Date of Publication
December 8, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

01 to 07 DECEMBER 2025

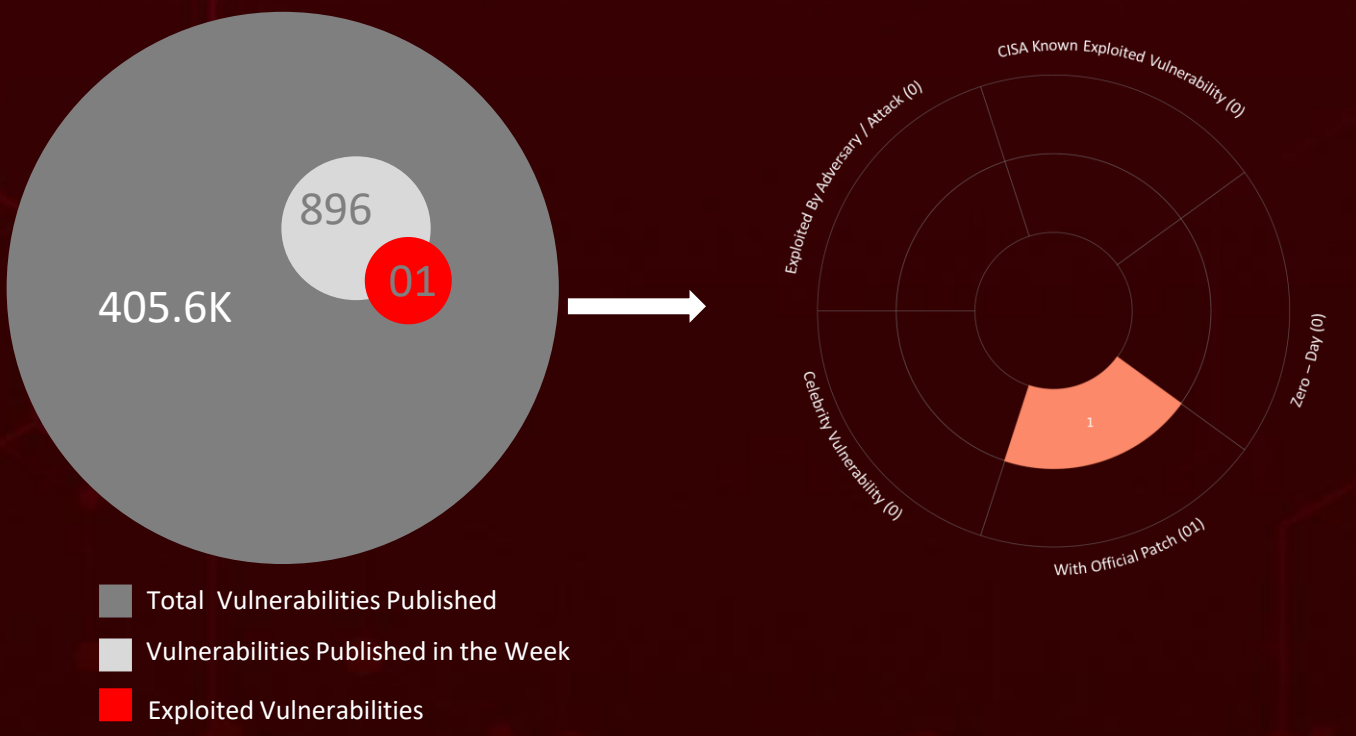
Table Of Contents

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, **ten** major attacks were detected, **one** critical vulnerability was publicly disclosed, and **one** active threat actor group was monitored, signaling a concerning escalation in malicious activity.

One glaring example is a critical flaw in the King Addons for Elementor plugin (**CVE-2025-8489**), which allows attackers to silently grant themselves admin access on vulnerable WordPress sites. Despite a patch released in late September, exploitation surged almost immediately, with over 48,400 malicious attempts blocked. The bug's simplicity, permitting anyone to register as an administrator without authentication, has made it a prime target, illustrating how quickly attackers rush to exploit unpatched software in the wild.

