Date of Publication
March 10, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

02 to 08 MARCH 2026

Table Of Contents

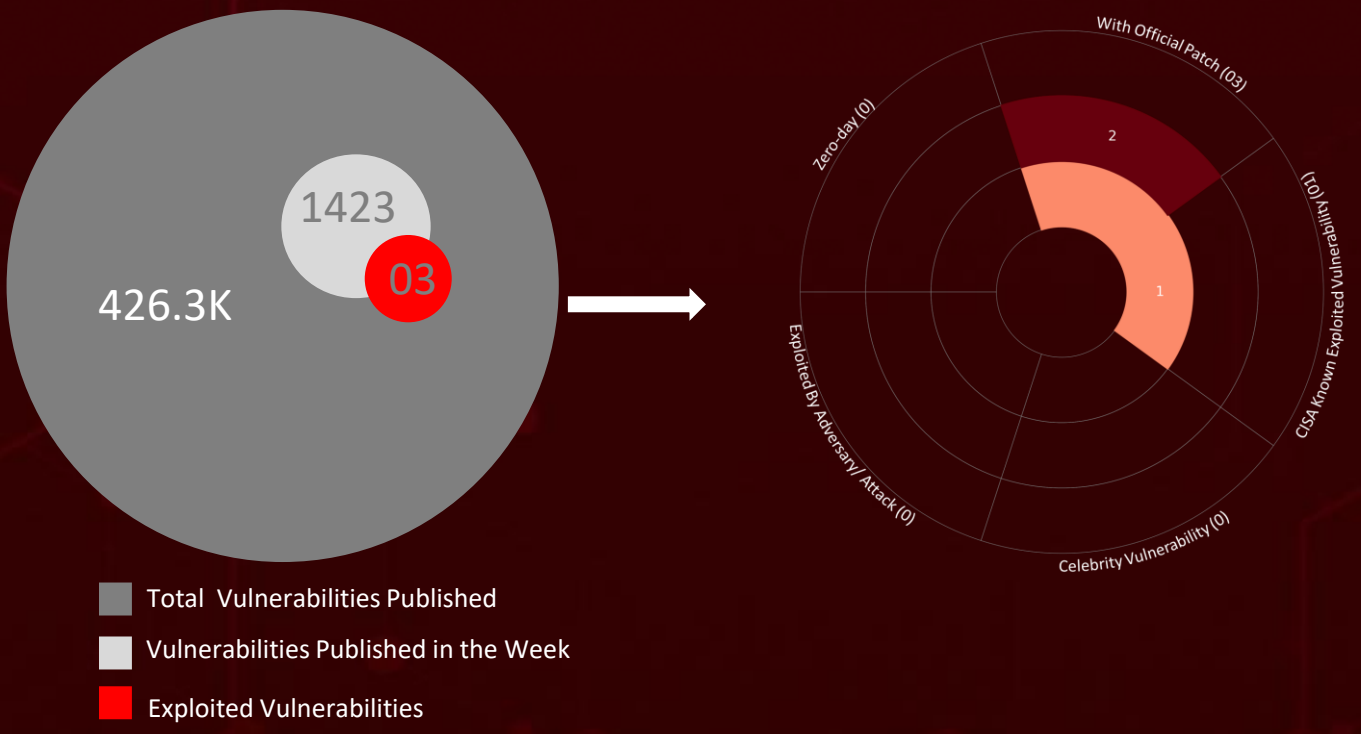
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **twelve** major attacks were detected, **three** critical vulnerabilities were publicly disclosed, and **two** active threat actor groups were monitored, signaling a concerning escalation in malicious activity.

Among the most pressing developments, VMware has issued urgent security updates to address multiple vulnerabilities in VMware Aria Operations, including the actively exploited flaw **CVE-2026-22719**. The vulnerability stems from inadequate input validation within a migration workflow component and could allow unauthenticated attackers to execute arbitrary operating system commands during support-assisted migrations.

