Date of Publication
March 2, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

23 February to 1 March 2026

Table Of Contents

Summary 03

High Level Statistics 04

Insights 05

Targeted Countries 06

Targeted Industries 07

Top MITRE ATT&CK TTPs 07

Attacks Executed 08

Vulnerabilities Exploited 12

Adversaries in Action 14

Recommendations 17

Threat Advisories 18

Appendix 19

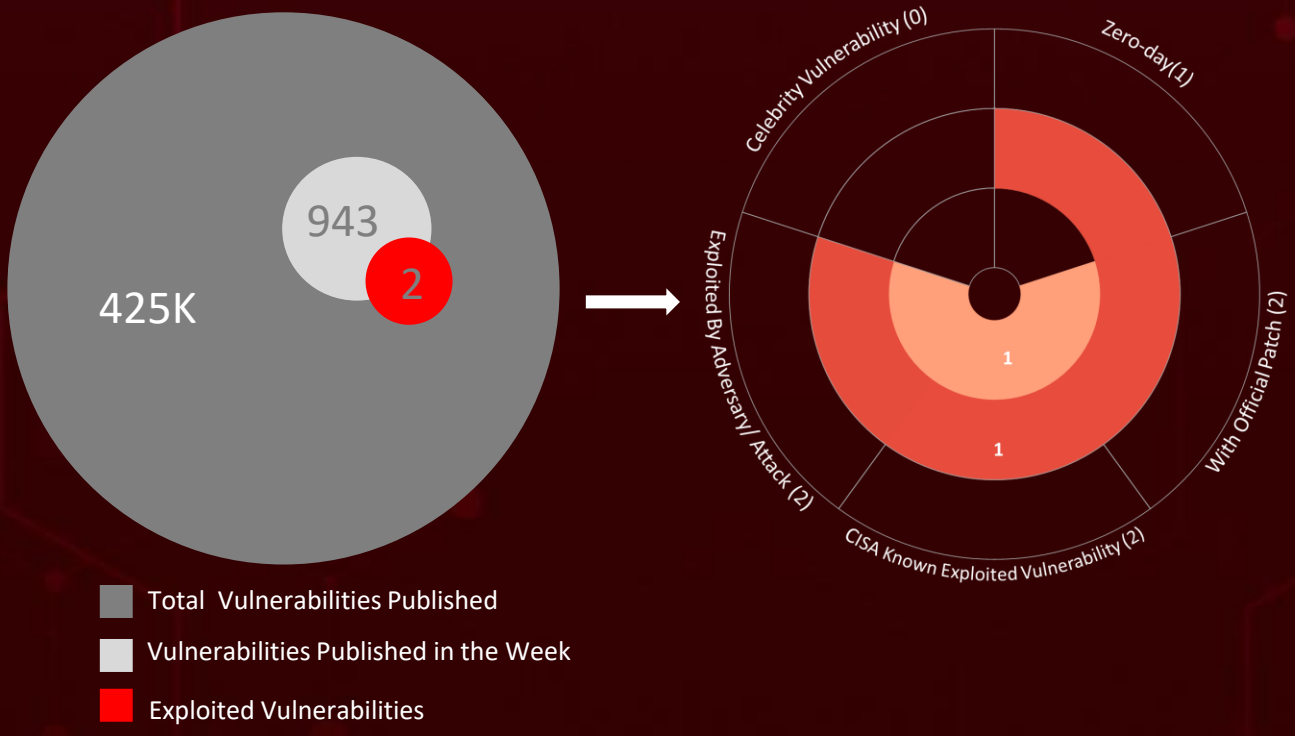
What Next? 20

Summary

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

CVE-2026-20127 is being actively exploited to achieve unauthenticated control-plane takeover of Cisco SD-WAN environments, enabling persistent network compromise and root access when chained with additional flaws. **SANDWORM_MODE** npm worm demonstrated self-propagating supply chain compromise by harvesting developer secrets, hijacking CI/CD pipelines, and poisoning AI-assisted workflows.

