Date of Publication
January 19, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

12 to 18 January 2026

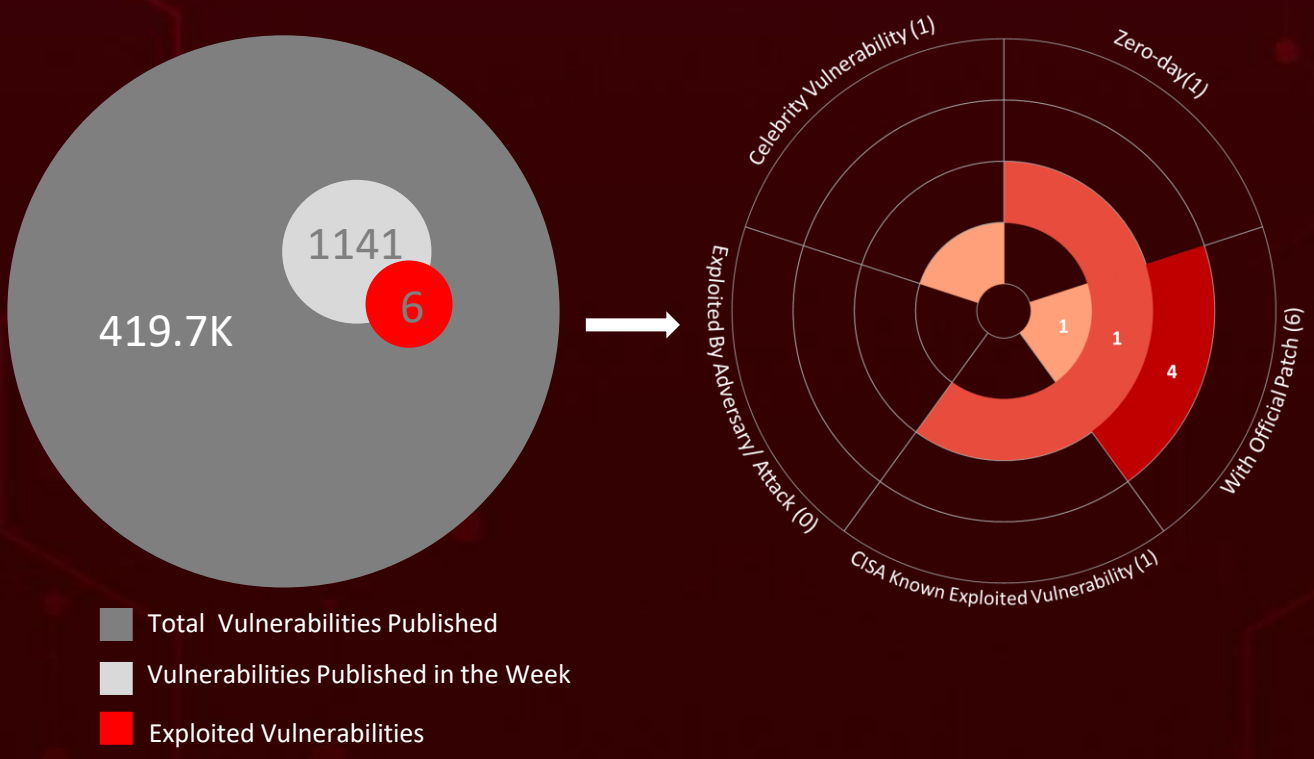
Table Of Contents

Summary

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

CVE-2026-23550 allows unauthenticated attackers to fully compromise WordPress sites via an actively exploited authentication bypass in the Modular DS Connector plugin. **CVE-2025-64155** lets unauthenticated attackers fully compromise on-prem FortiSIEM systems, with active PoCs raising urgent exploitation risk.

Meanwhile, **MuddyWater** has advanced its attack tradecraft by adopting Rust-based implants and sophisticated delivery techniques, signaling a strategic evolution beyond its traditional PowerShell and VBS tooling. **UAT-7290** conducts long-term espionage against telecom networks while repurposing compromised infrastructure as covert relays for broader China-aligned operations. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

7
Attacks Executed

6
Vulnerabilities Exploited

2
Adversaries in Action

- RustyWater
- RushDrop
- DriveSwitch
- SilentRaid
- Bulbature
- AsyncRAT
- VoidLink

- CVE-2026-20805
- CVE-2026-21265
- CVE-2023-31096
- CVE-2025-64155
- CVE-2026-21858
- CVE-2026-23550

- MuddyWater
- UAT-7290

Insights

MuddyWater is evolving by using Rust-based malware and advanced phishing techniques to enhance stealth and persistence.

