Date of Publication
March 16, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

09 to 15 MARCH 2026

Table Of Contents

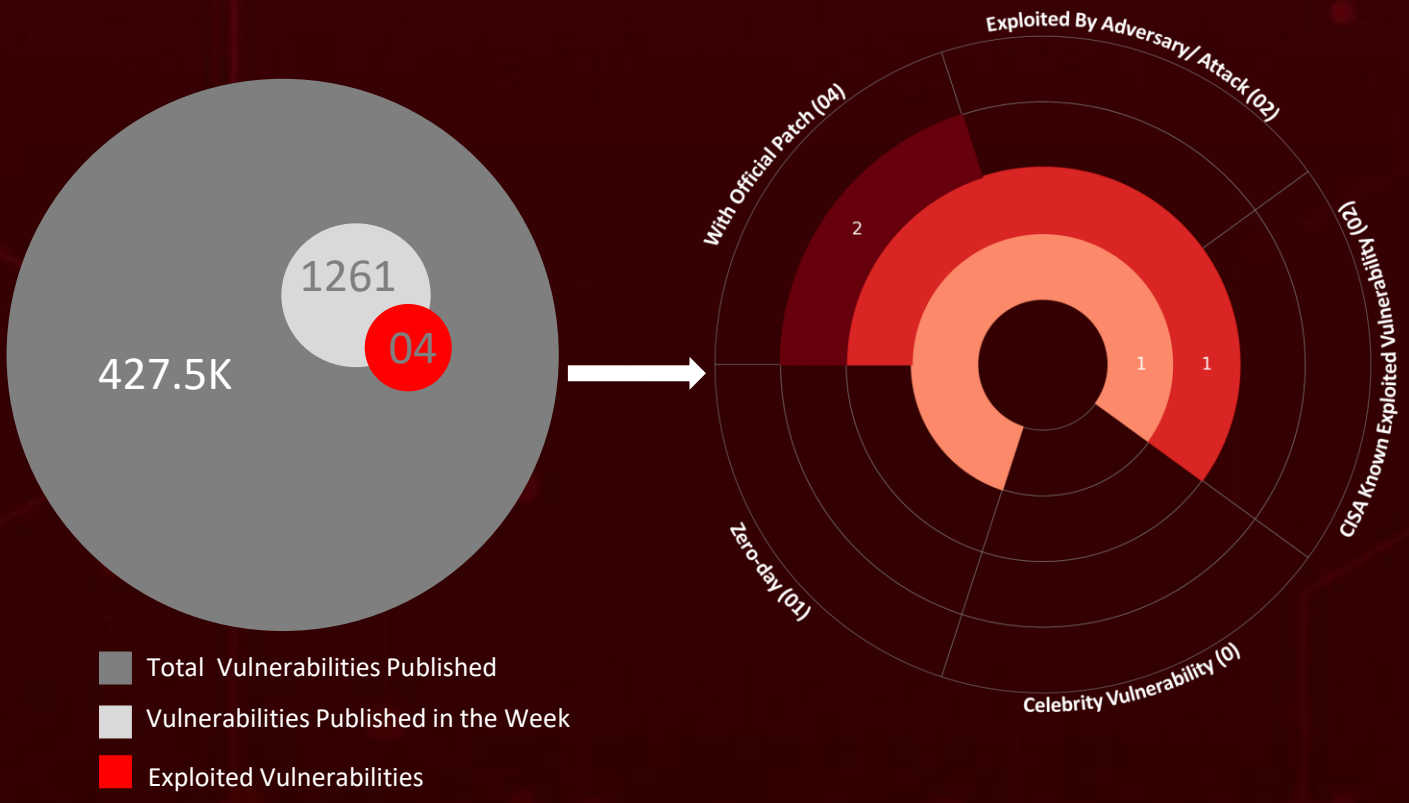
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **13** major attacks were detected, **four** critical vulnerabilities were publicly disclosed, and **four** active threat actor groups were monitored, signaling a concerning escalation in malicious activity.

Mustang Panda is distributing the **LOTUSLITE** backdoor through malicious ZIP archives using **Iran conflict-themed lures**. The files reference Iranian missile strikes on **U.S. military bases** to trick victims into opening them.