Cisco has also warned of critical vulnerabilities impacting Cisco Catalyst SD-WAN Manager, confirming that two flaws, **CVE-2026-20122** and **CVE-2026-20128**, are already being actively exploited in the wild. At the same time, emerging threat campaigns continue to demonstrate increasing operational sophistication. The ***Ruby Jumper campaign*** highlights the calculated tactics of **APT37**, where a seemingly benign Windows shortcut (LNK) file initiates a multi-stage infection chain that ultimately deploys the RESTLEAF malware and leverages Zoho WorkDrive as a covert command-and-control channel.

Adding to the threat landscape is **ClipXDaemon**, an autonomous Linux clipboard hijacker designed to target cryptocurrency users operating within X11 desktop environments. Delivered through a bincrypter-based encrypted loader, the malware persistently monitors clipboard activity and silently replaces copied cryptocurrency wallet addresses with attacker-controlled ones. Together, these incidents emphasize the growing diversity of modern cyber threats and reinforce the need for timely patching, continuous monitoring, and strong defensive practices to stay ahead of increasingly adaptive attackers.



High Level Statistics

12
Attacks Executed

3
Vulnerabilities Exploited

2
Adversaries in Action

- Dohdoor
- RESTLEAF
- SNAKEDROPPER
- THUMBSBD
- VIRUSTASK
- FOOTWINE
- BLUELIGHT
- SPLITDROP
- TWINTASK
- TWINTALK
- GHOSTFORM
- ClipXDaemon

- CVE-2026-22719
- CVE-2026-20122
- CVE-2026-20128

- APT37
- Dust Specter

Insights

Cisco Catalyst SD-WAN Manager, **CVE-2026-20122** and **CVE-2026-20128**, are already being actively exploited, exposing organizations to real-world attacks.

CVE-2026-22719 flaw in VMware Aria Operations allows unauthenticated attackers to execute OS commands and potentially take full control of affected systems.

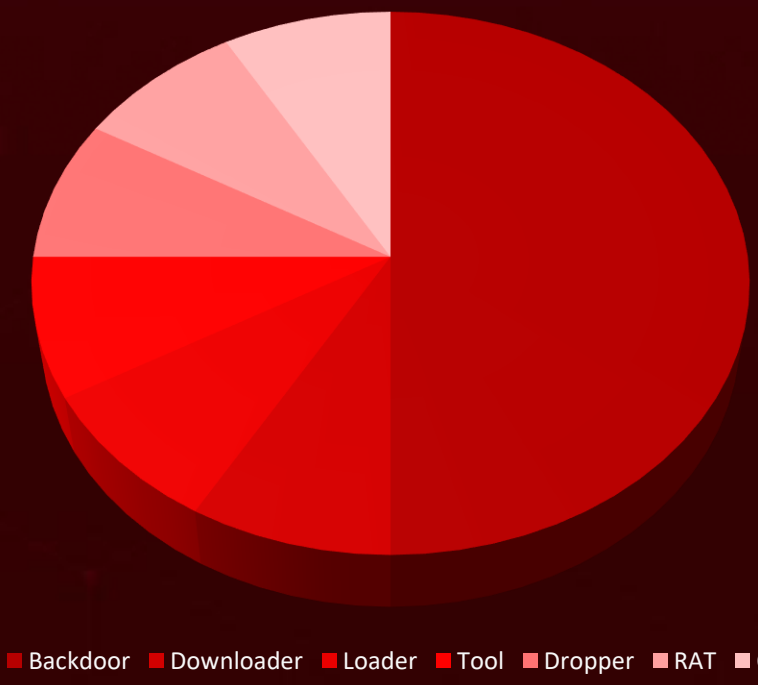
ClipXDaemon is a Linux clipboard hijacker that silently swaps copied cryptocurrency wallet addresses with attacker-controlled ones, targeting users in X11 environments through an encrypted loader.