Ni8mare (CVE-2026-21858) turns exposed n8n instances into high-impact entry points that can cascade into full infrastructure compromise.

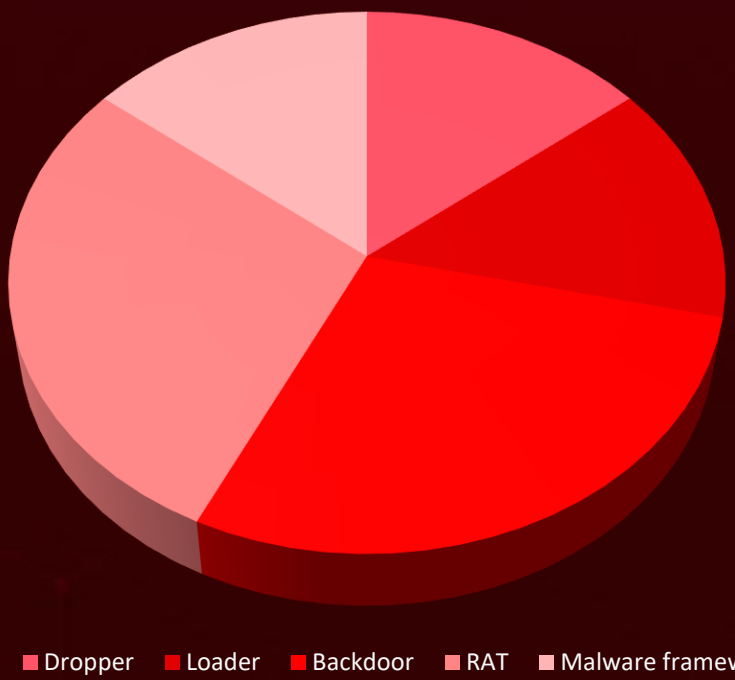
CVE-2025-64155 poses a severe risk to on-prem FortiSIEM deployments, enabling unauthenticated full system compromise amid active exploitation and public PoCs.

UAT-7290 conducts telecom-focused espionage while repurposing compromised infrastructure as covert relay nodes for broader China-aligned operations.

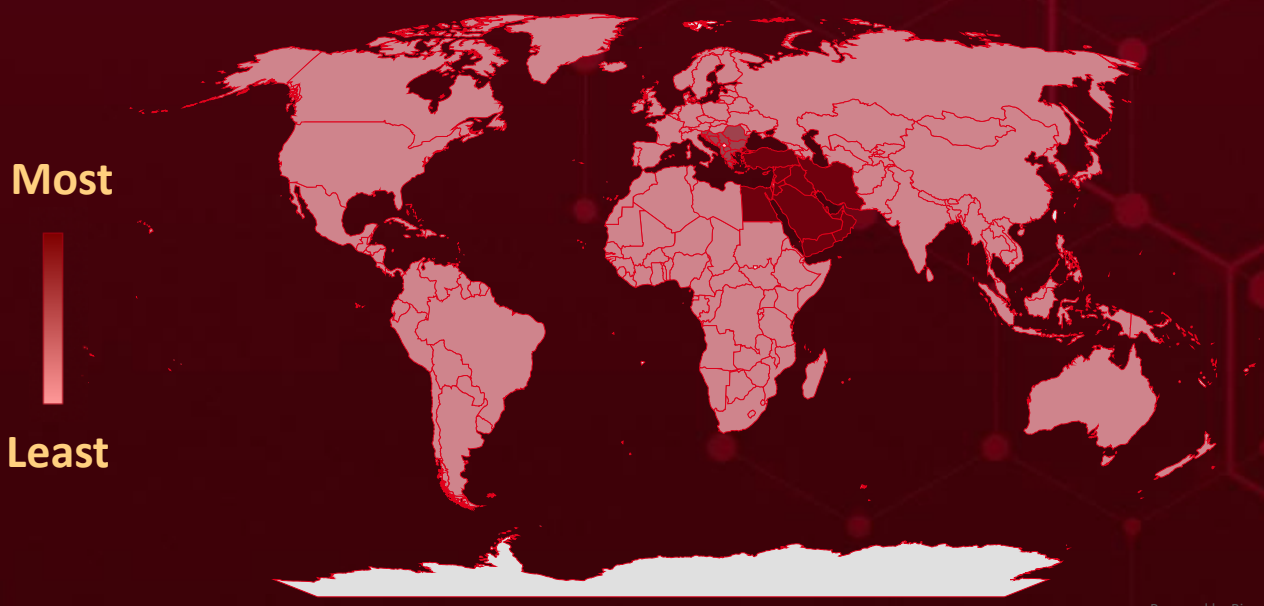
The AsyncRAT campaign demonstrates a shift toward stealthy, trust-abusing intrusions that leverage cloud services, native tools, and subtle deception to achieve persistent compromise.