Meanwhile, MuddyWater's **Operation Olalampo** leveraged macro-based spear-phishing to deploy multiple malware families across the MENA region, utilizing diversified C2 infrastructure and suspected AI-assisted development to enable sustained espionage and strategic intrusion operations. **Mercenary Akula** (UAC-0050) targeted a European financial institution supporting Ukraine through spoofed judicial-domain spear-phishing, deploying RMS via a multi-layered archive chain to establish persistent, stealthy access for likely intelligence collection or financial theft. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

7
Attacks Executed

2
Vulnerabilities Exploited

3
Adversaries in Action

- MIMICRAT
- Lua loader
- GhostFetch
- HTTP_VIP
- CHAR
- GhostBackDoor
- SANDWORM_MODE

- CVE-2026-20127
- CVE-2022-20775

- MuddyWater
- Mercenary Akula
- UAT-8616

Insights

CLICKFIX Trusted websites weaponized to silently deploy **MIMICRAT** for stealth remote control.

SANDWORM_MODE SUPPLY CHAIN WORM Self-propagating npm malware abuses 19 typosquatted packages to harvest secrets and hijack CI/CD pipelines.

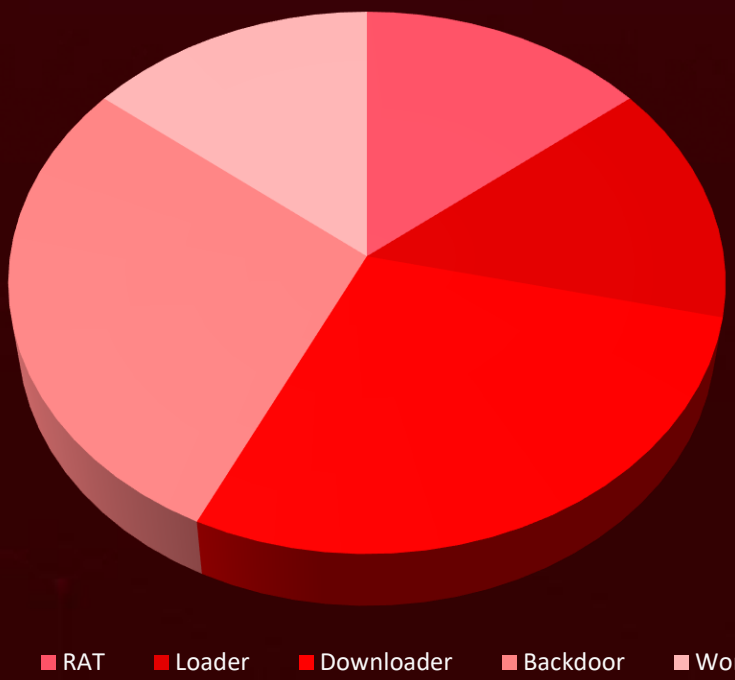
MERCENARY AKULA Russia-aligned actors spoofed a Ukrainian judicial domain to deliver RMS via multi-layered archive phishing.

MuddyWater deploys GhostFetch, GhostBackDoor, HTTP_VIP, and CHAR via weaponized Office documents.

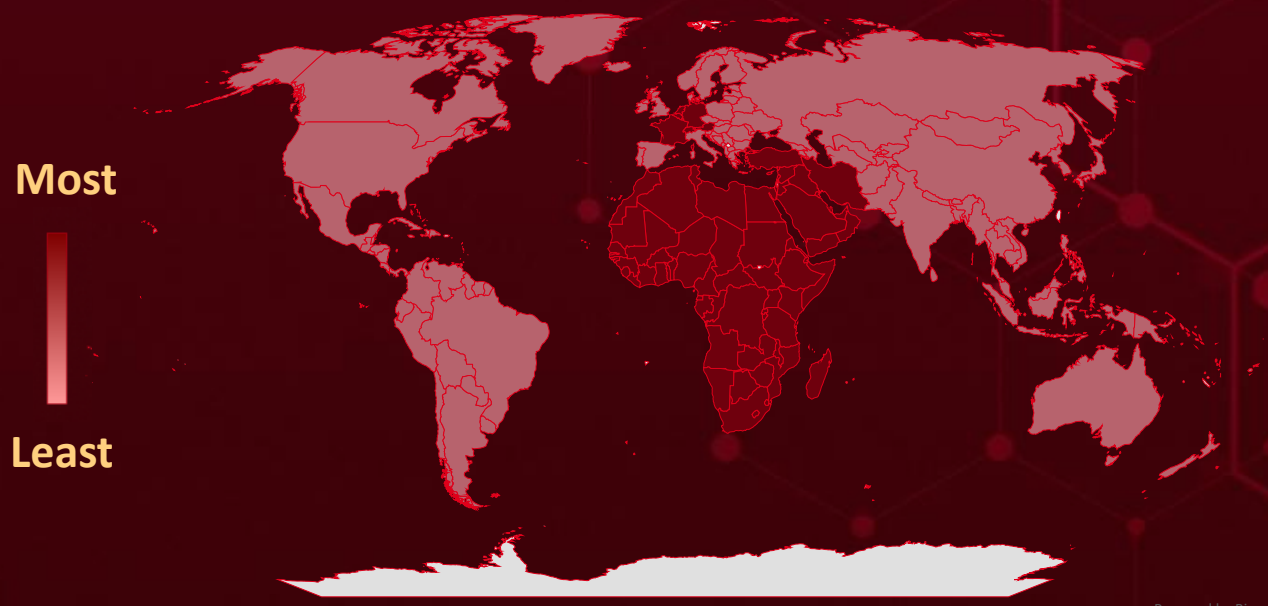
LINUX ECOSYSTEM THREAT SURGE 381+ new vulnerabilities disclosed, including 10 high-risk flaws with active or probable exploitation.