Meanwhile, threat actors are refining their tactics with more stealth and precision. **MuddyWater** has shifted from noisy operations to calculated espionage, using disguised games and trusted tools to infiltrate organizations in Israel and Egypt, deploying custom loaders, backdoors, and credential stealers. Similarly, **Operation Hanoi Thief** hides **LOTUSHARVEST** implants inside seemingly innocent resumes targeting Vietnamese IT and HR teams, while **Water Saci** spreads through WhatsApp with multi-stage Python-based loaders to deliver banking-focused backdoors. These campaigns underscore the urgent need for proactive updates, vigilant monitoring, and layered defenses to stay ahead of rapidly evolving cyber threats.



High Level Statistics

10
Attacks Executed

1
Vulnerabilities Exploited

1
Adversaries in Action

- LOTUSHARVEST
- Fooder
- MuddyViper
- CE-Notes
- LP-Notes
- Blub
- go-socks5
- SORVEPOTEL
- Arkanix
- ValleyRAT
- CVE-2025-8489
- MuddyWater

Insights

A simple file over WhatsApp is all **Water Saci** needs to kick off its multi-stage infection chain and target victims' financial data.

Operation Hanoi Thief: hides malware inside "resumes," quietly slipping LOTUSHARVEST into Vietnamese IT and HR teams.

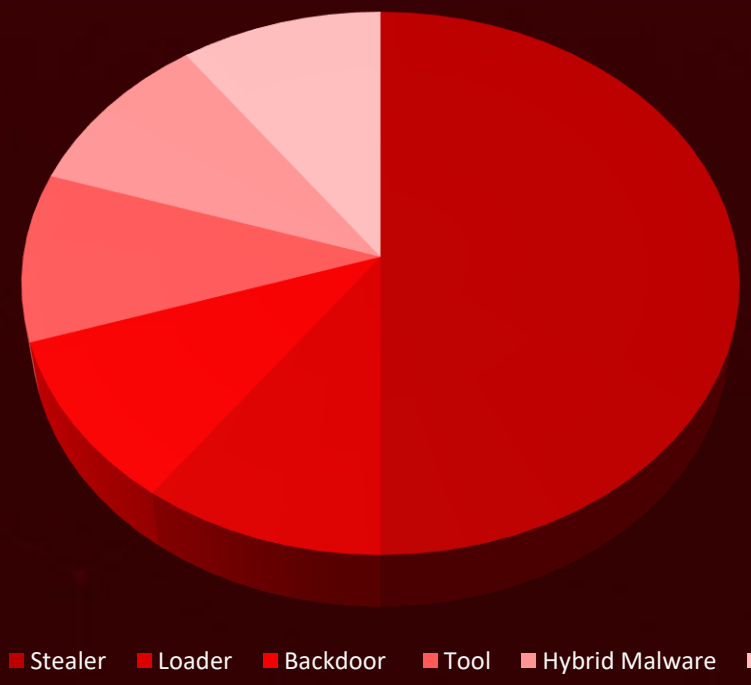
Arkanix Stealer hides behind "legit" tools on Discord and forums, tricking users into running a fast-moving infostealer.

CVE-2025-8489 lets attackers slip into WordPress sites as hidden admins, fueling a spike in real-world takeovers through the King Addons plugin.