Void Manticore is an **Iranian state-sponsored** threat group linked to the **Ministry of Intelligence and Security (MOIS)**. The group conducts hybrid cyber warfare through wiper malware such as **BiBi** Wiper, coordinated data leaks, and psychological operations.

Finally, the **Russian-linked group APT28** is targeting **Ukrainian government** organizations by exploiting the **Microsoft Office** vulnerability **CVE-2026-21509**. The attackers distribute weaponized documents via spear-phishing and messaging platforms such as Signal. These underscore the need for disciplined security updates and sustained monitoring in response to rapidly evolving attack methodologies.



High Level Statistics

13
Attacks Executed

4
Vulnerabilities Exploited

4
Adversaries in Action

- A0Backdoor
- LOTUSLITE
- BiBi Wiper
- CI Wiper
- No-Justice Wiper
- SlimAgent
- BeardShell
- Covenant
- VENON
- Slopoly
- NodeSnake
- Interlock
- InterlockRAT
- CVE-2019-0604
- CVE-2026-26127
- CVE-2026-21262
- CVE-2026-21509
- Mustang Panda
- Void Manticore
- APT28
- Hive0163

Insights

The Helpdesk Hoax: How Social Engineers Breach **Financial and Healthcare** Networks

From Homeland Justice to Handala: The Evolving Faces of Void Manticore

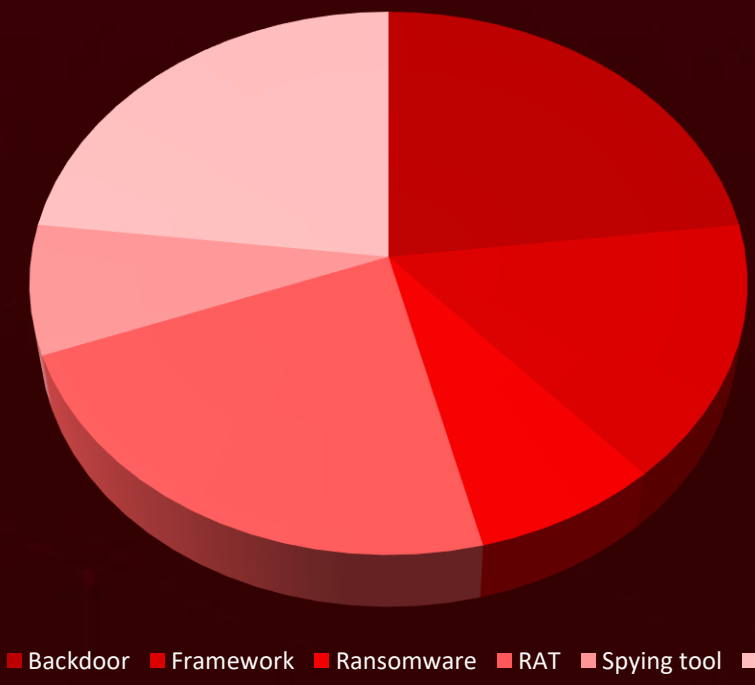
War as Bait: Mustang Panda's Iran-Themed Malware Campaign

