Date of Publication
February 16, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

09 to 15 FEBRUARY 2026

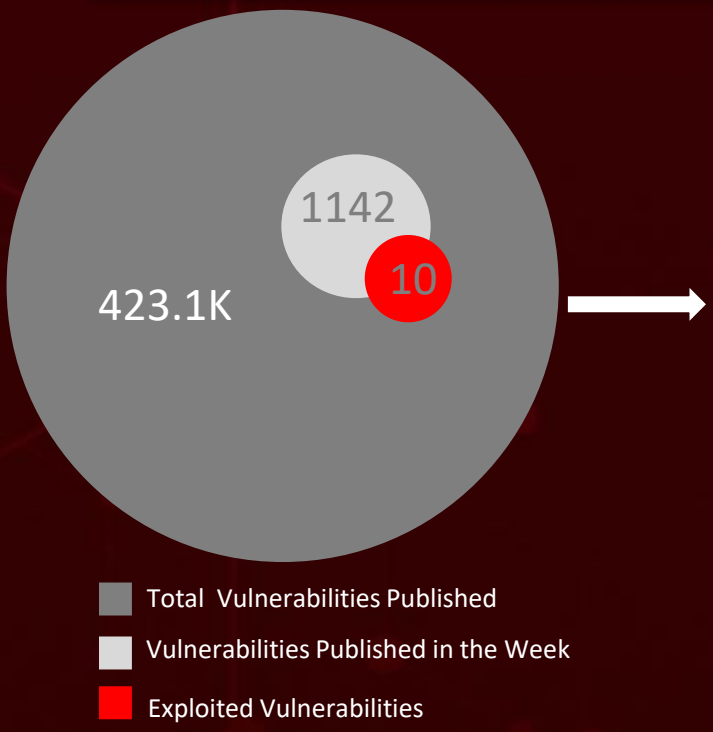
Table Of Contents

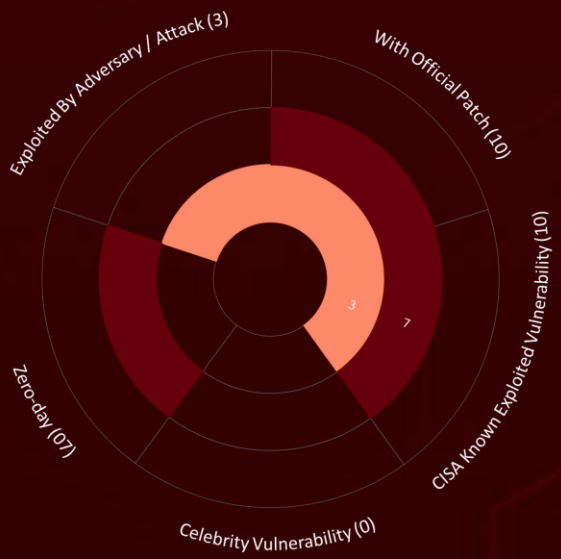
Summary

HiveForce Labs has observed a notable surge in cyber threats, reflecting how rapidly global attack activity is growing in both scale and sophistication. Within just one week, analysts tracked **seven** major incidents, the disclosure of **ten** critical vulnerabilities, and active operations from **two** threat actor groups, an unsettling combination that points to increasingly aggressive and coordinated malicious campaigns worldwide.

Attackers are already capitalizing on critical SmarterMail flaws, **CVE-2026-23760** and **CVE-2026-24423**, to seize administrator accounts and execute remote commands on exposed servers, effectively transforming email infrastructure into gateways for deeper network compromise. Activity attributed to Storm-2603 shows how quickly these breaches can evolve into ransomware staging operations, with adversaries masking malicious actions as routine processes and even misusing legitimate security tools to evade detection. At the same time, Apple has issued urgent patches to address **CVE-2026-20700**, a zero-day memory corruption flaw in dyld that has already been exploited in highly targeted, sophisticated attacks, underscoring how quickly attackers weaponize newly discovered weaknesses.

Meanwhile, the state-aligned espionage group **TGR-STA-1030**, also tracked as UNC6619, continues to expand its global intelligence-gathering operations, compromising over 70 organizations across 37 countries and conducting reconnaissance against government infrastructure worldwide. Government, diplomatic, law enforcement, and critical infrastructure sectors remain primary targets, illustrating how cyber operations increasingly intersect with geopolitical interests. Together, these developments highlight a clear reality: disciplined patch management, continuous monitoring, and proactive defense strategies are now essential to keep pace with rapidly evolving attack techniques.