UAT-8616 chains CVE-2026-20127 with CVE-2022-20775 to achieve root-level control.

Threat Distribution



Targeted Countries



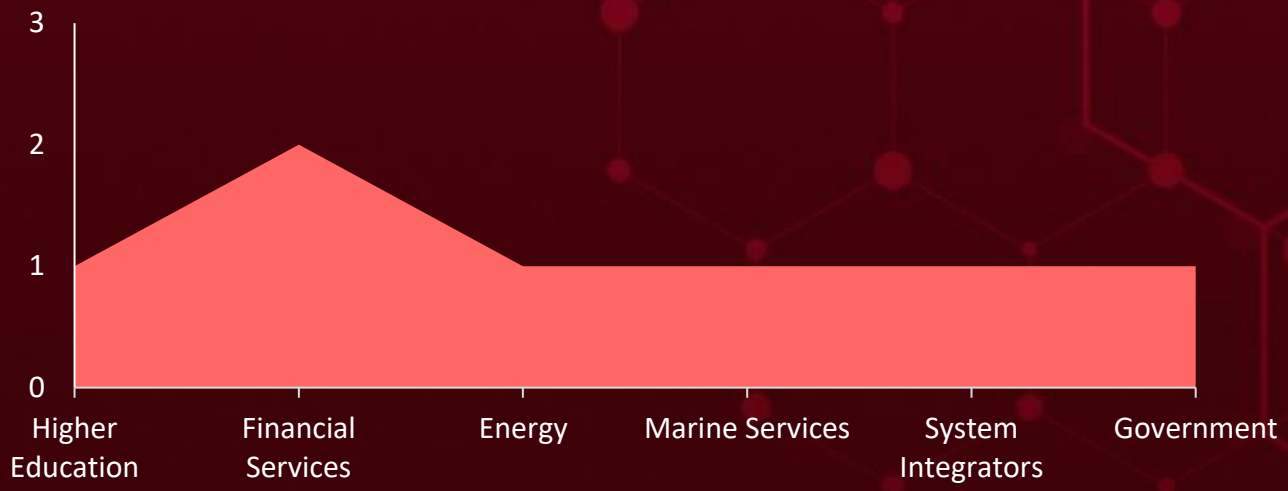
Countries
Sierra Leone
Mauritius
Lesotho
Algeria
Oman
Angola
Togo
Austria
Madagascar
Bahrain
Namibia
Belgium
Sao Tome & Principe
Benin
Sudan
Botswana
United Arab Emirates
Burkina Faso
Liechtenstein
Luxembourg

Countries
Burundi
Mali
Cabo Verde
Morocco
Cameroon
Niger
Central African Republic
Republic of congo
Chad
Senegal
Comoros
South Africa
Congo
Syria
Côte d'Ivoire
Turkey
Cyprus
Zambia
Djibouti
Liberia
DR Congo
Egypt

Countries
Malawi
Equatorial Guinea
Mauritania
Eritrea
Monaco
Eswatini
Mozambique
Ethiopia
Netherlands
France
Nigeria
Gabon
Qatar
Gambia
Rwanda
Germany
Saudi Arabia
Ghana
Seychelles
Guinea
Somalia
Guinea-Bissau
South Sudan
Iran

Countries
Switzerland
Iraq
Tanzania
Israel
Tunisia
Jordan
Uganda
Kenya
Yemen
Kuwait
Zimbabwe
Lebanon
Libya
Portugal
Tajikistan
Singapore
India
Uruguay
Indonesia
Samoa
Canada
Spain
Bahamas
Azerbaijan