Iran-linked **Dust Specter** impersonates Iraq's Ministry of Foreign Affairs to target government officials, deploying newly discovered .NET malware through password-protected archives and ClickFix-style lures.

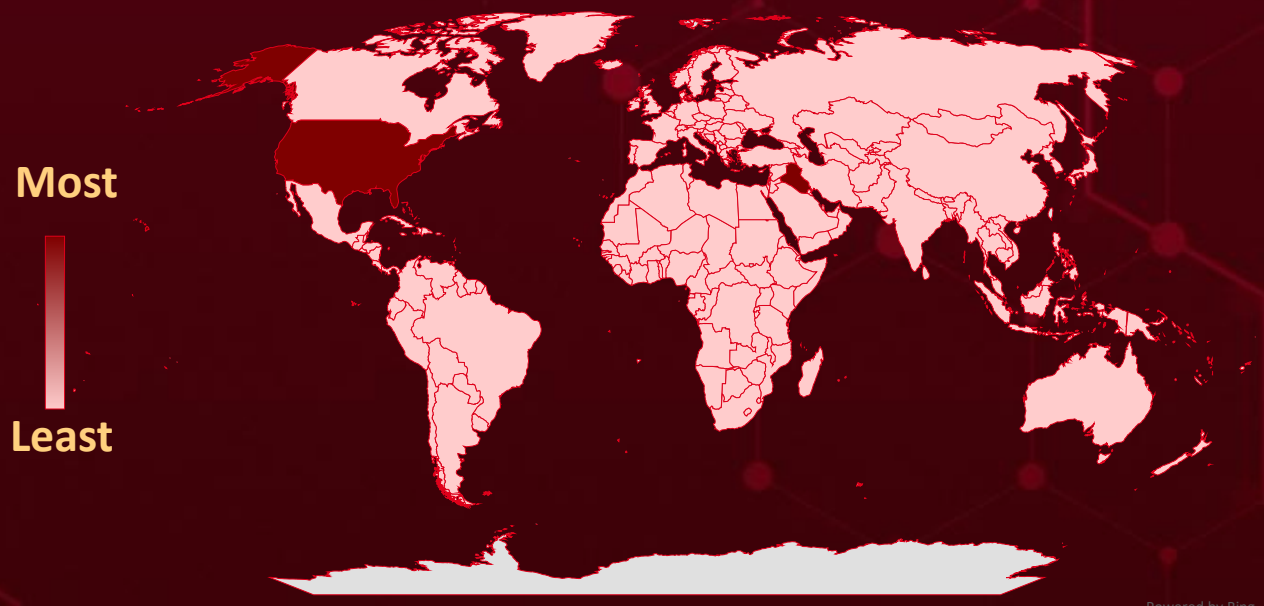
APT37's **Ruby Jumper campaign** turns a harmless-looking LNK file into a stealthy, multi-stage espionage chain, using cloud services like Zoho WorkDrive to quietly manage command-and-control.

The **Dohdoor campaign** uses phishing to trigger a stealthy multi-stage attack that abuses PowerShell, DLL sideloading, and trusted Windows binaries for covert persistence.