VoidLink is a China-linked, modular Linux cloud implant enabling stealthy, long-term compromise of cloud environments.

Threat Distribution

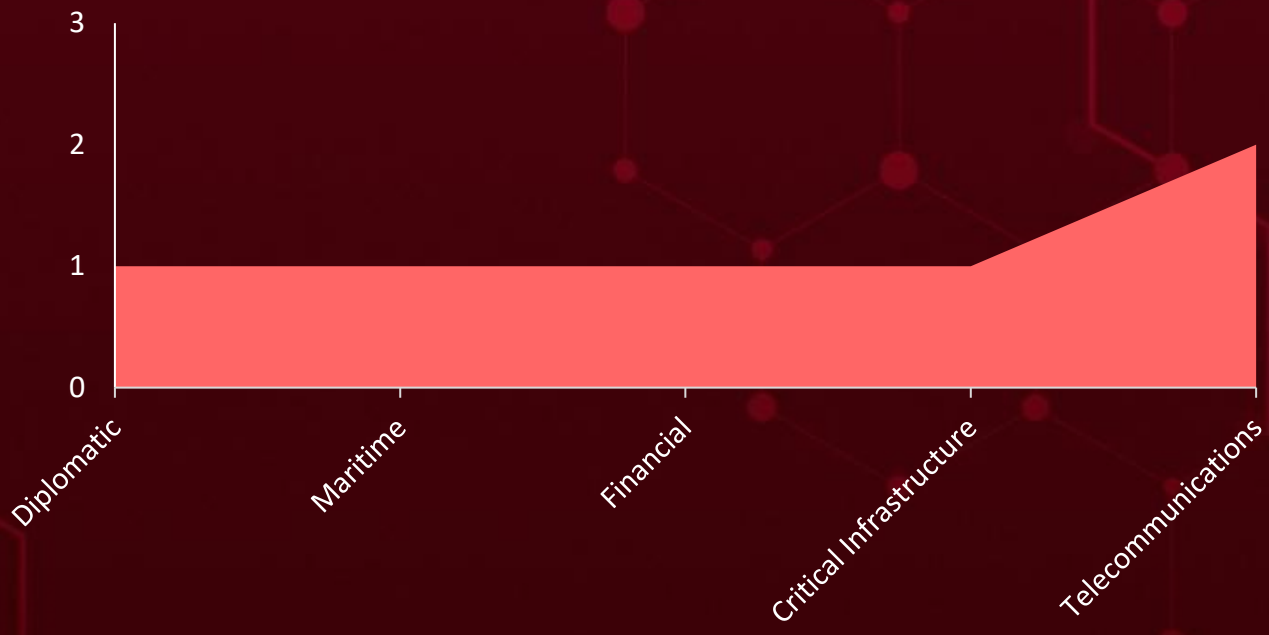


Targeted Countries



Countries	Countries	Countries	Countries
United Arab Emirates	Albania	Marshall Islands	Djibouti
Qatar	Croatia	China	Monaco
Lebanon	Greece	Belize	Dominica
Bahrain	Slovenia	Colombia	Mozambique
Syria	Brunei	New Zealand	Dominican Republic
Cyprus	Namibia	Comoros	Nepal
Kuwait	Belgium	Pakistan	DR Congo
Egypt	Burundi	Congo	Niger
Oman	Papua New Guinea	Poland	Ecuador
Iran	Cabo Verde	Costa Rica	Norway
Saudi Arabia	Togo	Saint Lucia	Andorra
Iraq	Cambodia	Côte d'Ivoire	Palestine
Turkey	Micronesia	Sierra Leone	El Salvador
Israel	Cameroon	Bhutan	Peru
Jordan	North Korea	Tajikistan	Equatorial Guinea
Yemen	Canada	Cuba	Bahamas
Romania	Brazil	Barbados	Eritrea
Montenegro	Central African Republic	Algeria	Rwanda
Serbia	Suriname	Uruguay	El Salvador
Bosnia and Herzegovina	Chad	Czech Republic	Estonia
North Macedonia	Ukraine	Mali	San Marino
Bulgaria	Chile	Denmark	Eswatini
		Mauritius	Benin
		Panama	Ethiopia

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter

T1027 Obfuscated Files or Information

T1588 Obtain Capabilities

T1071 Application Layer Protocol

T1190 Exploit Public-Facing Application

T1497 Virtualization/ Sandbox Evasion

T1059.001 PowerShell

T1555 Credentials from Password Stores

T1204 User Execution

T1552 Unsecured Credentials

T1071.001 Web Protocols

T1566 Phishing

T1078 Valid Accounts

T1083 File and Directory Discovery

T1566.001 Spearphishing Attachment

T1068 Exploitation for Privilege Escalation

T1204.001 Malicious Link

T1027.013 Encrypted/Encoded File

T1041 Exfiltration Over C2 Channel

T1082 System Information Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RustyWater	RustyWater Rust-based RAT deployed by Iran's MuddyWater APT targeting diplomatic, maritime, financial, and telecom entities in the Middle East. Delivered via spear-phishing with malicious Word documents. Features anti-debugging, registry persistence, encrypted strings, and asynchronous C2 communication over HTTP/HTTPS. Represents MuddyWater's evolution from PowerShell/VBS loaders to modern compiled implants.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		System Compromise, Espionage	Windows