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter

T1190 Exploit Public-Facing Application

T1588 Obtain Capabilities

T1204 User Execution

T1566 Phishing

T1082 System Information Discovery

T1068 Exploitation for Privilege Escalation

T1555 Credentials from Password Stores

T1071 Application Layer Protocol

T1195 Supply Chain Compromise

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

T1041 Exfiltration Over C2 Channel

T1021 Remote Services

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
MIMICRAT	MIMICRAT is a custom C++ remote access trojan delivered via ClickFix campaigns that compromise legitimate websites. It features malleable C2 profiles, Windows token impersonation, SOCKS5 tunneling, and a 22-command dispatch table for post-exploitation. It communicates over HTTPS on port 443, disguised to look like legitimate web analytics traffic.	ClickFix	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Remote access, Data exfiltration	Windows
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	a508d0bb583dc6e5f97b6094f8f910b5b6f2b9d5528c04e4dee62c343fce6f4b

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Lua Loader	Lua Loader is a custom in-memory loader used in the MIMICRAT ClickFix campaign that embeds its own Lua interpreter. It decrypts an XOR-encoded shellcode payload and executes it entirely in memory, leaving no disk artifacts. The shellcode matches Meterpreter signatures and is used to reflectively load the MIMICRAT RAT into the victim's system.	-	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Payload delivery, Defense evasion	Windows
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	5e0a30d8d91d5fd46da73f3e6555936233d870ac789ca7dd64c9d3cc74719f51

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
GhostFetch	GhostFetch is a first-stage downloader used by MuddyWater (Operation Olalampo) designed to fetch and execute secondary payloads directly in memory. It profiles compromised systems by validating mouse movement, screen resolution, detecting debuggers, VM artifacts, and AV software before proceeding. It ultimately drops an advanced second-stage implant called GhostBackDoor.	Phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		Payload delivery, Sandbox evasion	Windows
Downloader			
ASSOCIATED ACTOR			PATCH LINK
MuddyWater			-

IOC TYPE	VALUE
Domain	Promoverse[.]org
SHA256	8d2227f2c53d7e22a57e12c45cecdd43dbec08dbc3ab93e74e6df52cdf80548b

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
HTTP_VIP	HTTP_VIP is a native downloader attributed to MuddyWater that performs system reconnaissance and connects to an external C2 server for authentication. It deploys AnyDesk from the C2 server, and newer variants can retrieve victim information, start an interactive shell, download/upload files, capture clipboard contents, and update beaconing intervals.	Phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		Reconnaissance, Remote access, Data exfiltration	Windows
Downloader			
ASSOCIATED ACTOR			PATCH LINK
MuddyWater			-

IOC TYPE	VALUE
Domains	codefusiontech[.]org, miniquest[.]org
SHA256	f717d0abf3f7e8b08b8461c711caaa808b8888e8631cd3386f4f588b5fefbfb3

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
CHARA	CHARA is a Rust-based backdoor used by MuddyWater, controlled via a Telegram bot (named "Olalampo") to execute cmd.exe or PowerShell commands and change directories. Group-IB's analysis revealed signs of AI-assisted development, including emojis in debug strings. It shares structural similarities with the previously known BlackBeard/Archer RAT malware.	Phishing	-
		IMPACT	AFFECTED PRODUCT
TYPE		Payload delivery, Sandbox evasion	Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
MuddyWater			-

IOC TYPE	VALUE
SHA256	3a19c19d9f3bac6628a968110477ee01e5867b2534e914e1be5c4485947bd819