APT28 Exploits Microsoft Office Flaw to Spy on Ukrainian Government Systems

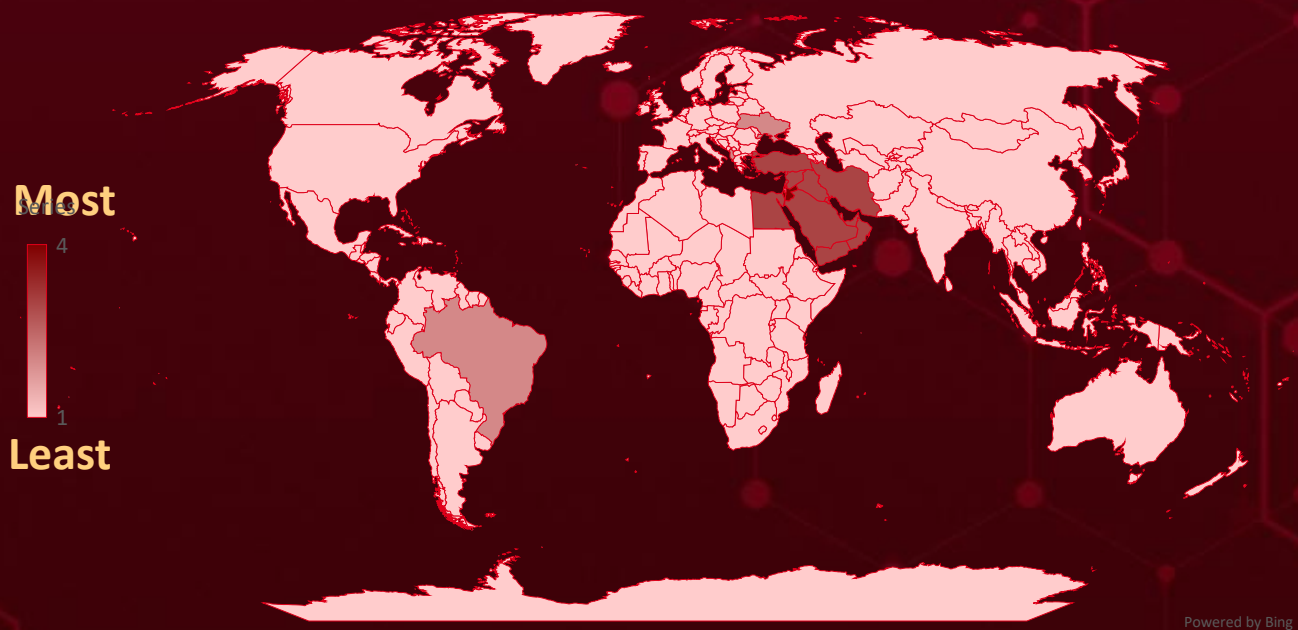
VENON RAT Campaign Targets 33 **Brazilian Financial** and **Crypto** Platforms