Threat Distribution

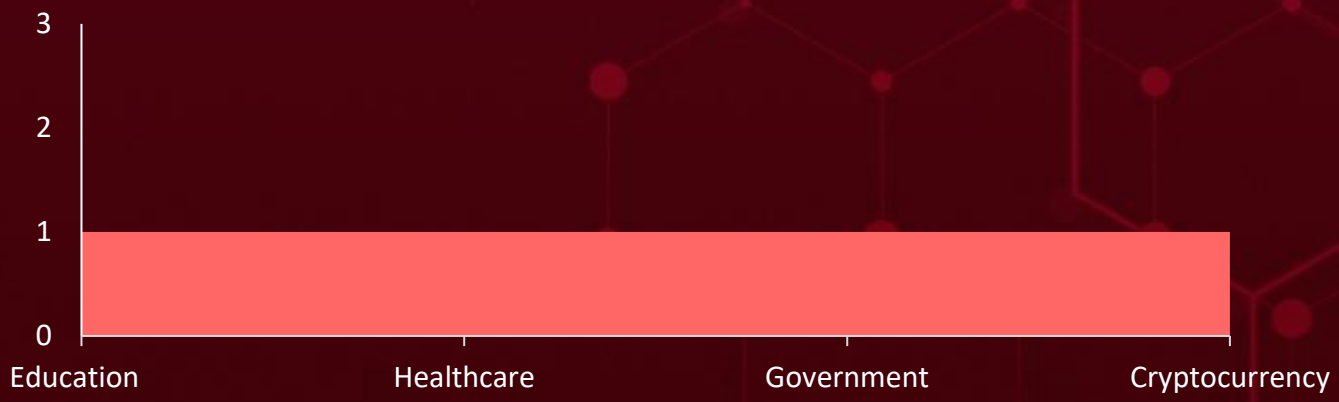


Targeted Countries



Countries	Countries	Countries	Countries
United States	Bahrain	Malawi	Slovenia
Iraq	Mauritania	Bulgaria	Costa Rica
North Macedonia	Bangladesh	Malta	Albania
Zambia	Morocco	Burkina Faso	Côte d'Ivoire
Somalia	Barbados	Mexico	Suriname
Algeria	Nicaragua	Burundi	Croatia
Moldova	Belarus	Mongolia	Tajikistan
Andorra	Palau	Cabo Verde	Cuba
Rwanda	Belgium	Myanmar	Togo
Angola	Portugal	Cambodia	Cyprus
Trinidad and Tobago	Belize	Netherlands	Turkey
Antigua and Barbuda	Samoa	Cameroon	Czechia
Maldives	Benin	Nigeria	Ukraine
Argentina	Singapore	Canada	Democratic Republic of the Congo
Nauru	Bhutan	Oman	Uruguay
Armenia	Sri Lanka	Central African Republic	Denmark
Paraguay	Bolivia	Panama	Vietnam
Australia	Thailand	Chad	Djibouti
Senegal	Bosnia and Herzegovina	Philippines	Libya
Austria	Tuvalu	Chile	Dominica
Switzerland	Botswana	Romania	Lithuania
Azerbaijan	Vanuatu	China	Dominican Republic
United Kingdom	Brazil	Saint Lucia	Madagascar
Bahamas	Afghanistan	Colombia	Ecuador
Luxembourg	Brunei	Sao Tome and Principe	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1036** Masquerading	**T1204** User Execution	**T1027** Obfuscated Files or Information	**T1055** Process Injection
T1140 Deobfuscate/ Decode Files or Information	**T1566** Phishing	**T1059.001** PowerShell	**T1574** Hijack Execution Flow	**T1082** System Information Discovery
T1053 Scheduled Task/Job	**T1071** Application Layer Protocol	**T1565** Data Manipulation	**T1588** Obtain Capabilities	**T1071.001** Web Protocols
T1106 Native API	**T1547** Boot or Logon Autostart Execution	**T1588.006** Vulnerabilities	**T1068** Exploitation for Privilege Escalation	**T1132** Data Encoding

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Dohdoor	Dohdoor uses a method called DNS-over-HTTPS (DoH) to communicate with its control server. It can also download and run additional malicious files in memory without writing them to the disk. Once it infects a system, it creates a hidden backdoor, allowing the attacker to load and run further malicious payloads, like Cobalt Strike Beacon, directly in the system's memory through legitimate Windows processes.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Evades detection, Deploys other malware	Windows
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
SHA256	54e18978c6405f56cd59ba55a62291436639f21cf325ae509f0599b15e8f7f53		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RESTLEAF	RESTLEAF is an initial malware that uses Zoho WorkDrive to communicate with its control server and fetch more malicious files. It gets a valid access token by using embedded credentials, allowing it to perform further actions on Zoho WorkDrive.	Phishing	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Bypasses traditional communication channels, Fetches additional malware	Windows
Downloader			**PATCH LINK**
ASSOCIATED ACTOR			-
APT37			
IOC TYPE	**VALUE**		
MD5	ad556f4eb48e7dba6da14444dcce3170		
SHA256	cf2e3f46b26bae3d11ab6c2957009bc1295b81463dd67989075592e81149c8ec		