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
GhostBackDoor	GhostBackDoor is a second-stage implant delivered by GhostFetch in MuddyWater's Operation Olalampo campaign. It supports an interactive shell, file read/write operations, and the ability to re-run GhostFetch. It adapts its installation method based on the target's privilege level, installing as a service with admin access or using the startup registry folder for standard users.	Dropped by GhostFetch	-
		IMPACT	AFFECTED PRODUCT
TYPE		System compromise, Data exfiltration	Windows
Backdoor			
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.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td rowspan="2">SANDWORM_MODE</td><td rowspan="5">SANDWORM_MODEA is a self-propagating npm supply chain worm spread through 19 typosquatted packages that steals credentials, infects projects, and propagates across developer environments. It uniquely poisons AI development toolchains by injecting a rogue MCP server into AI coding assistants like Claude Code and Cursor, manipulating them into silently exfiltrating credentials. It also contains a dormant destructive dead switch capable of wiping the home directory.</td><td>Typosquatted npm packages</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Credential theft, Supply chain compromise, AI toolchain poisoning</td><td rowspan="2">macOS, Linux, Windows</td></tr>
<tr><td>Worm</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">5ce544f624fd2aee173f4199da62818ff78deca4ba70d9cf33460974d460395c, 5440e1a424631192dff1162eebc8af5dc2389e3d3b23bd26e9c012279ae116e4</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-2026-20127	✗	Cisco Catalyst SD-WAN Controller & SD-WAN Manager (Before 20.9.8.2, 20.12.6.1, 20.12.5.3, 20.15.4.2, 20.18.2.1)	UAT-8616
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:catalyst_sd-wan_controller:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Controller and Manager Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-20775		Cisco SD-WAN Software (Before 20.6.3 to 20.6.4)	UAT-8616
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:sd-wan:*:*:*:*:*:*:*:*	-
Cisco SD-WAN Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-25 CWE-22	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
MuddyWater (aka Earth Vetala, Mango Sandstorm, MUDDYCOAST, Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Boggy Serpens, Yellow Nix)	Iran	Energy, Marine Services, System Integrators, Government	Middle East and North Africa (MENA), META (Middle East, Turkey, Africa)
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	-	GhostFetch, HTTP_VIP, CHAR, GhostBackDoor	Windows

TTPs
T1587: Develop Capabilities, T1587.001: Malware, T1566: Phishing , T1566.001: Spear-phishing Attachment, T1190: Exploit Public-Facing Application, T1204: User Execution , T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1106: Native API, T1547: Boot or Logon Autostart , T1140: Deobfuscate/Decode Files or Information, T1620: Reflective Code Loading, T1027: Obfuscated Files or Information , T1027.013: Encrypted/Encoded File, T1497: Virtualization/Sandbox Evasion , T1497.001: System Checks, T1036: Masquerading, T1082: System Information Discovery, T1033: System Owner/User Discovery, T1555: Credentials from Password Stores, T1115: Clipboard Data, T1005: Data from Local System, T1071: Application Layer Protocol , T1071.001: Web Protocols, T1102: Web Service, T1219: Remote Access Software, T1573: Encrypted Channel, T1029: Scheduled Transfer, T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Mercenary Akula (aka UAC-0050, DaVinci Group, Fire Cells Group)	Russia	Financial Services	Western Europe
	MOTIVE		
	Information theft, Espionage and Financial gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	-	-

TTPs
T1589: Gather Victim Identity Information, T1589.003: Employee Names , T1566: Phishing , T1566.002: Spearphishing Link, T1204: User Execution , T1204.002: Malicious File , T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys /Startup Folder, T1036: Masquerading , T1036.007: Double File Extension, T1027: Obfuscated Files or Information, T1027.013: Encrypted/Encoded File, T1218: System Binary Proxy Execution , T1218.011: Rundll32, T1562: Impair Defenses , T1562.004: Disable or Modify System Firewall, T1672: Email Spoofing, T1219: Remote Access Software, T1071: Application Layer Protocol , T1071.001: Web Protocols, T1102: Web Service, T1005: Data from Local System, T1560: Archive Collected Data , T1560.001: Archive via Utility, T1657: Financial Theft

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 UAT-8616	-	All	All
	MOTIVE		
	Information theft and Espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2026-20127 CVE-2022-20775	-	Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Manager
TTPs			
T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts, T1098: Account Manipulation , T1098.004: SSH Authorized Keys, T1136: Create Account, T1070: Indicator Removal , T1070.003: Clear Command History, T1601: Modify System Image , T1601.001: Patch System Image, T1036: Masquerading, T1021: Remote Services , T1021.004: SSH, T1529: System Shutdown/Reboot , T1588: Obtain Capabilities , T1588.006: Vulnerabilities			

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 actor **MuddyWater, Mercenary Akula, UAT-8616** and malware **MIMICRAT, Lua loader, GhostFetch, HTTP_VIP, CHAR, GhostBackDoor, SANDWORM_MODE.**

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 **two exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **MuddyWater** and malware **MIMICRAT, GhostFetch, HTTP_VIP, CHAR,** in Breach and Attack Simulation(BAS).