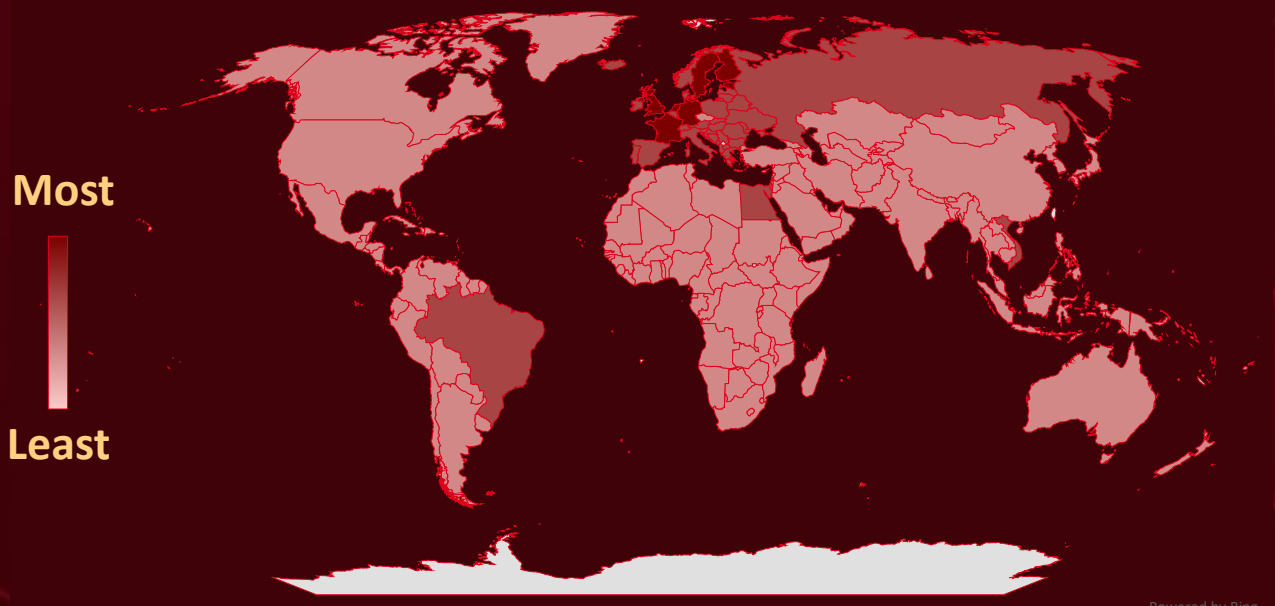
MuddyWater is trading loud tactics for quiet precision, sneaking into Israeli and Egyptian networks through game-themed lures and fake tools.

By mimicking recruitment material, **ValleyRAT** turns job hunting into an attack surface, slipping past defenses with ease.