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
SNAKEDROPPER	SNAKEDROPPER is a loader that installs the Ruby runtime, ensures the malware stays active on the system, and drops additional malicious files like THUMBSBD and VIRUSTASK. It prepares for execution by replacing a key file, `operating_system.rb`, with a modified version that automatically loads when Ruby starts.	RESTLEAF malware	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Persistence, Drops additional malware	Windows
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
APT37			
IOC TYPE	**VALUE**		
MD5	098d697f29b94c11b52c51bfe8f9c47d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
THUMBSBD	THUMBSBD is disguised as a Ruby file called `ascii.rb`. It uses removable media to connect separate network segments, allowing two-way communication and data theft across isolated networks.	SNAKEDROPPER	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Data Exfiltration	Windows
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
APT37			
IOC TYPE	**VALUE**		
Domains	philion[.]store, homeatedke[.]store,high		

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
VIRUSTASK	VIRUSTASK is a tool that spreads through removable media by replacing files with malicious LNK shortcuts. It runs a multi-stage infection process that takes control of files.	SNAKEDROPPER	-
		IMPACT	AFFECTED PLATFORM
TYPE		Persistence	Windows
Tool			PATCH LINK
ASSOCIATED ACTOR			-
APT37			
IOC TYPE	VALUE		
MD5	5c6ff601ccc75e76c2fc99808d8cc9a9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
FOOTWINE	FOOTWINE is a backdoor delivered later in the attack. It's an encrypted payload with a shellcode launcher that includes surveillance features like keylogging and audio/video capturing.	VIRUSTASK	-
		IMPACT	AFFECTED PLATFORM
TYPE		Surveillance, Remote Access	Windows
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
APT37			
IOC TYPE	VALUE		
MD5	476bce9b9a387c5f39461d781e7e22b9		
SHA256	c61c679eec1c1b43bbd01727fdfb6a69b11485931eb8569e6b20ada30bfe84af		

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
BLUELIGHT	BLUELIGHT is a backdoor that uses cloud services like Google Drive, OneDrive, pCloud, and BackBlaze for communication. Its functions include executing commands, browsing files, downloading additional malware, uploading files, and removing itself.	VIRUSTASK	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data theft, Downloads additional malware	Windows
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
APT37			
IOC TYPE	VALUE		
MD5	585322a931a49f4e1d78fb0b3f3c6212		
SHA256	a8b8a92d170029885d4e7763675f10eb172150f8503592677cadedc392edccf4		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SPLITDROP	SPLITDROP is a .NET-based dropper that uses a user-provided password to decrypt embedded malware and carry out its attack.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Facilitates attack, Bypasses detection	Windows
Dropper			PATCH LINK
ASSOCIATED ACTOR			-
Dust Specter			
IOC TYPE	VALUE		
SHA256	6bb0d45799076b3f2d7f602b978a0779868fc72a1188374f6919fbbfba23efce		

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
TWINTASK	TWINTASK is a worker module that repeatedly checks a file for new commands every 15 seconds and runs them using PowerShell. It operates in an endless loop.	SPLITDROP	-
		IMPACT	AFFECTED PLATFORM
TYPE		Remote Control	Windows
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
Dust Specter			
IOC TYPE	VALUE		
SHA256	ad26cd72a83b884a8bc5aaa87309683953e151ebb3fde42eda7bf9a4406e530d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
TWINTALK	TWINTALK is a 32-bit .NET DLL that acts as a C2 orchestrator. It checks the C2 server for new commands, coordinates with the worker module, and sends back the results. It works alongside the worker module to execute commands using a file-based polling system.	SPLITDROP	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Exfiltration, Remote Control	Windows
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
Dust Specter			
IOC TYPE	VALUE		
SHA256	f3f2dc31f70a105db161a5e7b463b2215d3cbd64ac0146fd68e39da1c279f7ef		