Threat Advisories

MIMICRAT Remote Control Delivered Through Trusted Platforms

February 2026 Linux Patch Roundup

Operation Olalampo: MuddyWater's Expanding Campaign Across MENA

Mercenary Akula's Court-Themed Campaign Hits European Finance

SANDWORM_MODE: npm Supply Chain Attack Targeting AI Development Tools

CVE-2026-20127: UAT-8616 Exploiting Cisco Catalyst SD-WAN Zero-Day

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)

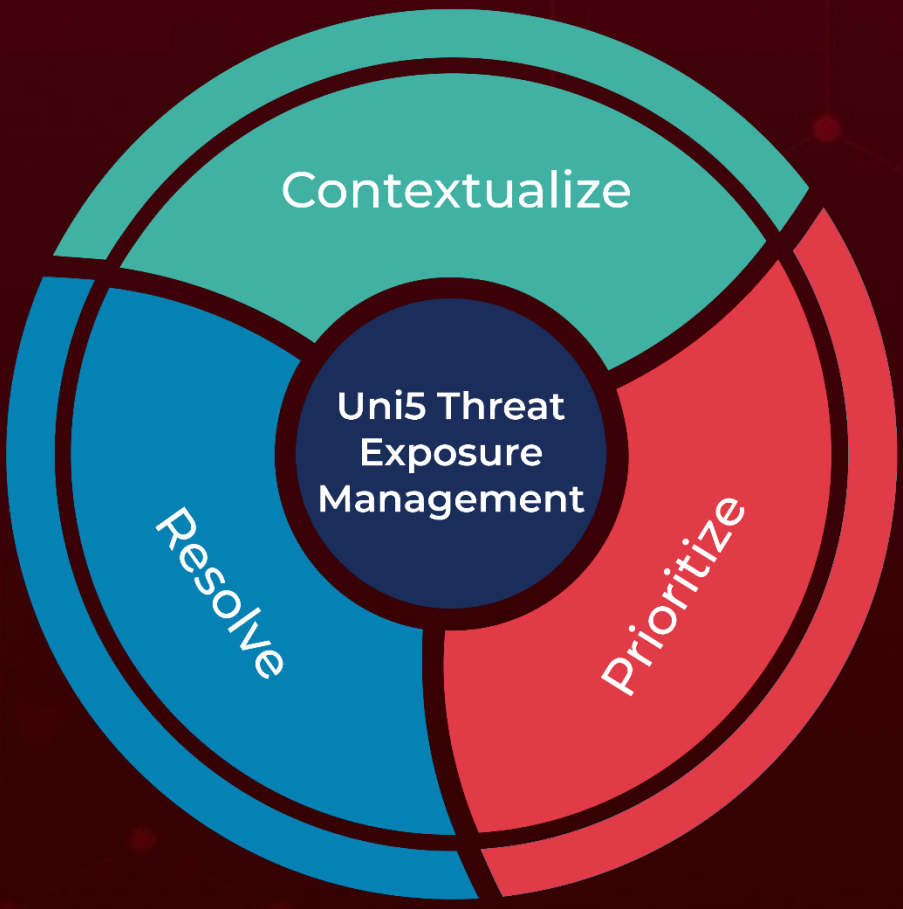
Attack Name	TYPE	VALUE
MIMICRAT	SHA256	a508d0bb583dc6e5f97b6094f8f910b5b6f2b9d5528c04e4dee62c343fce6f4b
Lua loader	SHA256	5e0a30d8d91d5fd46da73f3e6555936233d870ac789ca7dd64c9d3cc74719f51
GhostFetch	Domain	Promoverse[.]org
	SHA256	8d2227f2c53d7e22a57e12c45cecdd43dbec08dbc3ab93e74e6df52cdf80548b
HTTP_VIP	Domains	codefusiontech[.]org, miniquest[.]org
	SHA256	f717d0abf3f7e8b08b8461c711caaa808b8888e8631cd3386f4f588b5fefbfb3
CHAR	SHA256	3a19c19d9f3bac6628a968110477ee01e5867b2534e914e1be5c4485947bd819
SANDWORM_MODE	SHA256	5ce544f624fd2aee173f4199da62818ff78deca4ba70d9cf33460974d460395c, 5440e1a424631192dff1162eebc8af5dc2389e3d3b23bd26e9c012279ae116e4

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

March 2, 2026 . 11:30 PM

More at www.hivepro.com