Threat Distribution



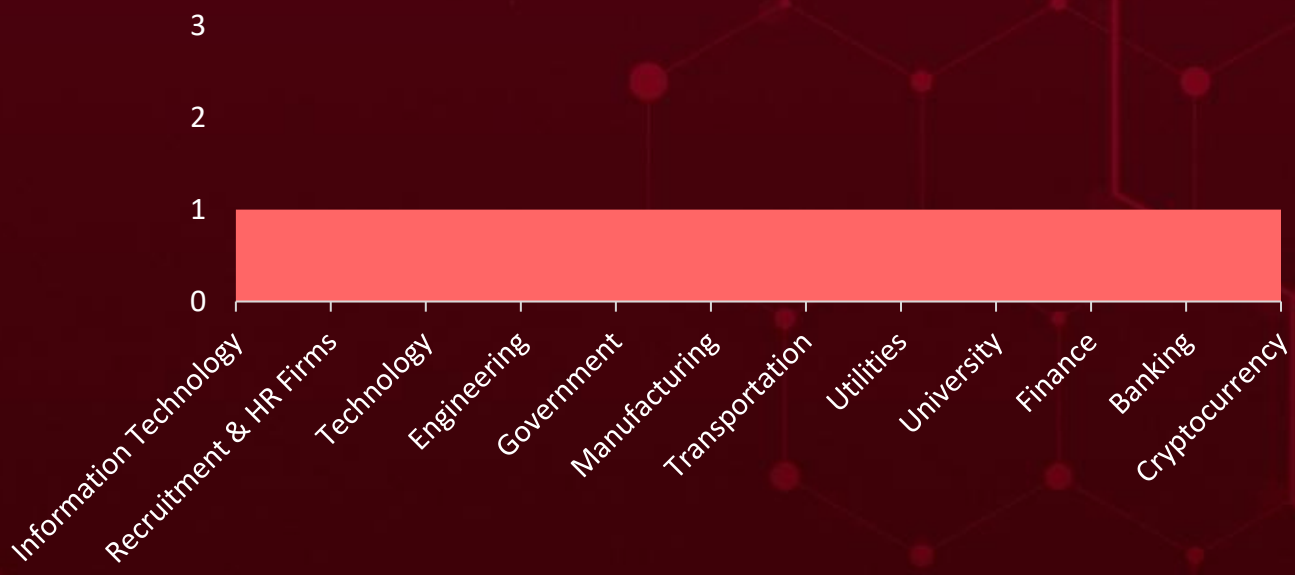
Targeted Countries



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

Countries	Countries	Countries	Countries
France	Malta	Dominican Republic	Syria
Netherlands	Greece	Somalia	Gabon
Germany	Monaco	DR Congo	Tunisia
Estonia	Holy See	Myanmar	Gambia
Sweden	Belgium	Ecuador	United States
Finland	Hungary	Papua New Guinea	Georgia
United Kingdom	Norway	Bahamas	Nauru
San Marino	Iceland	Senegal	Angola
Montenegro	Portugal	El Salvador	Nicaragua
Luxembourg	Ireland	Sudan	Ghana
Bulgaria	Russia	Equatorial Guinea	Central African Republic
Poland	Israel	Uganda	Antigua and Barbuda
Croatia	Serbia	Eritrea	
Spain	Ukraine	Canada	Palau
Denmark	Slovenia	Bahrain	Grenada
Moldova	Vietnam	Oman	Peru
Egypt	Bosnia and Herzegovina	Eswatini	Guatemala
North Macedonia	Liechtenstein	Chile	Qatar
Albania	Brazil	Ethiopia	Guinea
Romania	Lithuania	Samoa	Guyana
Andorra	Italy	Fiji	Seychelles
Slovakia	Latvia	Singapore	Haiti
Austria	Timor-Leste	Bangladesh	Algeria
Switzerland	Comoros	Cuba	Syria
Belarus	Nigeria	Barbados	Gabon

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1041** Exfiltration Over C2 Channel	**T1204** User Execution	**T1036** Masquerading	**T1071** Application Layer Protocol
T1555.003 Credentials from Web Browsers	**T1204.002** Malicious File	**T1027** Obfuscated Files or Information	**T1566** Phishing	**T1555** Credentials from Password Stores
T1082 System Information Discovery	**T1083** File and Directory Discovery	**T1071.001** Web Protocols	**T1140** Deobfuscate/ Decode Files or Information	**T1059.001** PowerShell
T1059.006 Python	**T1573** Encrypted Channel	**T1518** Software Discovery	**T1574.001** DLL	**T1518.001** Security Software Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LOTUSHARVEST	LOTUSHARVEST is a C++-based DLL implant designed to run quietly on a victim's machine via DLL sideloading, blending into legitimate processes to avoid attention. Once active, it focuses on harvesting data from browsers like Google Chrome and Microsoft Edge by opening and reading targeted files to extract stored information. After collecting these details, the implant enriches the stolen data by appending the victim's computer name and username, retrieved through system functions, creating a more complete profile for the attackers.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Steal data	-
Information Stealer			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	48e18db10bf9fa0033affaed849f053bd20c59b32b71855d1cc72f613d0cac4b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Fooder	Fooder is a newly uncovered loader crafted to execute the MuddyViper backdoor, entirely in memory. Several versions of Fooder cleverly disguise themselves as the classic Snake game, an approach that inspired the "MuddyViper" designation. Beneath this harmless façade, the loader uses a custom delay mechanism that mimics the logic of the Snake game, paired with repeated Sleep API calls. This combination intentionally slows down execution to evade automated analysis and obscure its true malicious purpose before deploying the backdoor.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Loads MuddyViper	-
Loader			PATCH LINK
ASSOCIATED ACTOR			-
MuddyWater			
IOC TYPE	VALUE		
SHA1	76632910CF67697BF5D7285FAE38BFCF438EC082,		

