Date of Publication
April 21, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

13 to 19 April 2026

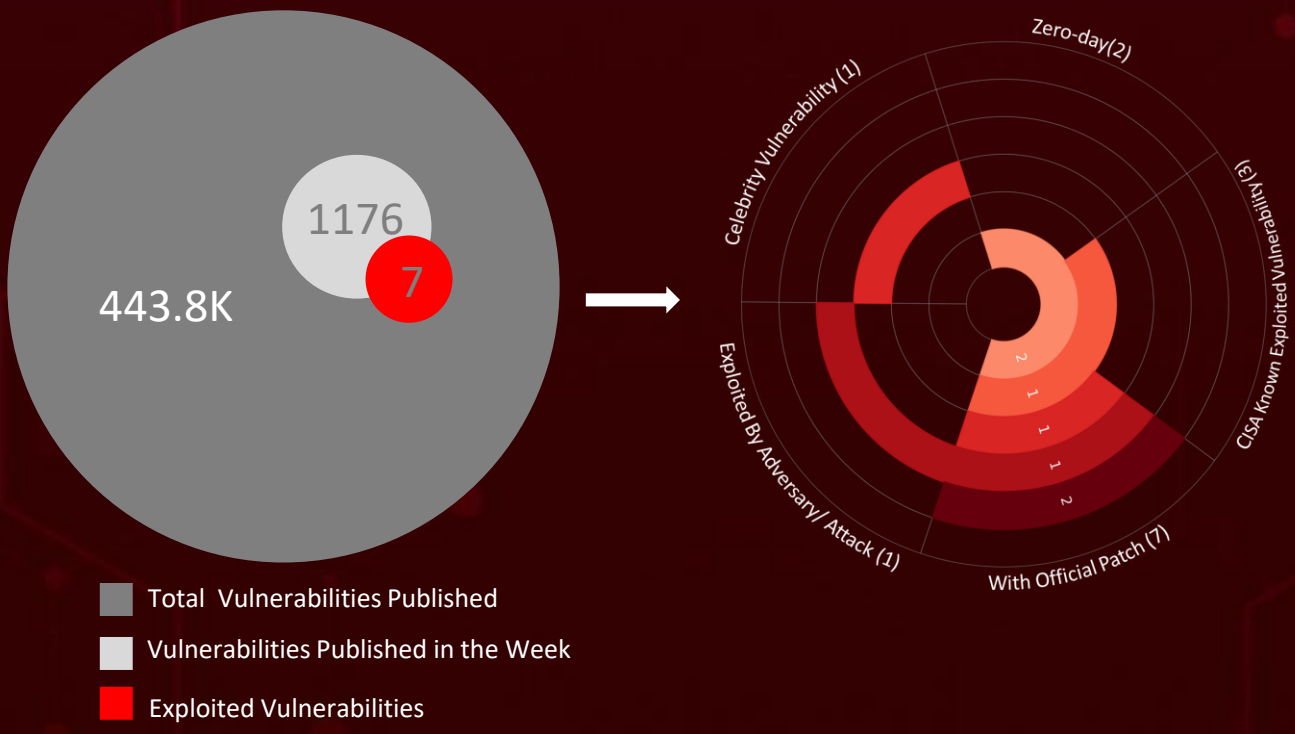
Table Of Contents

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, **four** major attacks were detected, **seven** critical vulnerabilities were actively exploited, and **two** threat actors were closely monitored, reflecting an alarming escalation in malicious activities.

CVE-2026-34621 Adobe Acrobat/Reader Critical prototype pollution flaw in the JavaScript engine, exploited via crafted PDFs to trigger privileged APIs like util.readFileIntoStream() for local file access, with data exfiltrated via RSS.addFeed() to attacker-controlled servers. **Handala Hack Team** Iran-affiliated threat group launched a destructive campaign against GCC critical infrastructure, allegedly wiping 6 PB of data and exfiltrating 149 TB of classified documents via compromised VPN credentials, infostealer-harvested accounts, and targeted phishing.