RAT			
ASSOCIATED ACTOR			PATCH LINK
MuddyWater			-

IOC TYPE	VALUE
SHA256	03457a4428dfe510acc1f147d54a2000a658d562d0edcff2b5ff0897cf6ea516, a2001892410e9f34ff0d02c8bc9e7c53b0bd10da58461e1e9eab26bdbf410c79

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RushDrop	RushDrop Linux dropper used by China-nexus APT UAT-7290 targeting telecommunications infrastructure in South Asia and Southeastern Europe. Contains three embedded binaries (DriveSwitch, SilentRaid, BusyBox) that it decodes and deploys after anti-VM checks. Also known as ChronosRAT. Initiates the infection chain for deeper network compromise and espionage operations.	-	-
		IMPACT	AFFECTED PLATFORM
TYPE		Initial Access, Malware Deployment	Linux
Dropper			
ASSOCIATED ACTOR			PATCH LINK
UAT-7290			-

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
DriveSwitch	DriveSwitch Peripheral Linux malware component deployed by UAT-7290 as part of the RushDrop infection chain. Its sole purpose is to execute the main SilentRaid implant on compromised systems. Acts as an intermediary executor between the dropper and the primary backdoor. Targets edge devices in telecom infrastructure.	Dropped by RushDrop dropper	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Malware Execution, Persistence	Linux
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
UAT-7290			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SilentRaid	SilentRaid is a C++ Linux backdoor (also called MystRodX) used by UAT-7290 for persistent access to telecom networks. Features plugin-based architecture supporting remote shell, port forwarding, file operations, and credential harvesting. Resolves C2 domains via Google DNS and performs anti-analysis checks. Primary implant for espionage operations against South Asian critical infrastructure.	Dropped and executed via RushDrop/DriveSwitch chain	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise, Persistent Access, Espionage, Data Theft	Linux
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
UAT-7290			