High Level Statistics

7
Attacks Executed

10
Vulnerabilities Exploited

2
Adversaries in Action

- Warlock
- ShadowGuard
- Diaoyu
- VShell
- Havoc
- Sliver
- SparkRat

- CVE-2026-24423
- CVE-2026-23760
- CVE-2019-11580
- CVE-2026-21510
- CVE-2026-21513
- CVE-2026-21514
- CVE-2026-21519
- CVE-2026-21525
- CVE-2026-21533
- CVE-2026-20700

- Storm-2603
- TGR-STA-1030

Insights

CVE-2026-21513 is a zero-day in the MSHTML framework that bypasses security protections when users open malicious links or crafted HTML content.

Microsoft's **February 2026** Patch Tuesday drops fixes for **59 flaws**, spotlighting **six zero-days** already being weaponized in the wild.

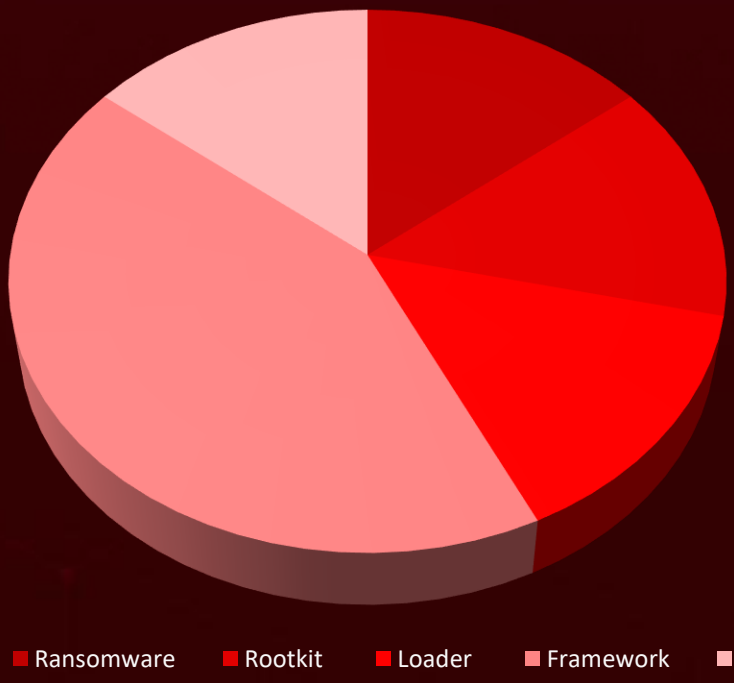
Apple patched **CVE-2026-20700**, a critical zero-day that could let attackers silently take over vulnerable devices.

Attackers are exploiting **CVE-2026-23760** and **CVE-2026-24423** to seize admin control of SmarterMail servers from SmarterTools, turning email systems into entry points for ransomware and broader network compromise.