Meanwhile, **Storm-2755** Payroll Heist Financially motivated group leveraging CVE-2025-27152 in Axios and AiTM phishing via fake Microsoft 365 login pages to capture session tokens, bypass MFA, and reroute salary payments through Workday HR systems. **PHANTOMPULSE** Multi-stage social engineering campaign weaponizing Obsidian community plugins to deliver the PHANTOMPULL loader and PHANTOMPULSE RAT, using LinkedIn and Telegram lures with Ethereum blockchain as a dead-drop C2 resolver. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

4
Attacks Executed

7
Vulnerabilities Exploited

2
Adversaries in Action

- Handala Wiper
- Payouts King Ransomware
- PHANTOMPULSE
- PHANTOMPULL

- CVE-2026-34621
- CVE-2026-39987
- CVE-2025-27152
- CVE-2026-32201
- CVE-2026-5281
- CVE-2026-33825
- CVE-2026-33032

- Handala Hack Team
- Storm-2755

Insights

PHANTOMPULSE AI-built .NET RAT delivered via Obsidian plugins after LinkedIn lures, uses Ethereum blockchain as dead-drop C2.

Handala Hack Team Iran-linked threat group hit GCC critical infrastructure, wiping 6 PB and stealing 149 TB via compromised VPNs and phishing.

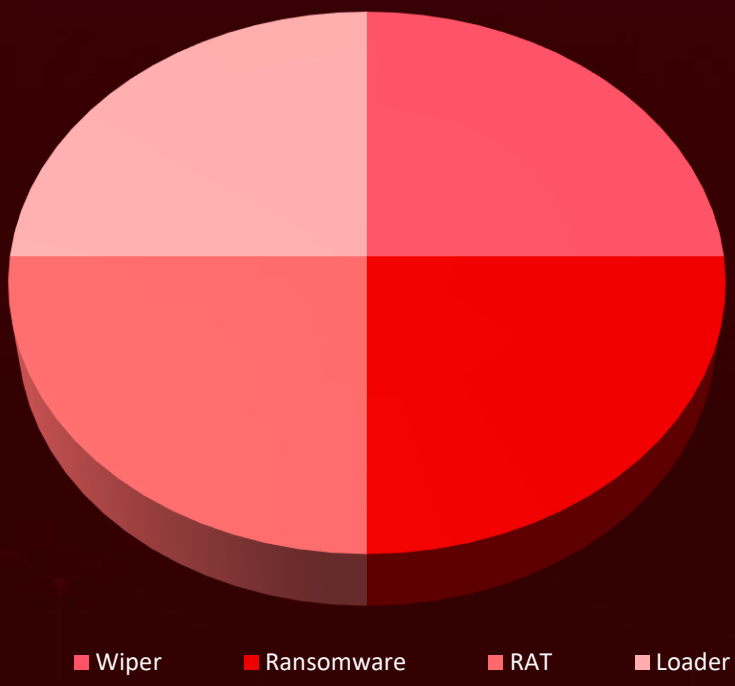
MCPwn (CVE-2026-33032) Auth bypass in Nginx UI ≤2.3.5 lets unauthenticated attackers invoke MCP tools via JSON-RPC to alter configs.

Payouts King Ransomware Ex-BlackBasta crew uses spam-bombing and Teams vishing with Quick Assist to deploy ransomware and kill EDR via direct syscalls.

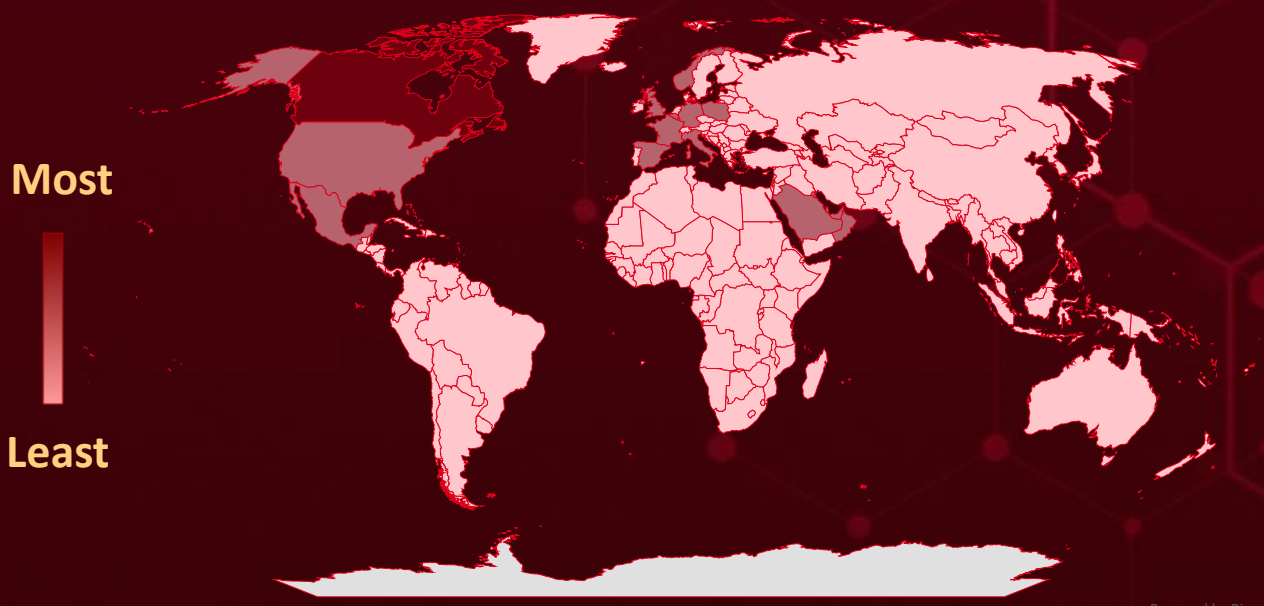
Storm-2755 AiTM phishing via fake M365 logins steals session tokens, bypasses MFA, and reroutes salaries through Workday.