IOC TYPE	VALUE
SHA256	723c1e59accbb781856a8407f1e64f36038e324d3f0bdb606d35c359ade08200, 59568d0e2da98bad46f0e3165bcf8adadbf724d617ccebcfdaeafbb097b81596, 961ac6942c41c959be471bd7eea6e708f3222a8a607b51d59063d5c58c54a38d

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
Bulbature	Bulbature is a Linux implant first disclosed in late 2024, used to convert compromised edge devices into Operational Relay Boxes (ORBs). Deployed by China-nexus actors including UAT-7290 to create proxy infrastructure for offensive operations. Has compromised over 75,000 hosts across 139 countries. Supports reverse shell capabilities and dynamic C2 switching.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Backdoor		System compromise	Linux
ASSOCIATED ACTOR			**PATCH LINK**
UAT-7290			-

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
AsyncRAT	AsyncRAT is an Open-source Windows RAT ranked 6th most prevalent malware globally in 2024. Distributed via phishing using Dropbox URLs, TryCloudflare tunnels, and malicious attachments. Capabilities include keylogging, screenshot capture, credential theft, and ransomware deployment. Its modular architecture has spawned numerous variants like VenomRAT and NonEuclid RAT.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCT**
RAT		System Compromise, Credential Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	eefd05a18e87dcee12fed7381761fb92f2c176f0b7476ecd7bee65c549c4c968, fdad0ac0500d50695b07aa45120713c147e473e1117996ba7b1d023dedb13735, f675f6062ca6a1ecb72499050aee1650a0ba79b95dc5d5a98edaf591ff06c844, 9265c6b4f354dcc7dce97e4b55d297687a39b67142f9288d28db09b7620a1286, c5ae3a569ef9dce592dd090bfa821303fc77a6012882c20a4b741b4552a793dd

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>VoidLink</td><td rowspan="5">VoidLink is an advanced cloud-native Linux malware framework written in Zig, discovered December 2025, developed by Chinese-affiliated actors. Designed for long-term stealth access to AWS, GCP, Azure, Alibaba, Tencent, Kubernetes, and Docker environments. Features 37 plugins for reconnaissance, credential harvesting, lateral movement, and anti-forensics. Targets software engineers for potential supply chain attacks.</td><td>-</td><td>-</td></tr>
<tr><td>TYPE</td><td rowspan="2">IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>Malware framework</td><td rowspan="3">System compromise, Espionage</td><td>Linux</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">05eac3663d47a29da0d32f67e10d161f831138e10958dcd88b9dc97038948f69,
15cb93d38b0a4bd931434a501d8308739326ce482da5158eb657b0af0fa7ba49,
6850788b9c76042e0e29a318f65fceb574083ed3ec39a34bc64a1292f4586b41,
6dcfe9f66d3aef1efd7007c588a59f69e5cd61b7a8eca1fb89a84b8ccef13a2b,
28c4a4df27f7ce8ced69476cc7923cf56625928a7b4530bc7b484eec67fe3943</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-2026-20805	✗	Windows 10 - 11 25H2, Windows Server 2012, 2016, 2019, 2025, 2022	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Desktop Window Manager Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059.006: Python, T1082: System Information Discovery, T1588.007: Artificial Intelligence	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-20805

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21265	✗	Windows 10 - 11 25H2, Windows Server 2012, 2016, 2025, 2022, 2019	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Secure Boot Certificate Expiration Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1329	T1542: Pre-OS Boot, T1553: Subvert Trust Controls	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21265

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-31096	✗	Windows 10 - 11 25H2, Windows Server 2012, 2008, 2016, 2025, 2022, 2019	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Agere Soft Modem Driver Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1068: Exploitation for Privilege Escalation, T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-31096

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-64155	✗	Fortinet FortiSIEM (7.4.0, 7.3.0-7.3.4, 7.2.0-7.2.6, 7.1.0-7.1.8, 7.0.0-7.0.4, 6.7.0-6.7.10)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortisiem:*:*:*:*:*:*:*:*:*	-
Fortinet FortiSIEM OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-25-772

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21858	Ni8mare	n8n version 1.65.0 - 1.120.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:n8n:n8n:*:*:*:*:*:*:*:*:*	-
n8n Unauthenticated Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1552: Unsecured Credentials	https://github.com/n8n-io/n8n/releases