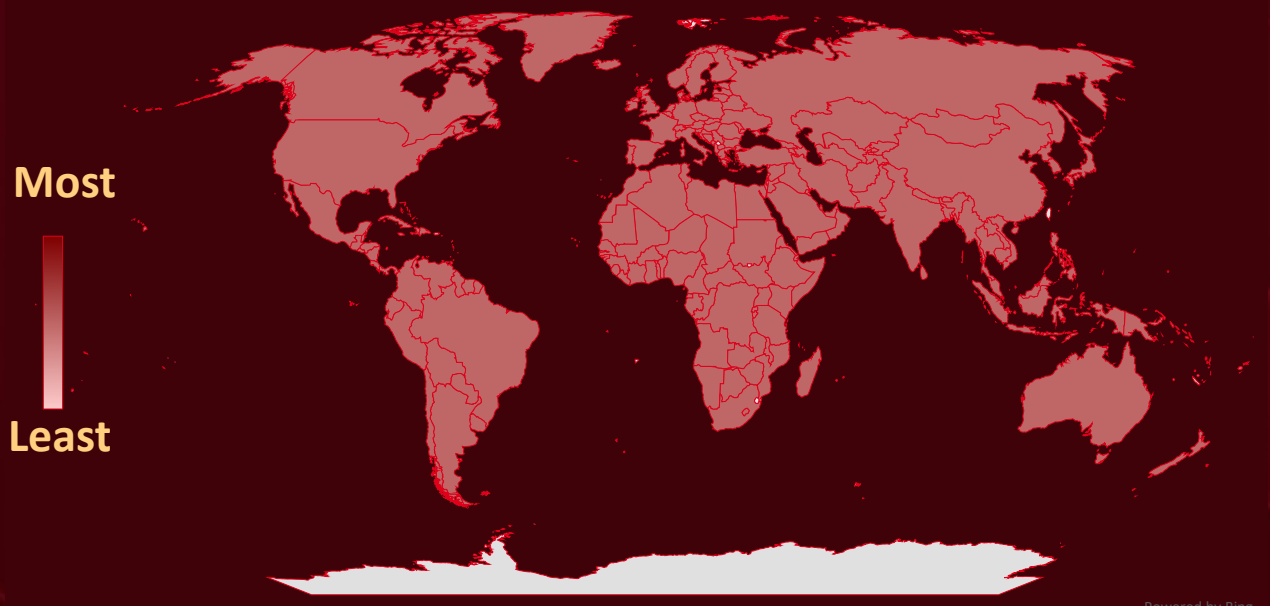
Active since early 2024, **TGR-STA-1030** (aka UNC6619) has compromised dozens of organizations worldwide, conducting wide-scale reconnaissance and long-term espionage against government and critical infrastructure targets.

CVE-2026-21514 allows crafted Office documents to bypass Word's OLE protections and trigger exploitation, now patched by Microsoft.

Threat Distribution



Targeted Countries



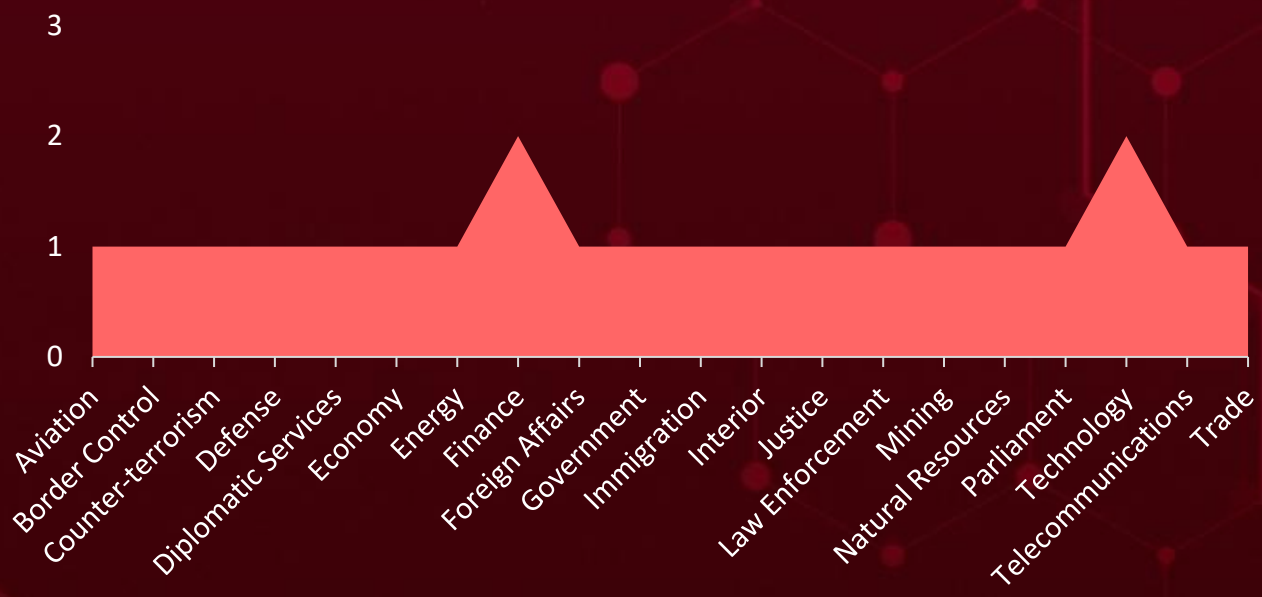
Countries
Afghanistan
Albania
Algeria
Andorra
Angola
Antigua and Barbuda
Argentina
Armenia
Australia
Austria
Azerbaijan
Bahamas
Bahrain
Bangladesh
Barbados
Belarus
Belgium
Belize
Benin
Bhutan
Bolivia
Bosnia and Herzegovina
Botswana