CVE-2026-39987 Marimo Pre-auth RCE in Python notebook platform, exposed WebSocket grants full shell, exploited within 10 hours.

Threat Distribution

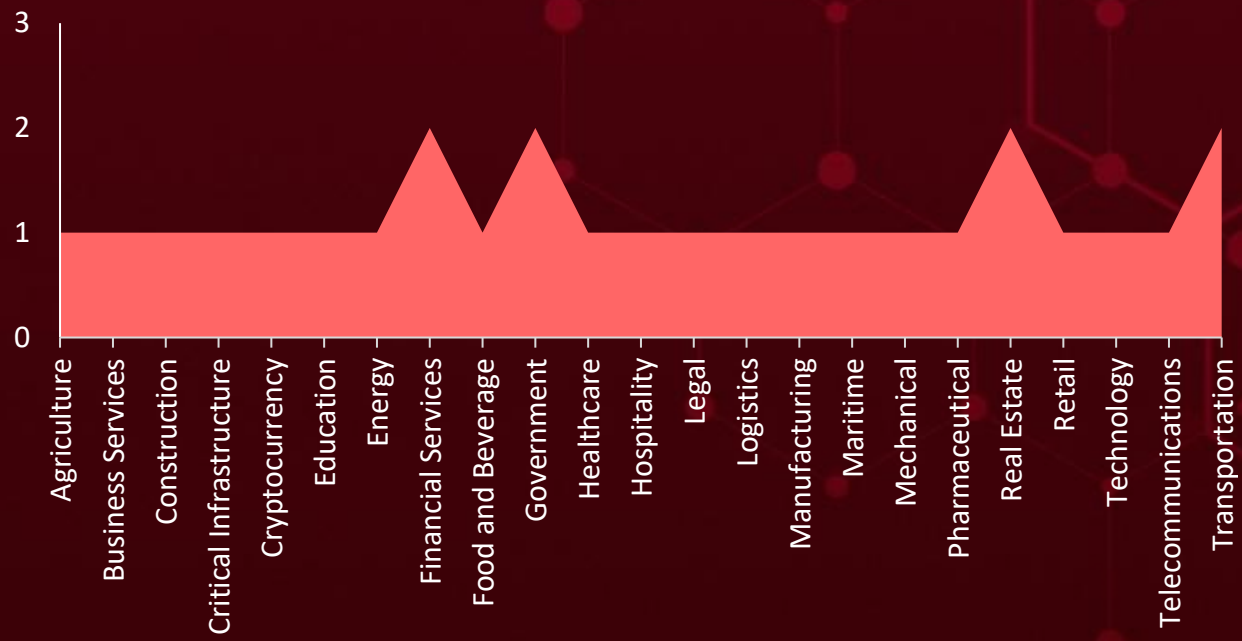


Targeted Countries



Countries	Countries	Countries	Countries
Canada	Benin	Albania	Nauru
Bahrain	Nigeria	Cameroon	Cuba
Poland	Bhutan	Bangladesh	Nicaragua
Norway	Solomon Islands	Andorra	Cyprus
Belgium	Bolivia	Saint Lucia	North Macedonia
Saudi Arabia	Malawi	Central African Republic	Czech Republic
United Arab Emirates	Bosnia and Herzegovina	Sierra Leone	Palau
United States	Myanmar	Chad	Denmark
Mexico	Botswana	South Sudan	Peru
France	Papua New Guinea	Chile	Djibouti
Oman	Brazil	China	Barbados
Germany	Belarus	Trinidad and Tobago	Dominica
Qatar	Brunei	Colombia	Rwanda
Italy	State of Palestine	Luxembourg	Dominican Republic
Spain	Bulgaria	Comoros	San Marino
Kuwait	Tuvalu	Maldives	DR Congo
United Kingdom	Burkina Faso	Congo	Serbia
Romania	Malta	Mauritania	Ecuador
Azerbaijan	Burundi	Costa Rica	Slovakia
Thailand	Mongolia	Moldova	Egypt
	Cabo Verde	Côte d'Ivoire	South Africa
	Netherlands	Morocco	El Salvador
	Cambodia	Croatia	Sri Lanka
			Equatorial Guinea

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter

T1566 Phishing

T1190 Exploit Public-Facing Application

T1204 User Execution

T1588 Obtain Capabilities

T1557 Adversary-in-the-Middle

T1068 Exploitation for Privilege Escalation

T1555 Credentials from Password Stores

T1071 Application Layer Protocol

T1082 System Information Discovery

T1078 Valid Accounts

T1027 Obfuscated Files or Information

T1071.001 Web Protocols

T1083 File and Directory Discovery

T1566.001 Spearphishing Attachment

T1059.001 PowerShell

T1204.001 Malicious Link

T1588.006 Vulnerabilities

T1021 Remote Services

T1041 Exfiltration Over C2 Channel