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
MuddyViper	MuddyViper is a C/C++ backdoor designed to give attackers extensive control over a compromised system. Once deployed, it can gather detailed system information, execute files and arbitrary shell commands, and handle both file uploads and downloads. Beyond basic control features, MuddyViper also focuses on credential theft, specifically targeting Windows account passwords and browser-stored data, allowing attackers to deepen their access and move further within the victim's environment.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data Theft, System Compromise	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
CE-Notes	CE-Notes is a browser-data stealing tool named after its staging file, ce-notes.txt, which it uses to temporarily store the information it collects. First identified in 2024, this stealer came to light when MuddyWater was seen deploying both EXE and DLL variants of it across compromised systems. Its primary role is to quietly extract sensitive browser data, adding another layer to the group's broader espionage toolkit.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	-
Browser-data Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-
IOC TYPE	**VALUE**		
SHA1	8E21DE54638A79D8489C59D958B23FE22E90944A, CD47420F5CE408D95C98306D78B977CDA0400C8F, C1299E8C9A8567A9C292157F3ED65B818AA78900		

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
LP-Notes	LP-Notes is a C/C++-based Windows credential stealer built with the same design philosophy as the CE-Notes browser-data stealer but focused entirely on harvesting login credentials. Its only purpose is to trick victims into entering their Windows username and password by presenting a convincing fake Windows Security dialog. Once displayed, the prompt encourages users to "re-authenticate," effectively handing their credentials to the attacker. LP-Notes delivered and launched via PowerShell using command lines nearly identical to those associated with CE-Notes.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal data	-
Credential Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-
IOC TYPE	**VALUE**		
SHA1	29CDA06701F9A9C0A6791775C3EB70F5B52BBEFF, 8F3ED626E7B929450E36E97BA5539C8371DF0EF8		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Blub	Blub is a C/C++ browser-data stealer named after its executable, Blub.exe, and is built with a statically linked SQLite library to make data extraction seamless. Once running, it targets major web browsers, including Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera, to pull stored login credentials directly from their local databases.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Steal Data	-
Browser-data Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-
IOC TYPE	**VALUE**		
SHA1	1723D5EA7185D2E339FA9529D245DAA5D5C9A932, 69B097D8A3205605506E6C1CC3C13B71091CB519, B7A8F09CB5FF8A33653988FFBA585118ACF24C13		

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
go-socks5	MuddyWater's go-socks5 reverse tunnels are a set of Go-compiled proxy tools built on publicly available libraries like go-socks5, yamux, and resocks, and they have become a staple in the group's recent operations. These tools function as intermediaries, relaying traffic from a compromised machine, over a designated port, to a hardcoded C&C server, authenticating the connection with an embedded key over SSL/TLS.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Stealthy persistence	-
Tool			
ASSOCIATED ACTOR			**PATCH LINK**
MuddyWater			-
IOC TYPE	**VALUE**		
SHA1	25361183DE63F296BA71B6FCF0725E022B3C989A, 0E9A4892CFA1C9065B36D8F2E164E28609A8CF5D, 2B09241CA025BDC4455E9F6BA6009E2F27C08EDF		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SORVEPOTEL	Water Saci is a malicious campaign that spreads SORVEOTEL, a hybrid malware. It uses deceptive messages with ZIP attachments that execute PowerShell commands to load additional payloads directly into memory. SORVEOTEL can hijack active WhatsApp Web sessions to propagate infected files to contacts and deploy convincing banking overlays to harvest credentials.	Spear-phishing via WhatsApp	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Credential Theft, Financial Loss	Windows
Hybrid Malware			
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	2d95769a016b397333ba90fdc2f668f883c64774a2c0aaaf6b2d942bebaee9e0		