Countries
Brazil
Brunei
Bulgaria
Burkina Faso
Burundi
Cabo Verde
Cambodia
Cameroon
Canada
Central African Republic
Chad
Chile
China
Colombia
Costa Rica
Côte d'Ivoire
Croatia
Cuba
Cyprus
Czechia (Czech Republic)
Democratic Republic of the Congo
Denmark
Djibouti

Countries
Finland
France
Gabon
Gambia
Georgia
Germany
Ghana
Greece
Grenada
Guatemala
Guinea
Guinea-Bissau
Guyana
Haiti
Holy See
Honduras
Hungary
Iceland
India
Indonesia
Iran
Iraq
Ireland
Israel
Italy

Countries
Uganda
Ukraine
United Arab Emirates
United Kingdom
United States of America
Uruguay
Uzbekistan
Vanuatu
Venezuela
Vietnam
Yemen
Zambia
Zimbabwe
French Guiana
Poland
Portugal
Qatar
Romania
Russia
Liberia
Libya
Liechtenstein
Lithuania
Luxembourg
Madagascar

Targeted Industries



TOP MITRE ATT&CK TTPs

T1068 Exploitation for Privilege Escalation	**T1036** Masquerading	**T1189** Drive-by Compromise	**T1566** Phishing	**T1059** Command and Scripting Interpreter
T1190 Exploit Public-Facing Application	**T1203** Exploitation for Client Execution	**T1204** User Execution	**T1204.002** Malicious File	**T1071** Application Layer Protocol
T1566.002 Spearphishing Link	**T1071.001** Web Protocols	**T1218** System Binary Proxy Execution	**T1518.001** Security Software Discovery	**T1564.003** Hidden Window
T1553 Subvert Trust Controls	**T1078** Valid Accounts	**T1021** Remote Services	**T1090** Proxy	**T1543.003** Windows Service

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Warlock	Warlock is a ransomware-as-a-service (RaaS) operation that debuted in June 2025 with an ad on a Russian cybercrime forum ("if you want a Lamborghini, please call me") and swiftly garnered attention by targeting businesses, governments, and other institutions.	Exploiting Vulnerabilities	CVE-2026-23760
		IMPACT	AFFECTED PRODUCTS
TYPE		Financial Loss, Data Encryption, and Exfiltration	SmarterTools SmarterMail
Ransomware			PATCH LINK
ASSOCIATED ACTOR			https://www.smartertools.com/smartermail/release-notes/current
-			
IOC TYPE	VALUE		
SHA256	d1f9ace720d863fd174753e89b9e889d2e2f71a287fde66158bb2b5752307474		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
ShadowGuard	ShadowGuard is a Linux-focused rootkit built using Extended Berkeley Packet Filter (eBPF) technology, allowing it to run directly inside the kernel's trusted environment. Because eBPF programs execute within the kernel's BPF virtual machine rather than as standalone modules, the malware leaves little visible footprint, making detection extremely difficult. This design enables ShadowGuard to operate stealthily while maintaining deep control over compromised systems.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	Atlassian Crowd and Crowd Data Center
Rootkit			PATCH LINK
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			
IOC TYPE	VALUE		
SHA256	7808B1E01EA790548B472026AC783C73A033BB90BBE548BF3006ABFBCB48C52D		

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
Diaoyu	Diaoyu Loader uses a dual-stage execution check to evade automated sandboxes and analysis environments. It first verifies that the system meets a minimum horizontal screen resolution of 1440 pixels, then checks for the presence of a specific file (pic1.png) in its working directory. If these conditions are not met, the malware halts execution, helping it avoid detection in controlled analysis setups.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	**AFFECTED PRODUCT**
TYPE		Loads Cobalt Strike payload	Atlassian Crowd and Crowd Data Center
Loader			**PATCH LINK**
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			
IOC TYPE	**VALUE**		
SHA256	23ee251df3f9c46661b33061035e9f6291894ebe070497ff9365d6ef2966f7fe, 66ec547b97072828534d43022d766e06c17fc1cafe47fbd9d1ffc22e2d52a9c0		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
VShell	VShell is a Go-based command-and-control (C2) framework commonly linked to cyber espionage operations. It enables attackers to maintain remote access to compromised systems, execute commands, and manage files during post-exploitation activities.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	**AFFECTED PRODUCT**
TYPE		Remote Control	Atlassian Crowd and Crowd Data Center
Framework			**PATCH LINK**
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			