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-23550</td><td>✗</td><td rowspan="2">Modular DS Modular Connector (Before 2.5.2)</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:modulards:modular_connector:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">WordPress Modular DS Privilege Escalation Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-284</td><td>T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1098: Account Manipulation</td><td>https://help.modulards.com/en/article/modular-ds-security-releases-modular-connector-260-and-252-dm3mv0/</td></tr>
</table>

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	Diplomatic, Maritime, Financial, and Telecom Entities	Middle East
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	RustyWater	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1106: Native API; T1047: Windows Management Instrumentation; T1620: Reflective Code Loading; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder; T1027: Obfuscated Files or Information; T1036: Masquerading; T1055: Process Injection; T1082: System Information Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1573: Encrypted Channel; T1140: Deobfuscate/Decode Files or Information; T1083: File and Directory Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UAT-7290	China	Critical Infrastructure, Telecommunications	South Asia, Southeastern Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	RushDrop, DriveSwitch, SilentRaid, Bulbature	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; TA0010: Exfiltration; TA0043: Reconnaissance; TA0042: Resource: Development; T1595: Active Scanning; T1587: Develop Capabilities; T1588: Obtain Capabilities; T1190: Exploit Public-Facing Application; T1110: Brute Force; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1027: Obfuscated Files or Information; T1497: Virtualization/Sandbox Evasion; T1140: Deobfuscate/Decode Files or Information; T1564: Hide Artifacts; T1027.002: Software Packing; T1552: Unsecured Credentials; T1082: System Information Discovery; T1016: System Network Configuration: Discovery; T1083: File and Directory Discovery; T1005: Data from Local System; T1071: Application Layer Protocol; T1132: Data Encoding; T1573: Encrypted Channel; T1090: Proxy; T1572: Protocol Tunneling; T1041: Exfiltration Over C2 Channel; T1595.002: Vulnerability: Scanning; T1587.001: Malware; T1588.005: Exploits; T1110.001: Password Guessing; T1059.004: Unix Shell; T1497.001: System Checks; T1564.001: Hidden Files and Directories; T1552.001: Credentials In Files; T1071.001: Web Protocols; T1573.002: Asymmetric Cryptography; T1090.002: External Proxy; T1588.006: Vulnerabilities		

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **six exploited vulnerabilities** and block the indicators related to the threat actor **MuddyWater, UAT-7290** and malware **RustyWater, RushDrop, DriveSwitch, SilentRaid, Bulbature, AsyncRAT, VoidLink.**

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 **six exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **MuddyWater** and malware **RustyWater, SilentRaid, AsyncRAT, VoidLink** in Breach and Attack Simulation(BAS).

Threat Advisories

MuddyWater’s Rust Implants Target the Middle East

Chinese APT Espionage Turns Telecom Systems Into Covert Relay Nodes

AsyncRAT Behind the Cloudflare Curtain

Microsoft’s January 2026 Patch Tuesday

CVE-2025-64155: Critical FortiSIEM RCE with Public Exploits Available

VoidLink: A Cloud-Native Linux Framework Built for Stealth and Scale

Ni8mare in n8n: CVE-2026-21858 Bug Exposing 100,000 Servers to Risk

Admin Access Without Credentials Puts 40,000+ WordPress Sites at Risk

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
RustyWater	SHA256	03457a4428dfe510acc1f147d54a2000a658d562d0edcff2b5ff0897cf6ea516, a2001892410e9f34ff0d02c8bc9e7c53b0bd10da58461e1e9eab26bdbf410c79
SilentRaid	SHA256	723c1e59accbb781856a8407f1e64f36038e324d3f0bdb606d35c359ade08200, 59568d0e2da98bad46f0e3165bcf8adadbf724d617ccebcfdaeafbb097b81596, 961ac6942c41c959be471bd7eea6e708f3222a8a607b51d59063d5c58c54a38d
AsyncRAT	SHA256	eefd05a18e87dcee12fed7381761fb92f2c176f0b7476ecd7bee65c549c4c968, fdad0ac0500d50695b07aa45120713c147e473e1117996ba7b1d023dedb13735, f675f6062ca6a1ecb72499050aee1650a0ba79b95dc5d5a98edaf591ff06c844, 9265c6b4f354dcc7dce97e4b55d297687a39b67142f9288d28db09b7620a1286, c5ae3a569ef9dce592dd090bfa821303fc77a6012882c20a4b741b4552a793dd, 02aa8cabeea2a0120a31adbf0886f821d10953fc6d4d9cd1959568093c48b04d,