PhantomRaven: The **npm Supply Chain Campaign** Infecting JavaScript Ecosystems

Threat Distribution

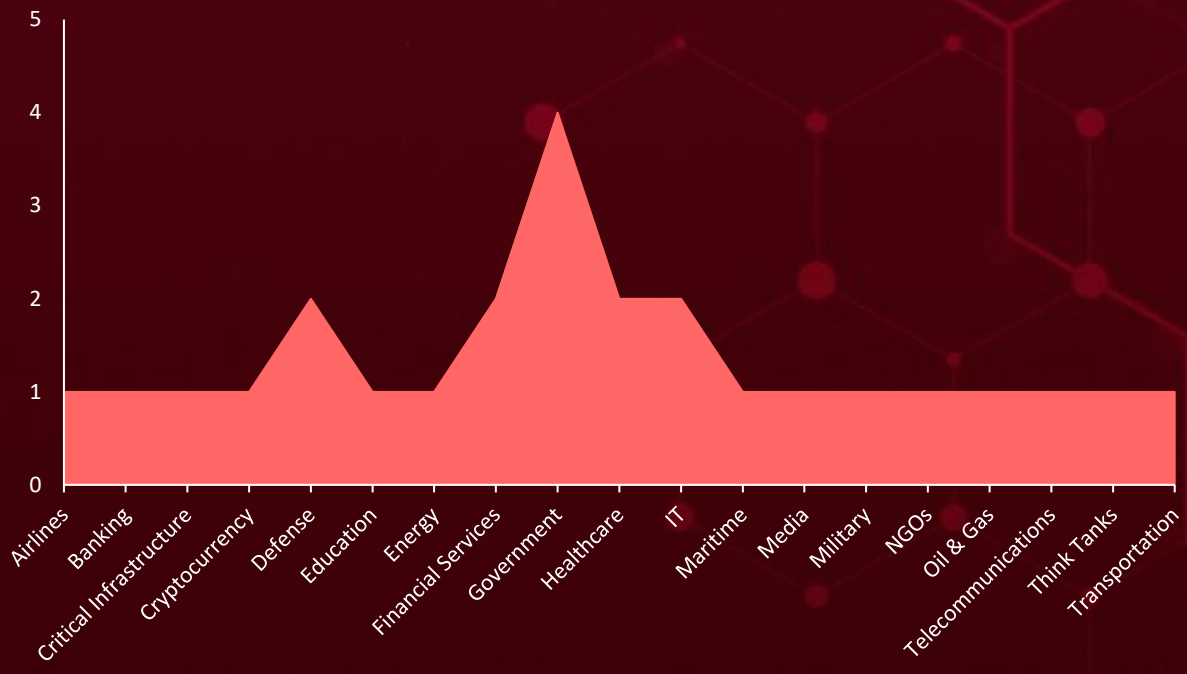


Targeted Countries



Countries	Countries	Countries	Countries
Israel	Pakistan	Slovenia	Portugal
Jordan	Botswana	Colombia	Dominican Republic
Yemen	South Korea	Sudan	Rwanda
Syria	Belgium	Comoros	Ecuador
Qatar	Marshall Islands	Bangladesh	Samoa
Egypt	Brunei	Congo-Brazzaville	Algeria
Cyprus	New Zealand	United States of America	Senegal
Iran	Bulgaria		El Salvador
Oman	Philippines	Costa Rica	Singapore
Iraq	Burkina Faso	Mali	Equatorial Guinea
Saudi Arabia	Seychelles	Côte d'Ivoire	Somalia
Bahrain	Burundi	Mauritius	Eritrea
Turkey	Togo	Croatia	Spain
United Arab Emirates	Cabo Verde	Monaco	Estonia
	Malaysia	Cuba	Sweden
Kuwait	Cambodia	Mozambique	Eswatini
Lebanon	Micronesia	Belize	Trinidad and Tobago
Ukraine	Cameroon	Nepal	Ethiopia
Albania	Namibia	Czechia	United Kingdom
Palestine	Canada	Niger	Finland
Brazil	North Korea	Democratic Republic of the Congo	Uzbekistan
Akrotiri and Dhekelia	Central African Republic		France
		Norway	Malta
Saint Lucia	Panama	Denmark	Gambia
Montenegro	Chad	Bhutan	Mauritania
Benin	Romania	Djibouti	Georgia
Bosnia and Herzegovina	Chile	Paraguay	Mexico
	China	Dominica	Germany

Targeted Industries



TOP MITRE ATT&CK TTPs

T1071 Application Layer Protocol	**T1204** User Execution	**T1071.001** Web Protocols	**T1059** Command and Scripting Interpreter	**T1204.002** Malicious File
T1566 Phishing	**T1036** Masquerading	**T1027** Obfuscated Files or Information	**T1082** System Information Discovery	**T1572** Protocol Tunneling
T1574 Hijack Execution Flow	**T1105** Ingress Tool Transfer	**T1140** Deobfuscate/ Decode Files or Information	**T1102** Web Service	**T1078** Valid Accounts
T1574.001 DLL	**T1567** Exfiltration Over Web Service	**T1547** Boot or Logon Autostart Execution	**T1059.001** PowerShell	**T1547.001** Registry Run Keys / Startup Folder

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
A0Backdoor	A0Backdoor uses runtime decryption to hide its core logic, making static analysis difficult. Upon execution, it allocates new memory and copies its code there. While this self-copying doesn't directly affect functionality, it's still significant. After decryption, the backdoor collects system-specific information to fingerprint the compromised machine.	Social Engineering	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Obscured Behavior, Memory Manipulation, Information Theft	
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
IOC TYPE	**VALUE**		
SHA256	26db06a2319c09918225e59c404448d92fe31262834d70090e941093e6bb650a		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
LOTUSLITE	LOTUSLITE is a C++ backdoor used for espionage, connecting to a hard-coded IP-based command-and-control server. It enables remote tasking, data theft, and ensures persistence, surviving system reboots. Its functionality is minimal but effective for covert operations.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Remote Control	
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			-
Mustang Panda			
IOC TYPE	**VALUE**		
SHA256	856476340706411772621 1ff8f89555e5a3b2b70bc9667032abd69cbe53b5216		