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Handala	Handala Wiper is a custom destructive malware deployed via Group Policy logon scripts as handala.bat, enabling it to execute remotely from the Domain Controller without being written to disk on target systems. It is designed to overwrite files across the system and corrupt the Master Boot Record (MBR), leading to severe, low-level data destruction and system inoperability. The wiper also leverages the Telegram Bot API for command-and-control communication, helping operators manage attacks while maintaining a level of stealth.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Data destruction	Windows
Wiper			
ASSOCIATED ACTOR			**PATCH LINK**
Handala Hack			-

IOC TYPE	VALUE
SHA256	454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567, 96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8

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
Payouts King	Payouts King is a new ransomware operation first observed in April 2025, assessed with high confidence to be run by former BlackBasta affiliates. It uses AES-256 (CTR) with RSA-4096 and intermittent encryption for large files, combined with heavy obfuscation and direct syscalls to bypass EDR. Double-extortion operation combining data theft with selective file encryption.	Vishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		File encryption, data exfiltration	Windows
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	335ad12a950f885073acdfebb250c93fb28ca3f374bbba5189986d9234dcbff4, d68ce82e82801cd487f9cd2d24f7b30e353cafd0704dcdf0bb8f12822d4227c2		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
PHANTOMPULSE	PHANTOMPULSE Is a novel, AI-assisted Windows .NET RAT featuring blockchain-based C2 resolution, tracked under campaign REF6598. It targets finance and cryptocurrency professionals, providing full host control including keylogging, screenshots, file upload/download, and shellcode/DLL injection. It queries transaction data from wallets on Ethereum, Base, and Optimism to dynamically resolve its active C2 server.	Obsidian plugin abuse	-
		IMPACT	AFFECTED PRODUCT
TYPE		Remote access, credential theft	Windows, macOS
RAT			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	33dacf9f854f636216e5062ca252df8e5bed652efd78b86512f5b868b11ee70f		
Domain	panel[.]fefea22134[.]net		

