB6943150ADE541580279E8E0E

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

October 27, 2025 . 9:30 AM

More at www.hivepro.com