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
BiBi Wiper	BiBi Wiper is a custom destructive malware designed to permanently damage files on compromised systems. It accepts command-line parameters such as target_path to specify which files or directories to wipe. The malware launches multiple threads based on the system's CPU cores to speed up the wiping process and uses a queue to coordinate tasks between them. It overwrites targeted files with random data and then renames them using random filenames with the ".BiBi" extension, rendering the files unusable.	Phishing	CVE-2019-0604
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Operational disruption	Microsoft SharePoint
Wiper			**PATCH LINK**
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604
Void Manticore			
IOC TYPE	**VALUE**		
SHA256	74d8d60e900f931526a911b7157511377c0a298af986d42d373f51aac4f362f6		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Cl Wiper	Cl Wiper is a destructive malware that erases data by executing cl.exe with command-line arguments and abusing the legitimate rwdsk.sys driver from ElRawDisk to gain raw access to disks, files, and partitions. This allows the malware to overwrite critical data and render systems unusable. Notably, the license key embedded in the wiper matches one used in the ZeroCleare malware, which has previously been linked to actors associated with Iran's Ministry of Intelligence and Security (MOIS), suggesting possible tooling overlap.	Phishing	CVE-2019-0604
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Operational disruption	Microsoft SharePoint
Wiper			**PATCH LINK**
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604
Void Manticore			
IOC TYPE	**VALUE**		
SHA256	e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0		

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
No-Justice Wiper	No-Justice wiper is a 220.34 KB binary that requires administrator privileges to erase the data on the computer.	Phishing	CVE-2019-0604
		IMPACT	AFFECTED PRODUCT
TYPE		Information Theft, Operational disruption	Microsoft SharePoint
Wiper			PATCH LINK
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604
Void Manticore			
IOC TYPE	VALUE		
SHA256	36cc72c55f572fe02836f25516d18fed1de768e7f29af7bdf469b52a3fe2531f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
SlimAgent	SlimAgent is a lightweight espionage tool derived from XAgent, the primary backdoor used by the APT28 group. It is designed for stealthy surveillance and can log keystrokes, capture screenshots, and collect clipboard data, allowing attackers to monitor user activity and steal sensitive information.	Exploiting The Microsoft Office Vulnerability	CVE-2026-21509
		IMPACT	AFFECTED PRODUCT
TYPE		Clipboard data theft	Microsoft Office
Spying tool			PATCH LINK
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509
APT28			
IOC TYPE	VALUE		
SHA1	5603e99151f8803c13d48d83b8a64d071542f01b		

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
BeardShell	BeardShell is a sophisticated malware implant that executes PowerShell commands within a .NET runtime environment. It uses the legitimate cloud storage service Icedrive as its command-and-control (C2) channel, allowing attackers to issue commands and maintain remote access while blending malicious traffic with normal cloud activity.	Exploiting The Microsoft Office Vulnerability	CVE-2026-21509
		IMPACT	**AFFECTED PRODUCT**
TYPE		Persistent unauthorized access	Microsoft Office
Backdoor			**PATCH LINK**
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509
APT28			
IOC TYPE	**VALUE**		
SHA1	6d39f49aa11ce0574d581f10db0f9bae423ce3d5		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Covenant	Covenant is an open-source .NET post-exploitation framework that allows attackers to create and manage implants through a web-based dashboard. In espionage operations, it can be used for long-term system access and control, enabling attackers to manage compromised machines efficiently during extended campaigns.	Exploiting The Microsoft Office Vulnerability	CVE-2026-21509
		IMPACT	**AFFECTED PRODUCT**
TYPE		Remote system control	Microsoft Office
Framework			**PATCH LINK**
ASSOCIATED ACTOR			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509
APT28			
IOC TYPE	**VALUE**		
SHA256	27a331384cfca9a4d2aa45afdc12c7156cfb4da775f1380d4870f06fbb77ccf2, 1b2b83d462493eb63d6655103cf968d396ee7bdf7dd317f8cb5a5eadee6b560f		