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">Arkanix</td><td rowspan="5">Arkanix is a fast-moving, financially motivated infostealer designed for quick monetization rather than long-term campaigns. It targets a broad spectrum of Chromium-based browsers and cryptocurrency extensions, while also harvesting wallet data from standalone clients like Electrum and various Ethereum applications. Initially released as a Python-based stealer, distributed through Discord channels and online forums where it was disguised as harmless tools, it was packaged with Nuitka to compile the Python code into bytecode. Within a month, the operators replaced it with a more capable C++ version, promoted as a “Premium” build on their web panel. This upgraded edition expands its reach by adding modules to steal VPN credentials and Steam accounts, positioning Arkanix as a commodity stealer aimed at rapid, high-volume financial gain.</td><td>circulated through Discord and underground forums</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>TYPE</td><td rowspan="3">Steal Data</td><td>-</td></tr>
<tr><td>Stealer</td><td rowspan="2">PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">-</td></tr>
<tr><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">6ea644285d7d24e09689ef46a9e131483b6763bc14f336060afaeffe37e4beb5, 6960d27fea1f5b28565cd240977b531cc8a195188fc81fa24c924da4f59a1389</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">ValleyRAT</td><td rowspan="5">ValleyRAT is a remote access trojan (RAT) designed to infiltrate systems and give attackers unauthorized control. It adds new capabilities, including screenshot capture, process filtering, forced shutdown, and clearing Windows event logs to cover its tracks.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>TYPE</td><td rowspan="3">Service Disruption, Remote Access, Data Theft</td><td>-</td></tr>
<tr><td>RAT</td><td rowspan="2">PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">-</td></tr>
<tr><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">a32fa6ba08db96ebd611f6ee06da44b419d569a6bac43ed00c68d6ca674004c3</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 PRODUCT	ASSOCIATED ACTORS
CVE-2025-8489	✗	WordPress King Addons for Elementor Plugin Versions 24.12.92 to 51.1.14	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:kingaddons:king_addons_for_elementor_plugin:*:*:*:*:*:*:*:*	-
WordPress King Addons for Elementor Plugin Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://wordpress.org/plugins/king-addons/

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, G0069)	Iran	Technology, Engineering, Government, Manufacturing, Transportation, Utilities, University	Israel and Egypt
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	Fooder loader, MuddyViper, CE-Notes, LP-Notes, Blub, go-socks5	-

TTPs

TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1591: Gather Victim Org Information; T1583: Acquire Infrastructure; T1608: Stage Capabilities; T1587: Develop Capabilities; T1587.001: Malware; 1588: Obtain Capabilities; T1588.002: Tool; T1566: Phishing; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1559: Inter-Process Communication; T1559.001: Component Object Model; T1106: Native API; T1204: User Execution; T1204.001: Malicious Link; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1543: Create or Modify System Process; T1543.003: Windows Service; T1053: Scheduled Task/Job; T1134: Access Token Manipulation; T1134.001: Token Impersonation/Theft; T1140: Deobfuscate/Decode Files or Information; T1620: Reflective Code Loading; T1497: Virtualization/Sandbox Evasion; T1497.003: Time Based Checks; T1027: Obfuscated Files or Information; T1027.007: Dynamic API Resolution; T1134.002: Create Process with Token; T1622: Debugger Evasion; T1070: Indicator Removal; T1622: Clear Persistence; T1070.004: File Deletion; T1036: Masquerading; T1036.004: Masquerade Task or Service; T1112: Modify Registry; T1027.009: Embedded Payloads; T1027.013: Encrypted/Encoded File; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1056: Input Capture; T1056.002: GUI Input Capture; T1082: System Information Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1074: Data Staged; T1074.001: Local Data Staging; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1219: Remote Access Tools; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer; T1001: Data Obfuscation; T1090: Proxy; T1041: Exfiltration Over C2 Channel; T1030: Data Transfer Size Limits

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 actor **MuddyWater,** and malware **LOTUSHARVEST, Fooder loader, MuddyViper, CE-Notes, LP-Notes, Blub, go-socks5, SORVEPOTEL, Arkanix,** and **ValleyRAT.**