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
GHOSTFORM	GHOSTFORM is a .NET-based RAT that combines all the functions of the initial attack into one file and runs PowerShell scripts in memory. It uses evasion techniques like invisible Windows forms and timers to delay its execution.	Phishing	-
		IMPACT	AFFECTED PLATFORM
TYPE		Defensive Evasion, Remote Control	Windows
RAT			PATCH LINK
ASSOCIATED ACTOR			-
Dust Specter			
IOC TYPE	VALUE		
SHA256	69294ad90aeb7f05e501e7191c95beb14e23da5587dd75557c867e2944a57fdc, fa51aff99d86a9f1f65aa0ebbf6ca40411d343cea59370851ab328b97e2164bb, 797325b3c8a9356dcace75d93cb5cfb7847d2049c66772d4cc2cee821618cb96		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ClipXDaemon	ClipXDaemon is an automated cryptocurrency clipboard hijacker. It uses the publicly available bincrypter framework to encrypt and hide shell payloads.	-	-
		IMPACT	AFFECTED PLATFORM
TYPE		Data Theft	Linux (X11 Desktop Environments)
Clipper			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	b6bb28160532400eafad532842e4ba9add6d6bbba4f7e7c85e3dbb650369eb00		

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-2026-22719	✗	Broadcom VMware Cloud Foundation, Broadcom VMware vSphere Foundation Version Before 9.0.2.0 Broadcom VMware Aria Operations (Before 8.18.6 / Before 9.0.2.0), VMware Telco Cloud Platform, VMware Telco Cloud Infrastructure	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:vmware:aria_operations:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_infrastructure:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:*	-
Broadcom VMware Aria Operations Command Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-20122	✗	Cisco Catalyst SD-WAN Manager (Before 20.9.8.2 / 20.12.6.1 / 20.15.4.2 / 20.18.2.1)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Manager Arbitrary File Overwrite Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-648	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-20128	✗	Cisco Catalyst SD-WAN Manager (Before 20.18)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-257	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
APT37 (aka ScarCruft, Reaper, TEMP.Reaper, Ricochet Chollima, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet, TA-RedAnt)	North Korea **MOTIVE** Information theft and espionage	All	Worldwide
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	RESTLEAF, SNAKEDROPPER, THUMBSBD, VIRUSTASK, FOOTWINE, and BLUELIGHT	-

TTPs

TA001: Initial Access; TA002: Execution; TA003: Persistence; TA005: Defense Evasion; TA007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; TA009: Collection: T1566: Phishing; T1204: User Execution; T1204.001: Malicious Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1055: Process Injection; T1620: Reflective Code Loading; T1036: Masquerading; T1036.005: Match Legitimate T1036.005: Match Legitimate Name or Location; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1132: Data Encoding; T1132.002: Non-Standard Encoding; T1092: Communication Through Removable Media; T1052: Exfiltration Over Physical Medium; T1052.001: Exfiltration over USB; T1567: Exfiltration Over Web Service; T1567.002: Exfiltration to Cloud Storage; T1056: Input Capture; T1056.001: Keylogging; T1113: Screen Capture; T1123: Audio Capture; T1125: Video Capture

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Dust Specter	Iran	Government	Iraq
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	SPLITDROP, TWINTASK, TWINTALK, GHOSTFORM	-