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
VENON	VENON is a Rust-based banking Remote Access Trojan (RAT) that targets financial platforms. It uses DLL sideloading through a legitimate NVIDIA executable, multiple anti-analysis evasion techniques, and advanced encryption to avoid detection. The malware also deploys credential-stealing banking overlays and uses VBScript-based shortcut hijacking to target banking applications.	Phishing	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Banking credential theft, Remote system control	Windows
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
IOC TYPE	**VALUE**		
SHA256	c482286a7fdfb64d308c197a4deabcd773b8b62d9e74d1d08fcfd02568d75d72, d61be2b21e135726c547a388ecb47552559e5221894f5005ce35bdb24efc0c26		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Slopoly	Slopoly a suspected AI-assisted PowerShell backdoor that was deployed in the later stages of the attack to maintain persistent access to the compromised server. Its use suggests the threat actor may have operated the C2 framework in a live, hands-on manner during the intrusion.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Persistent backdoor access	Windows, Linux
Framework			**PATCH LINK**
ASSOCIATED ACTOR			-
Hive0163			
IOC TYPE	**VALUE**		
SHA256	0884e5590bdf3763f8529453fbd24ee46a3a460bba4c2da5b0141f5ec6a35675		

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
NodeSnake	NodeSnake, a NodeJS-based malware that acts as the first stage of a larger command-and-control (C2) framework. Once installed, NodeSnake communicates with its C2 server using HTTP POST requests, allowing attackers to establish initial control over the compromised system.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Persistent foothold	Windows, Linux
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
Hive0163			

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Interlock	INTERLOCK is a ransomware group known for its technical sophistication, using C/C++-compiled malware targeting both Windows and Linux systems. The group employs refined double-extortion tactics and runs a leak site called “Worldwide Secrets Blog” to publish stolen data and pressure victims into negotiations.	Social Engineering	-
		IMPACT	**AFFECTED PRODUCT**
TYPE		Information Theft, Financial Loss	Windows, Linux
Ransomware			**PATCH LINK**
ASSOCIATED ACTOR			-
Hive0163			

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">InterlockRAT</td><td rowspan="6">InterlockRAT is a remote access trojan that allows attackers to remotely control infected systems, execute commands, steal credentials and files, and deploy additional payloads. It typically communicates with a command-and-control server to perform reconnaissance, exfiltrate system data, and maintain persistent access for follow-on attacks such as ransomware deployment.</td><td>Social Engineering</td><td>-</td></tr>
<tr><td rowspan="2">IMPACT</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>TYPE</td><td rowspan="3">Remote system control, Sensitive data exfiltration</td><td>Windows, Linux</td></tr>
<tr><td>RAT</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">-</td></tr>
<tr><td>Hive0163</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 PRODUCT	ASSOCIATED ACTORS
CVE-2019-0604		Microsoft SharePoint Server 2019, 2013 Service Pack 1, 2010 Service Pack 2; Microsoft SharePoint Foundation 2013 Service Pack 1, 2010 Service Pack 2; Microsoft SharePoint Enterprise Server 2016	Void Manticore
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:sharepoint_enterprise_server:*:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_foundation:*:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*:*:*:*	BiBi Wiper, Cl Wiper, No-Justice Wiper
Microsoft SharePoint Remote Code Execution Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-20	T1190: Exploit Public-Facing Application, T1505: Server Software Component, T1505.003: Web Server, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell, T1608: Stage Capabilities, T1608.001: Upload Malware	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-26127	✗	Microsoft.Bcl.Memory 9.0, 10.0; .NET 9.0 installed on Windows, Mac OS, Linux; .NET 10.0 installed on Linux, Mac OS, Windows	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:.net_core:*:*:*:*:*:*:*:*	-
.NET Denial of Service Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1498: Network Denial of Service, T1499: Endpoint Denial of Service, T1499.001: OS Exhaustion Flood	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26127

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-21262	✗	Microsoft SQL Server 2025, 2022, 2019, 2017, 2016	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sql_server_*:*:*:*:*:*:*:*:*	-
SQL Server Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts, T1078.002: Domain Accounts	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21262