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
Havoc	Havoc is an open-source command-and-control (C2) framework developed by C5pider. It allows operators to generate agents in multiple formats, including Windows executables, DLLs, and shellcode. Its modular architecture lets attackers tailor payloads for different objectives, making it a versatile toolkit for post-exploitation operations.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	AFFECTED PRODUCT
TYPE		System Compromise	Atlassian Crowd and Crowd Data Center
Framework			PATCH LINK
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			
IOC TYPE	VALUE		
SHA256	b773fa65bb375e6fe6d387f301f6bf33219189ea1d4a06762e965a9eba7de4e8		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Sliver	Sliver is an advanced malware framework used in cyberattacks, leveraging DLL sideloading and proxying techniques for persistence and stealth. It targets organizations, enabling data exfiltration and espionage while evading detection.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	AFFECTED PRODUCT
TYPE		Data exfiltration and Espionage	Atlassian Crowd and Crowd Data Center
Framework			PATCH LINK
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			
IOC TYPE	VALUE		
SHA256	e576938b137260200dd6a7e650b32adbf9cbe4b69199e98b06b1a0f4f3b8fff3		

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
SparkRat	SparkRAT is a cross-platform, open-source remote administration tool written in Go and released via GitHub in 2022. It supports Windows, macOS, and Linux, giving attackers broad remote-control capabilities, including file and process management, file transfer, remote desktop viewing, system reconnaissance, and command execution through a remote terminal.	Exploiting vulnerability	CVE-2019-11580
		IMPACT	**AFFECTED PRODUCT**
TYPE		System Compromise	Atlassian Crowd and Crowd Data Center
RAT			**PATCH LINK**
ASSOCIATED ACTOR			https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html
TGR-STA-1030			
IOC TYPE	**VALUE**		
SHA256	908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe326e00697		

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-2026-24423		SmarterTools SmarterMail (Before Build 9511)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:smartertools:smartermail:*:*:*:*:*:*:*:*	Warlock ransomware
SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.smartertools.com/smartermail/release-notes/current

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-23760		SmarterTools SmarterMail (Before Build 9511)	Storm-2603
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:smartertools:smartermail:*:*:*:*:*:*:*:*	Warlock ransomware
SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://www.smartertools.com/smartermail/release-notes/current

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2019-11580		Atlassian Crowd and Crowd Data Center	TGR-STA-1030 (aka UNC6619)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:crowd:*:*:*:*:*:*:*:*	ShadowGuard, Diaoyu, VShell, Cobalt Strike, Havoc, Sliver, SparkRat
Atlassian Crowd and Crowd Data Center Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	-	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21510	✗	Windows Shell	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:window:*:*:*:*:*:*:*:* pe:2.3:o:microsoft:windows_server*:*:*:*:*:*:*:*:*	-
Windows Shell Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1204.001: Malicious Link, T1204: User Execution	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21510

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21513	✗	MSHTML Framework	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:window:*:*:*:*:*:*:*:* pe:2.3:o:microsoft:windows_server*:*:*:*:*:*:*:*:*	-
MSHTML Framework Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-693	T1204: User Execution, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21513

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21514	✗	Microsoft Office Word	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:365_apps:-:*:*:*:enterprise:*:* cpe:2.3:a:microsoft:office_long_term_servicing_channel:*:*:*:*:*	-
Microsoft Word Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-807	T1566: Phishing	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21514

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21519	✗	Desktop Window Manager	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:window:*:*:*:*:*:*:*:* pe:2.3:o:microsoft:windows_server*:*:*:*:*:*:*:*:*	-
Desktop Window Manager Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-843	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21519