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">PHANTOMPULL</td><td rowspan="5">PHANTOMPULL is a custom first-stage loader deployed on Windows that decrypts and reflectively loads the PHANTOMPULSE RAT payload entirely in memory. It uses AES-256-CBC encryption and includes anti-analysis techniques to avoid detection. Delivered through abuse of Obsidian's community plugin ecosystem (Shell Commands and Hider plugins) when a victim opens a shared cloud vault.</td><td>Obsidian plugin abuse</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">In-memory payload loading</td><td rowspan="2">Windows, macOS</td></tr>
<tr><td>Loader</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">70bbb38b70fd836d66e8166ec27be9aa8535b3876596fc80c45e3de4ce327980</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-2026-34621		Adobe Acrobat DC (26.001.21367 and earlier), Adobe Acrobat Reader DC (26.001.21367 and earlier), Adobe Acrobat 2024 (24.001.30356 and earlier)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:acrobat_dc:*:*:*:*:continuous:*:*:* cpe:2.3:a:adobe:acrobat_reader_dc:*:*:*:*:continuous:*:*:* cpe:2.3:a:adobe:acrobat:*:*:*:*:classic:*:*:*	-
Adobe Acrobat and Reader Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1321	T1203: Exploitation for Client Execution, T1059.007 Command and Scripting Interpreter: JavaScript	https://helpx.adobe.com/security/products/acrobat/apsb26-43.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-39987	✗	Marimo versions before 0.23.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:marimo-team:marimo:*:*:*:*:*:python:*:*	-
Marimo Terminal WebSocket Pre-Auth Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059.006 Command and Scripting Interpreter: Python	https://github.com/marimo-team/marimo/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-27152	✗	Axios version before 1.8.2	Storm-2755
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:axios:axios:*:*:*:*:*:node.js:*:*	-
Axios SSRF and Credential Leakage Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	https://github.com/axios/axios/releases/tag/v1.8.2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-32201		Microsoft Office SharePoint Server	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:subscription:*:*:*	-
Microsoft SharePoint Server Spoofing Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190 Exploit Public-Facing Application, T1036 Masquerading, T1656 Impersonation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-5281	ZERO-DAY	Microsoft Edge (Chromium-based), Google Chrome	-
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Chromium Use after free in Dawn Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1189 Drive-by Compromise, T1203 Exploitation for Client Execution, T1068 Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281, https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-33825	✗	Microsoft Defender	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:microsoft_defender:*:*:*:*:*:*:*:*	-
Microsoft Defender Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1220	T1068 Exploitation for Privilege Escalation, T1562.001 Impair Defenses: Disable or Modify Tools, T1006 Direct Volume Access	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-33032	MCPwn	Nginx UI (all versions through v2.3.5)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:nginxui:nginx_ui:*:*:*:*:*:*:*:*	-
Nginx Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190 Exploit Public-Facing Application, T1505 Server Software Component, T1565.002 Data Manipulation: Transmitted Data Manipulation	https://github.com/0xJacky/nginx-ui/releases

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Handala Hack (aka HomeLand Justice, Karma, Storm-0842, Banished Kitten, Void Manticore)</td><td>Iran</td><td rowspan="2">Government, Real Estate, Legal, Transportation, and Critical Infrastructure</td><td rowspan="2">Gulf Cooperation Council (GCC)</td></tr>
<tr><td>MOTIVE
Espionage, Sabotage, Geopolitical disruption, Politically and ideologically motivated</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Handala</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development, TA0001: Initial Access, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1078: Valid Accounts, T1110: Brute Force, T1566: Phishing, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1133: External Remote Services, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1484: Domain or Tenant Policy Modification, T1003: OS Credential Dumping, T1003.001: LSASS Memory, T1003.002: Security Account Manager, T1087: Account Discovery T1087.002:Domain Account, T1021: Remote Services T1021.001: Remote Desktop Protocol, T1572: Protocol Tunneling, T1105: Ingress Tool Transfer Exfiltration, T1041: Exfiltration Over C2 Channel Impact, T1485: Data Destruction, T1561: Disk Wipe, T1561.002: Disk Structure Wipe,, T1486: Data Encrypted for Impact, T1005: Data from Local System, T1560: Archive Collected Data, T1583: Acquire Infrastructure, T1583.001: Domains, T1583.006: Web Services, T1585: Establish Accounts</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Storm-2755</td><td>Iran</td><td rowspan="3">-</td><td rowspan="3">Canada</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-27152</td><td>-</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development, TA0001: Initial Access, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, TA0040: Impact, T1608: Stage Capabilities, T1608.005: Link Target, T1583: Acquire Infrastructure, T1583.001: Domains, T1566: Phishing, T1566.003: Spearphishing via Service, T1189: Drive-by Compromise, T1557: Adversary-in-the-Middle, T1539: Steal Web Session Cookie, T1078: Valid Accounts, T1078.004: Cloud Accounts, T1098: Account Manipulation, T1087: Account Discovery, T1114: Email Collection, T1114.002: Remote Email Collection, T1564: Hide Artifacts, T1564.008: Email Hiding Rules, T1534: Internal Spearphishing, T1657: Financial Theft</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 actor **Handala Hack, Storm-2755** and malware **Handala Wiper, Payouts King Ransomware, PHANTOMPULSE, PHANTOMPULL.**

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 **Handala Hack** and malware **Handala Wiper, Payouts King Ransomware, PHANTOMPULSE, PHANTOMPULL,** in Breach and Attack Simulation(BAS).