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-21509</td><td>  </td><td rowspan="2">Microsoft Office 2016, 2019 (64-bit edition, 32-bit edition); Microsoft Office LTSC 2024, 2021 (64-bit editions, 32-bit editions); Microsoft 365 Apps for Enterprise (64-bit Systems, 32-bit Systems)</td><td rowspan="2">APT28</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:microsoft:office:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:enterprise:*:*:*</td><td rowspan="2">SlimAgent, BeardShell, Covenant</td></tr>
<tr><td rowspan="2">Microsoft Office Security Feature Bypass Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-807</td><td>T1566: Phishing, T1204: User Execution, T1204.002: Malicious File, T1055: Process Injection</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
Mustang Panda (aka Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, Hive0154)	China	Government, Defense	Middle East
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	-	LOTUSLITE	Windows

TTPs
TA0001: Initial Access, T1566: Phishing, T1566.001: Spearphishing Attachment, TA0002: Execution, T1204: User Execution, T1204.002: Malicious File, TA0003: Persistence, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys / Startup Folder, TA0005: Defense Evasion, T1574: Hijack Execution Flow, T1574.001: DLL, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, TA0007: Discovery, T1057: Process Discovery, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1105: Ingress Tool Transfer, TA0042: Resource Development, T1584: Compromise Infrastructure, T1584.004: Server, T1588: Obtain Capabilities, T1588.002: Tool

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Void Manticore (aka HomeLand Justice, Karma, Storm-0842, Banished Kitten, Handala Hack)	Iran	Government agencies and services, Critical infrastructure, Oil & Gas, Energy, Telecommunications, Defense, NGOs, Media, Think Tanks, IT and Service Providers, Education, Transportation, Airlines, Maritime and Healthcare	Israel, United States, Albania, Jordan, Gulf States
	MOTIVE		
	Espionage, Sabotage, Geopolitical disruption, Politically and ideologically motivated		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2019-0604	BiBi Wiper, Cl Wiper, No-Justice Wiper	Windows Microsoft SharePoint and Linux

TTPs

TA0001: Initial Access, T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1566: Phishing, TA0002: Execution, T1059: Command and Scripting Interpreter, T1204: User Execution, T1204.002: Malicious File, T1047: Windows Management Instrumentation, TA0003: Persistence, T1505: Server Software Component, T1505.003: Web Shell, T1547: Boot or Logon Autostart Execution, T1547.001: Registry Run Keys, T1053: Scheduled Task/Job, TA0004: Privilege Escalation, T1078: Valid Accounts, T1078.002: Domain Accounts, T1068: Exploitation for Privilege Escalation, TA0005: Defense Evasion, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1036: Masquerading, T1140: Deobfuscate/Decode Files or Information, T1070: Indicator Removal, TA0006: Credential Access, T1003: OS Credential Dumping, T1003.001: LSASS Memory, T1555: Credentials from Password Stores, TA0007: Discovery, T1087: Account Discovery, T1087.002: Domain Account, T1082: System Information Discovery, T1018: Remote System Discovery, T1069: Permission Groups Discovery, T1069.002: Domain Groups, T1016: System Network Configuration Discovery, TA0008: Lateral Movement, T1021: Remote Services, T1021.001: Remote Desktop Protocol, T1021.002: SMB/Windows Admin Shares, T1572: Protocol Tunneling Collection, T1114: Email Collection, T1005: Data from Local System, T1039: Data from Network Shared Drive, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1090: Proxy, T1105: Ingress Tool Transfer, T1572: Protocol Tunneling, TA0010: Exfiltration, T1041: Exfiltration Over C2 Channel, T1567: Exfiltration Over Web Service, TA0042: Resource Development, T1583: Acquire Infrastructure, T1583.006: Web Services, T1587: Develop Capabilities, T1587.001: Malware,T1586: Compromise Accounts, T1585: Establish Accounts, T1585.001: Social Media Accounts, TA0040: Impact, T1485: Data Destruction, T1561: Disk Wipe, T1561.001: Disk Content Wipe, T1561.002: Disk Structure Wipe, T1486: Data Encrypted for Impact, T1491: Defacement, T1491.002: External Defacement, T1489: Service Stop, T1529: System Shutdown/Reboot, T1531: Account Access Removal, TA0043: Reconnaissance, T1590: Gather Victim Network Information, T1589: Gather Victim Identity Information, T1589.001: Credentials

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110)	Russia	Government, Military	Ukraine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCT**
	CVE-2026-21509	SlimAgent, BeardShell, Covenant	Microsoft Office