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21525	✗	Windows Remote Access Connection Manager	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:window:*:*:*:*:*:*:*:* pe:2.3:o:microsoft:windows_server*:*:*:*:*:*:*:*:*	-
Windows Remote Access Connection Manager Denial of Service Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-476	T1499: Endpoint Denial of Service	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21525

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21533	✗	Windows Remote Desktop	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:window:*:*:*:*:*:*:*:* pe:2.3:o:microsoft:windows_server*:*:*:*:*:*:*:*:*	-
Windows Remote Desktop Services Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-269	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21533

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-20700</td><td>✗</td><td rowspan="2">Apple iOS (Before26.3), Apple iPadOS (Before 26.3), Apple macOS Tahoe (Before 26.3), Apple tvOS (Before 26.3), Apple watchOS (Before 26.3), Apple visionOS (Before 26.3)</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:o:apple:iphone_os:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td>Apple Multiple Buffer Overflow Vulnerability</td><td>✓</td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-119</td><td>T1189: Drive-by Compromise, T1068: Exploitation for Privilege Escalation, T1574: Hijack Execution Flow, T1574.004: Dylib Hijacking</td><td>https://support.apple.com/en-us/126346 , https://support.apple.com/en-us/126348 , https://support.apple.com/en-us/126351 , https://support.apple.com/en-us/126352 , https://support.apple.com/en-us/126353</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Storm-2603	China	All	Worldwide
	MOTIVE		
	Financial Gain		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2026-23760	-	SmarterTools SmarterMail
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0011: Command and Control; TA0040: Impact; TA0042: Resource Development; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1078: Valid Accounts; T1068: Exploitation for Privilege Escalation; T1218: System Binary Proxy Execution; T1218.007: Msiexec; T1036: Masquerading; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1486: Data Encrypted for Impact; T1588: Obtain Capabilities; T1588.006: Vulnerabilities			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
TGR-STA-1030 (aka UNC6619)</td><td>Asia</td><td rowspan="3">Government, Foreign Affairs, Finance, Interior, Justice, Trade, Economy, Energy, Immigration, Mining, Natural Resources, Law Enforcement, Border Control, Counter-terrorism, Defense, Telecommunications, Aviation, Financial Services, Technology, Public Sector IT, Parliament, Diplomatic Services</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2019-11580</td><td>ShadowGuard, Diaoyu, VShell, Cobalt Strike, Havoc, Sliver, SparkRat</td><td>Atlassian Crowd and Crowd Data Center</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0003: Persistence; TA0011: Command and Control; TA0042: Resource Development; TA0004: Privilege Escalation; TA0043: Reconnaissance; T1566: Phishing; T1566.002: Spearphishing Link; T1190: Exploit Public-Facing Application; T1204: User Execution; T1204.002: Malicious File; T1497: Virtualization/Sandbox Evasion; T1497.001: System Checks; T1014: Rootkit; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1564.003: Hidden Window; T1518: Software Discovery; T1518.001: Security Software Discovery; T1505: Server Software Component; T1505.003: Web Shell; T1105: Ingress Tool Transfer; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1572: Protocol Tunneling; T1090: Proxy; T1090.002: External Proxy; T1583: Acquire Infrastructure; T1583.001: Domains; T1583.003: Virtual Private Server; T1068: Exploitation for Privilege Escalation; T1595: Active Scanning; T1595.002: Vulnerability Scanning</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **ten exploited vulnerabilities** and block the indicators related to the threat actors **Storm-2603, TGR-STA-1030,** and malware **Warlock Ransomware, ShadowGuard, Diaoyu, VShell, Havoc, Sliver,** and **SparkRat.**

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 **ten exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actors **Storm-2603, TGR-STA-1030,** and malware **Warlock Ransomware,** and **Diaoyu** in Breach and Attack Simulation(BAS).