TTPs
TA0042: Resource Development; TA001: Initial Access; TA002: Execution; TA003: Persistence; TA005: Defense Evasion; TA007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1583: Acquire Infrastructure; T1583.001: Domains; T1587: Develop Capabilities; T1587.001: Malware; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.004: Malicious Copy and Paste; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1574: Hijack Execution Flow; T1574.001: DLL Side-Loading; T1112: Modify Registry; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1140: Deobfuscate/Decode Files or Information; T1205: Traffic Signaling; T1036: Masquerading; T1036.001: Invalid Code Signature; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1001: Data Obfuscation; T1001.003: Protocol or Service Impersonation; T1132: Data Encoding; T1132.001: Standard Encoding; T1041: Exfiltration Over C2 Channel

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerabilities** and block the indicators related to the threat actors **APT37, Dust Specter,** and malware **Dohdoor, RESTLEAF, SNAKEDROPPER, THUMBSBD, VIRUSTASK, FOOTWINE, BLUELIGHT, SPLITDROP, TWINTASK, TWINTALK, GHOSTFORM,** and **ClipXDaemon.**

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 **three exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **APT37, Dust Specter,** and malware **FOOTWINE, BLUELIGHT, RESTLEAF,** and **ClipXDaemon** in Breach and Attack Simulation(BAS).

Threat Advisories

Dohdoor Malware Campaign Targeting U.S. Education and Healthcare Sectors

Ruby Jumper: APT37's Cloud-to-Air-Gap Espionage Framework

Iran-Linked Dust Specter Launches Cyberattack on Iraqi Officials

VMware Patches Aria Operations Flaws as Exploitation Emerges in the Wild

ClipXDaemon Clipboard Attack: Linux Malware Targeting Crypto Payments

Cisco Warns of Actively Exploited Flaws in Catalyst SD-WAN Manager

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
Dohdoor	SHA256	54e18978c6405f56cd59ba55a62291436639f21cf325ae509f0599b15e8f7f53
RESTLEAF	MD5	ad556f4eb48e7dba6da14444dcce3170
	SHA256	cf2e3f46b26bae3d11ab6c2957009bc1295b81463dd67989075592e81149c8ec
SNAKEDROPPER	MD5	098d697f29b94c11b52c51bfe8f9c47d
THUMBSBD	Domains	philion[.]store, homeatedke[.]store, hightkdhe[.]store
VIRUSTASK	MD5	5c6ff601ccc75e76c2fc99808d8cc9a9
FOOTWINE	MD5	476bce9b9a387c5f39461d781e7e22b9
	SHA256	c61c679eec1c1b43bbd01727fdfb6a69b11485931eb8569e6b20ada30bfe84af
	IPv4:Port	144[.]172[.]106[.]66[:]8080
BLUELIGHT	MD5	585322a931a49f4e1d78fb0b3f3c6212
	SHA256	a8b8a92d170029885d4e7763675f10eb172150f8503592677cadedc392edccf4
SPLITDROP	MD5	78275f3fc7e209b85bff6a6f99acc68a
	SHA1	fc08f8403849c6233978a363f4cdc58cd7041823
	SHA256	6bb0d45799076b3f2d7f602b978a0779868fc72a1188374f6919fbbfba23efce
TWINTASK	MD5	19ab3fd2800f62a47bf13a4cc4e4c124
	SHA1	c79c261457def606c3393dde77c82832a5c0ded3
	SHA256	ad26cd72a83b884a8bc5aaa87309683953e151ebb3fde42eda7bf9a4406e530d