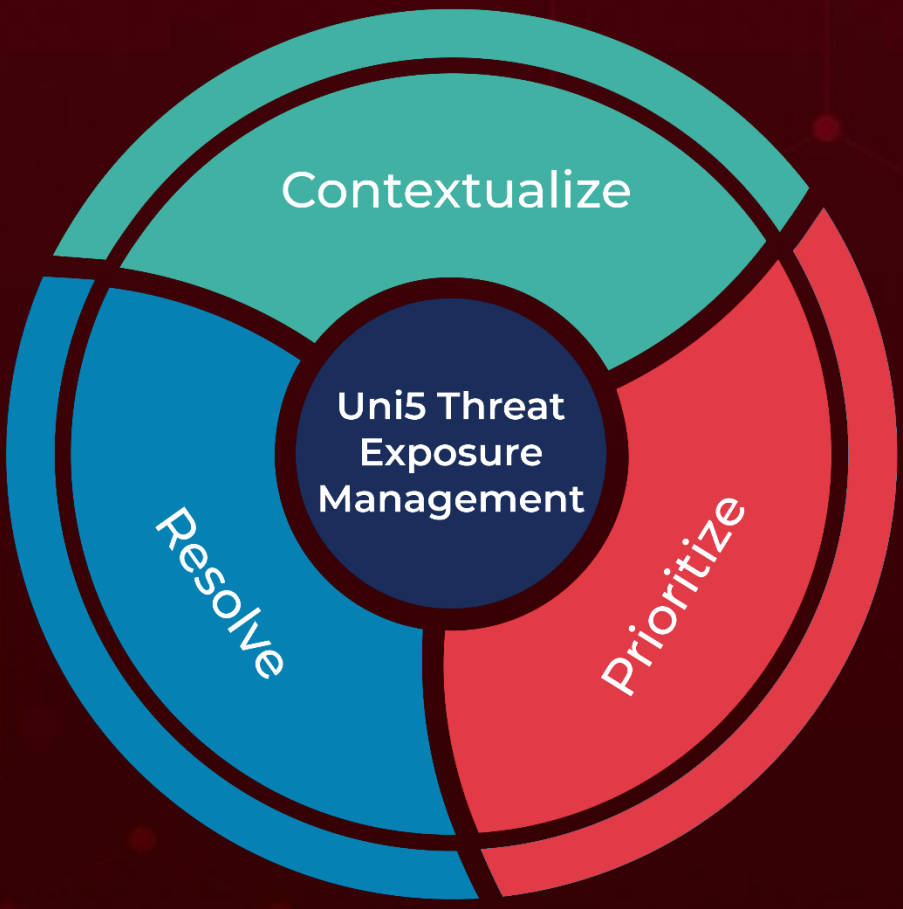
Attack Name	TYPE	VALUE
AsyncRAT	SHA256	279b157c99432100bab17e6f23bd90cb397582324b091010d8cf1ec2683d3e4d, 6da6e608ba1bf369e01785d677c8fc95e551ee847d420a1be885677871a30134
VoidLink	SHA256	05eac3663d47a29da0d32f67e10d161f831138e10958dcd88b9dc97038948f69, 15cb93d38b0a4bd931434a501d8308739326ce482da5158eb657b0af0fa7ba49, 6850788b9c76042e0e29a318f65fceb574083ed3ec39a34bc64a1292f4586b41, 6dcfe9f66d3aef1efd7007c588a59f69e5cd61b7a8eca1fb89a84b8ccef13a2b, 28c4a4df27f7ce8ced69476cc7923cf56625928a7b4530bc7b484eec67fe3943, e990a39e479e0750d2320735444b6c86cc26822d86a40d37d6e163d0fe058896, 4c4201cc1278da615bacf48deef461bf26c343f8cbb2d8596788b41829a39f3f

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

January 19, 2026 . 11:30 PM

More at www.hivepro.com