Threat Advisories

Unpatched SmarterMail Servers Become Launchpads for Ransomware Operations

TGR-STA-1030: Global State-Aligned Cyber Espionage Campaign

Microsoft’s February 2026 Patch Tuesday Fixes Active Zero-Day Exploits

Apple Zero-Day Exploited in Targeted Attacks (CVE-2026-20700)

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)

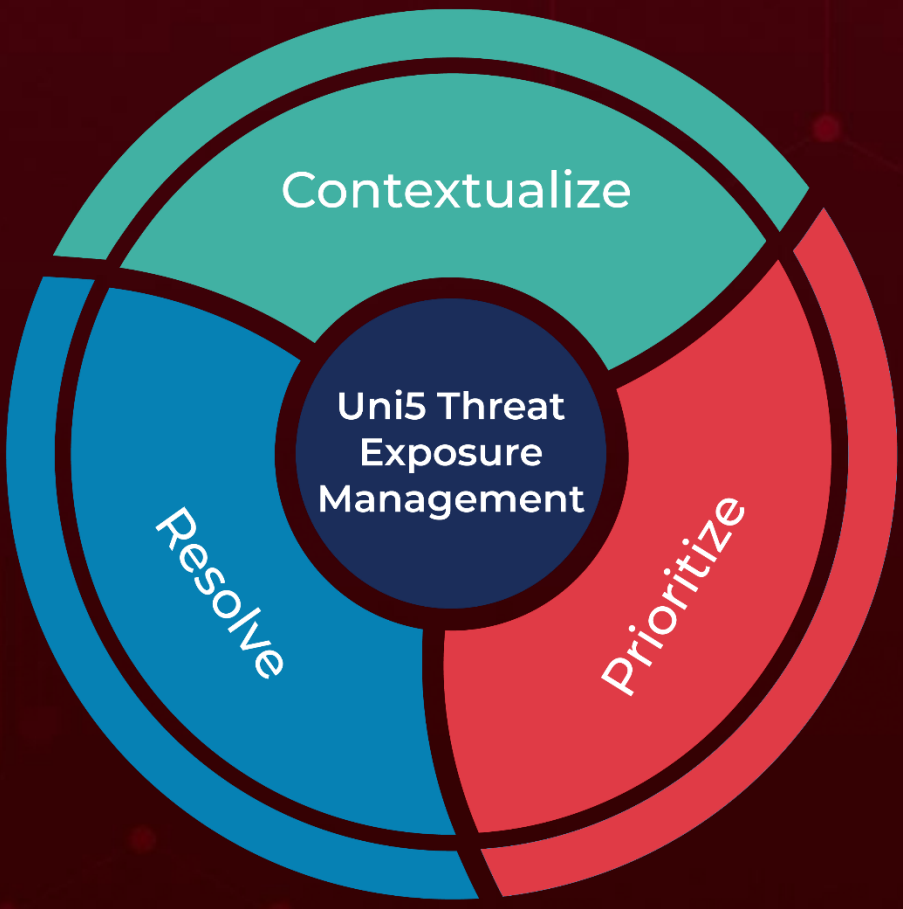
Attack Name	TYPE	VALUE
Warlock	SHA256	d1f9ace720d863fd174753e89b9e889d2e2f71a287fde66158bb2b5752307474
ShadowGuard	SHA256	7808B1E01EA790548B472026AC783C73A033BB90BBE548BF3006ABFBCB48C52D
Diaoyu	SHA256	23ee251df3f9c46661b33061035e9f6291894ebe070497ff9365d6ef2966f7fe, 66ec547b97072828534d43022d766e06c17fc1cafe47fbd9d1ffc22e2d52a9c0
Havoc	SHA256	b773fa65bb375e6fe6d387f301f6bf33219189ea1d4a06762e965a9eba7de4e8, 17637fac7f989549acd248ca9e5293d2b9a1a2e4bb0f7e4edf5571df35129f0c, 9f797d705facebd1687b7765cbf65231e71821eb3c38dcc171a3fc88b9f52328, b6cb8a7cdce0bfd3a7402d22fb0014dedb259d6c91c1538ac74097b8ca22ca5c
Sliver	MD5	8b553728900ba2e45b784252a1ff6d17, 9dc2819c176c60e879f28529b1b08da1
	SHA1	953bd0859c86e0a3a3da52fe392a7d579a9f937b, 538cb25bfae6501d8c3c7053a293e8ca85a8dba4
	SHA256	e576938b137260200dd6a7e650b32adbf9cbe4b69199e98b06b1a0f4f3b8fff3, b0555d287f41b160d3b8a275df2c00b112e98a5db7dd83907411415e5428f7a9
SparkRat	SHA256	908b30abf730a5b51a3d25965eff45a639e881a97505220a38591fe326e00697

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

February 16, 2026 . 7:00 AM

More at www.hivepro.com