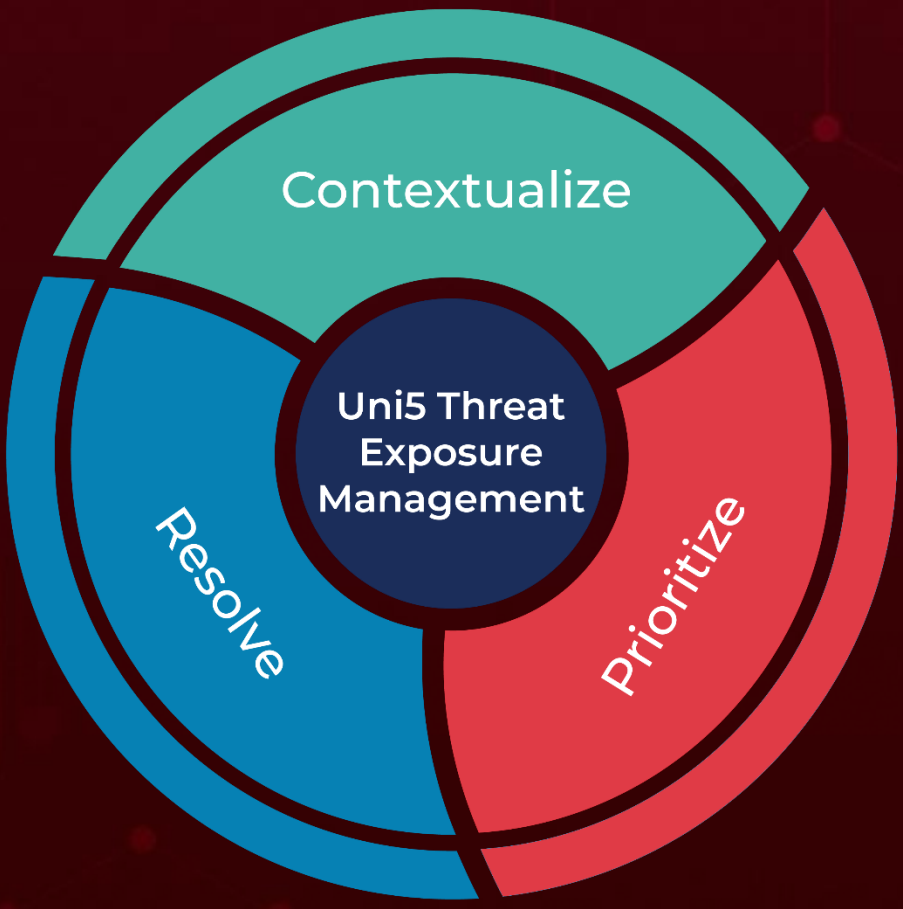
Attack Name	TYPE	VALUE
TWINTALK	MD5	63702bd6422ec2d5678d4487146ea434
	SHA1	c7dff3a0675f330feb9a7c469f8340369451d122
	SHA256	f3f2dc31f70a105db161a5e7b463b2215d3cbd64ac0146fd68e39da1c279f7ef
GHOSTFORM	MD5	b19add5ccaa17a1308993e6f3f786b06, 7f17fa22feaced1a16d4d39c545cdb16, 70a9b537b9b7e1b410576d798e6c5043, a7561eb023bb2c4025defcfe758d8ac2, 809139c237c4062baecab43570060d67
	SHA1	51a746c85bd486f223130173b7e674379a51b694, 369b56a89b2fce2cbdc36f5a23bdec6067242911, cb1760c90fb6c399e0125c7aa793efe37c4ce533, df04e36c106691f9fe88e5798e4ae86438bd4f1d, 8735ee29c409b8d101eb3170f011455be41b7a91
	SHA256	69294ad90aeb7f05e501e7191c95beb14e23da5587dd75557c867e2944a57fdc, fa51aff99d86a9f1f65aa0ebbf6ca40411d343cea59370851ab328b97e2164bb, a27d53608ab05b5c7cb86bcf4a273435238beeb7e7efd7845375b2aa765f51e2, eb5b7275c41de8e98d72696eeac9cba3719f334f8e7974e6b8760ece820b1d0c, 3a66ae5942f6feb79cf81ee70451f761253e0e0bde95f0840abdd42a804fad39, 797325b3c8a9356dcace75d93cb5cfb7847d2049c66772d4cc2cee821618cb96
ClipXDaemon	SHA256	b6bb28160532400eafad532842e4ba9add6d6bbba4f7e7c85e3dbb650369eb00

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 10, 2026 • 8:20 AM

More at www.hivepro.com