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 actor **MuddyWater,** and malware **LOTUSHARVEST, go-socks5, SORVEPOTEL, Arkanix,** and **ValleyRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

Operation Hanoi Thief: When Fake CVs Become Cyber Weapons

Serpents in Disguise: MuddyWater’s Hidden Toolset Exposed

The Admin Shortcut: King Addons Flaw Under Fire

Water Saci Campaign: Multi-Stage Malware Spreading via WhatsApp Web

Arkanix Stealer's Fast-Evolving Design Driving Widespread Compromise

ValleyRAT’s Stealthy Job-Lure Campaign

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
LOTUSHARVEST	SHA256	48e18db10bf9fa0033affaed849f053bd20c59b32b71855d1cc72f613d0cac4b
Fooder	SHA1	76632910CF67697BF5D7285FAE38BFCF438EC082,
CE-Notes	SHA1	8E21DE54638A79D8489C59D958B23FE22E90944A, CD47420F5CE408D95C98306D78B977CDA0400C8F, C1299E8C9A8567A9C292157F3ED65B818AA78900
LP-Notes	SHA1	29CDA06701F9A9C0A6791775C3EB70F5B52BBEFF, 8F3ED626E7B929450E36E97BA5539C8371DF0EF8
Blub	SHA1	1723D5EA7185D2E339FA9529D245DAA5D5C9A932, 69B097D8A3205605506E6C1CC3C13B71091CB519, B7A8F09CB5FF8A33653988FFBA585118ACF24C13, B8997526E4781A6A1479690E30072F38E091899D
go-socks5	SHA1	25361183DE63F296BA71B6FCF0725E022B3C989A, 0E9A4892CFA1C9065B36D8F2E164E28609A8CF5D, 2B09241CA025BDC4455E9F6BA6009E2F27C08EDF, 2E9BE23CDD8152DB6CD1A54E001C4EA82FF6F1C6, 45FA7DE711FEA1F8D1E348E87834246C455DD2ED, 4E0EF2386980639FC5355FD68DAFF54EB2AD622E, 4E9529BA4A6E42D6278D37E3FDEE9E1D991CEBE0, 50C6D4A2AD16A231CF11C43F3BBC868D90E20D25, 52009F36058337B6401DA0A0F4885A0C185F0520, 535882B6EDAB29247E035236A84CA510FB1E0854, 544CE18E4C1F1B288DEE6018DFCF4E4D4A315F7A, 54EBC125039CC83E4682CA44DD592534562B25C3, 5A08150C1DC17E9F691296F0A577C2EC9BA8028C, 5D1E61DA8083C41FF1FC23A1222A4A88B43A4E9B,