Threat Advisories

Active Exploitation of Critical Adobe Prototype Pollution Flaw

Handala Claims Destructive Wiper Attack on GCC Nation's Critical Infrastructure

From Advisory to Attack in Under 10 Hours: Marimo's Critical RCE Flaw

Storm-2755's Silent Payroll Heist Targeting Canada

Microsoft's April 2026 Patch Tuesday

MCPwn: Critical Nginx UI Bug Opens the Door to Remote Control

Payouts King Ransomware Blending In Before Breaking Through

Inside the PHANTOMPULSE Social Engineering Kill Chain

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)

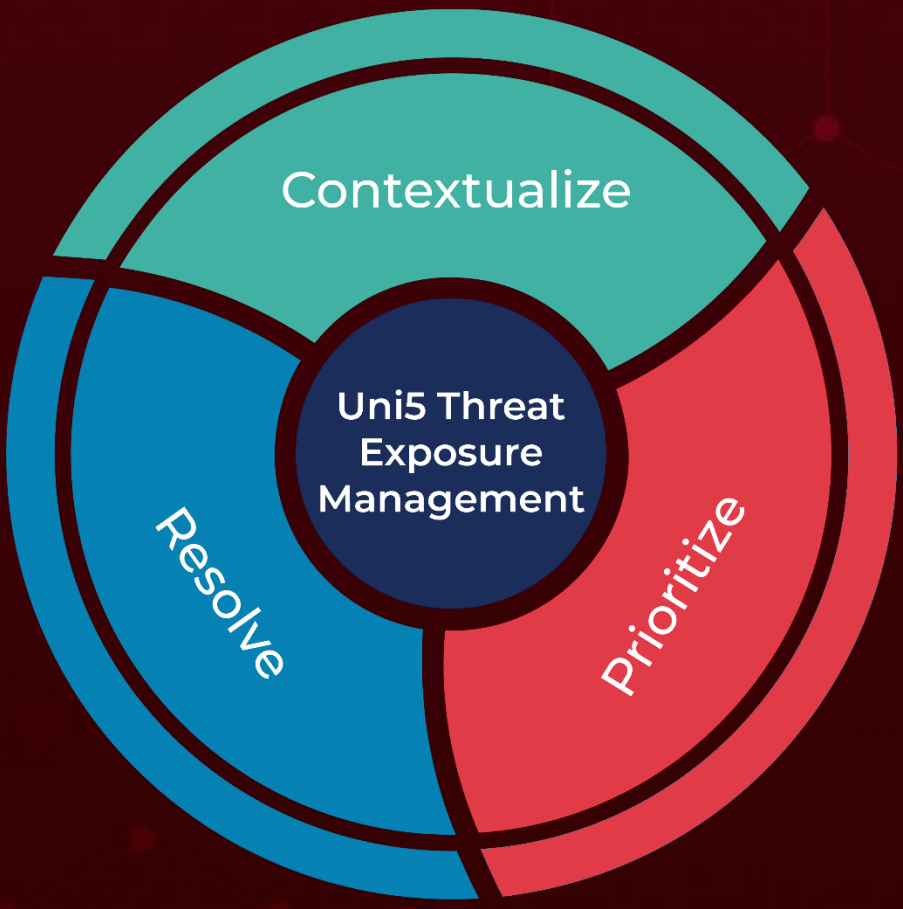
Attack Name	TYPE	VALUE
Handala Wiper	MD5	5986ab04dd6b3d259935249741d3eff2
	SHA256	454e6d3782f23455875a5db64e1a8cd8eb743400d8c6dadb1cd8fd2ffc2f9567, 96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8
Payouts King	SHA256	335ad12a950f885073acdfebb250c93fb28ca3f374bbba5189986d9234dcbff4, d68ce82e82801cd487f9cd2d24f7b30e353cafd0704dcdf0bb8f12822d4227c2
PHANTOMPULSE	SHA256	33dacf9f854f636216e5062ca252df8e5bed652efd78b86512f5b868b11ee70f
	Domain	panel[.]fefea22134[.]net
PHANTOMPULL	SHA256	70bbb38b70fd836d66e8166ec27be9aa8535b3876596fc80c45e3de4ce327980

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 21, 2026 • 01:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com