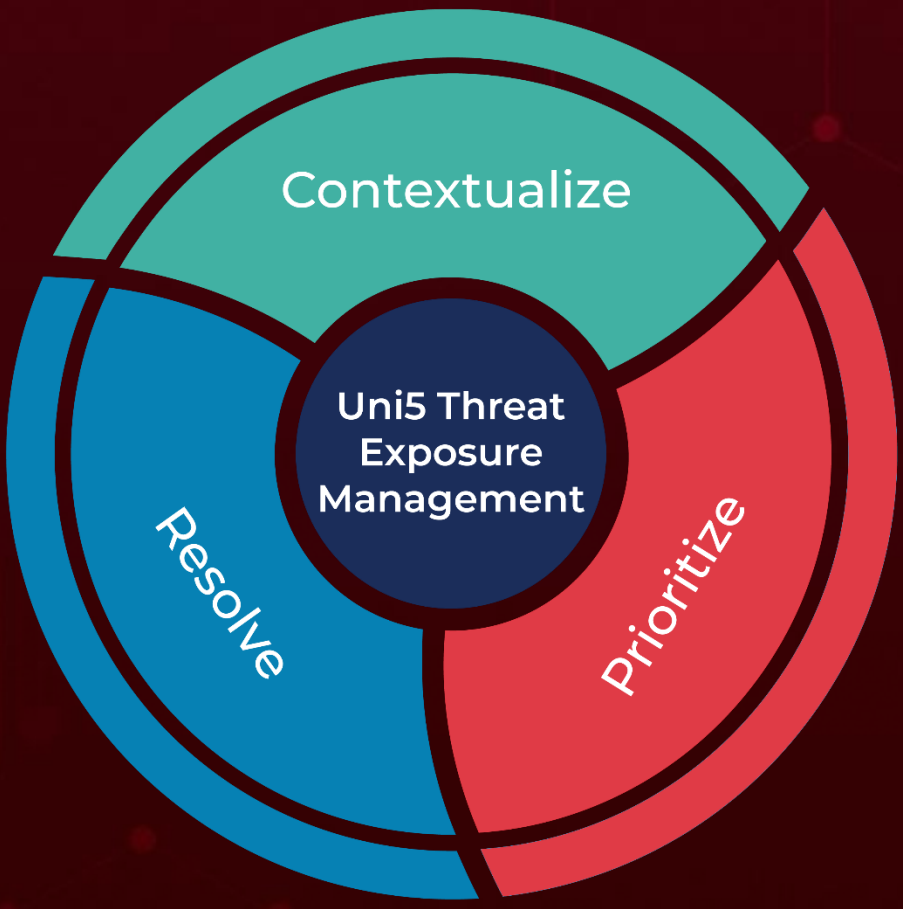
Attack Name	TYPE	VALUE
go-socks5	SHA1	6532E0437C8913FA418F1EE258561B15BBEE9052, 6CA41565844118385B345A39A9B79E0BBC0DD338, 6FC50A99AAE1D6C40111632D4F49BD19F9794CF6, 826CFF5D85713CE4B2F3C15AB53A84E6848D2E2C, 87ADD79C7C8335447113EE0D413F52AE2B17F066, 93055115559219BE8441880597C533381B99213B, 97C3376AB551E899F347CC9DDF49EA01DB2D7903, 99FAD0862E2E8D363F3E18952FD92E09493CC27D, A101CBCCD950AA36FC3B40C3C331FDE43ACDBBD2, A227C0A4425E24268B759A740231676A589CA4E6, A997A7AAE727D2C12CCE80FE3607317775A4DF3E, B0271CA76052EC340014D7BCCDBD69325A4E60F2, B0CD4F5DF192BFFE6500E44B80C28505DFD9CA66, B16E7D56A8DC0FF6B3AFD797E1EAB22B20DFFB39, D49979D0063B28BD73390481E6AE642C00CE0791, D518F5C648AB64B390A29AA2858219318CFC556A, DF223D653F761ED55F9C0774F1DBF545FD741F86, DF8FC5213AA11EE445EAD1AAE17A826E7D51A743, E02DD79A8CAED662969F6D5D0792F2CB283116E8, E8F4EA3857EF5FDFEC1A2063D707609251F207DB, F26CAE9E79871DF3A47FA61A755DC028C18451FC, FF09608790077E1BA52C03D9390E0805189ADAD7, A9747A3F58F8F408FECEFC48DB0A18A1CB6DACAE
SORVEPOTEL	SHA256	2d95769a016b397333ba90fdc2f668f883c64774a2c0aaaf6b2d942bebaee9e0
Arkanix	URLs	hxxps[:]//arkanix[.]pw/stealer[.]py, hxxps[:]//arkanix[.]pw/delivery, hxxps[:]//arkanix[.]pw/api/upload/direct
	Domain	arkanix[.]pw
	SHA256	6ea644285d7d24e09689ef46a9e131483b6763bc14f336060afaeffe37e4beb5, 6960d27fea1f5b28565cd240977b531cc8a195188fc81fa24c924da4f59a1389
ValleyRAT	SHA256	a32fa6ba08db96ebd611f6ee06da44b419d569a6bac43ed00c68d6ca674004c3

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

December 8, 2025 . 10:00 AM

More at www.hivepro.com