TTPs
TA0042: Resource Development, T1583: Acquire Infrastructure, T1583.006: Web Services, T1587: Develop Capabilities, T1587.001: Malware, TA0001: Initial Access, T1566: Phishing, T1566.001: Spearphishing Attachment, TA0002: Execution, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1129: Shared Modules, TA0003: Persistence, T1546: Event Triggered Execution, T1546.015: Component Object Model Hijacking, TA0005: Defense Evasion, T1211: Exploitation for Defense Evasion, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1480: Execution Guardrails, T1564: Hide Artifacts, TA0009: Collection, T1056: Input Capture, T1056.001: Keylogging, T1113: Screen Capture, T1115: Clipboard Data, T1005: Data from Local System, TA0007: Discovery, T1082: System Information Discovery, TA0011: Command and Control, T1102: Web Service, T1102.002: Bidirectional Communication, T1573: Encrypted Channel, T1573.002: Asymmetric Cryptography, T1001: Data Obfuscation, T1071: Application Layer Protocol, T1071.001: Web Protocols, TA0010: Exfiltration T1567: Exfiltration Over Web Service, T1567.002: Exfiltration to Cloud Storage

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Hive0163</td><td>-</td><td rowspan="2">Corporate Enterprises</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Financial gains</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>Slopoly, NodeSnake, Interlock ransomware, InterlockRAT</td><td>Windows, Linux</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0002: Execution, T1204: User Execution, T1204.004: Malicious Copy and Paste, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.003: Windows Command Shell, T1059.007: JavaScript, TA0003: Persistence, T1053: Scheduled Task/Job, T1053.005: Scheduled Task, T1574: Hijack Execution Flow, T1574.001: DLL, TA0007: Discovery, T1016: System Network Configuration Discovery, T1082: System Information Discovery, T1046: Network Service Discovery, TA0011: Command and Control, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1572: Protocol Tunneling, T1090: Proxy, T1090.001: Internal Proxy, T1102: Web Service, TA0010: Exfiltration, T1567: Exfiltration Over Web Service, TA0040: Impact, T1486: Data Encrypted for Impact, T1489: Service Stop</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploitable vulnerabilities** and block the indicators related to the threat actors **Mustang Panda, Void Manticore, APT28, Hive0163,** and malware **A0Backdoor, LOTUSLITE, BiBi Wiper, Cl Wiper, No-Justice Wiper, SlimAgent, BeardShell, Covenant, VENON, Slopoly, NodeSnake, Interlock, InterlockRAT.**

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 **four exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Mustang Panda, APT28,** and malware **A0Backdoor, SlimAgent, BEARDSHELL, and VENON RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

Microsoft Teams Social Engineering Delivers A0Backdoor Malware

Fake Strike Reports, Real Malware: The LOTUSLITE Delivery Chain

Void Manticore: Iran's Evolving Cyber Warfare Model

Microsoft's March 2026 Patch Tuesday

APT28 Deploys Modified Covenant to Spy on Ukrainian Government

PhantomRaven: Multi-Wave npm Campaign Stealing CI/CD and Developer Credentials

VENON Trojan Targets 33 Brazilian Financial Platforms

AI-Assisted Slopoly Backdoor Powers Interlock Ransomware Intrusion

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
A0Backdoor	Domain	fsdgh[.]com
	SHA256	26db06a2319c09918225e59c404448d92fe31262834d70090e941093e6bb650a
LOTUSLITE	MD5	10fb1122079b5ae8e4147253a937f40f
	SHA1	7d4e31c8b11be7c970860c4fbc8fe85c70724cb1
	SHA256	856476340706411772621 1ff8f89555e5a3b2b70bc9667032abd69cbe53b5216
BiBi Wiper	SHA256	74d8d60e900f931526a911b7157511377c0a298af986d42d373f51aac4f362f6
Cl Wiper	SHA256	e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0
No-Justice Wiper	SHA256	36cc72c55f572fe02836f25516d18fed1de768e7f29af7bdf469b52a3fe2531f
SlimAgent	SHA1	5603e99151f8803c13d48d83b8a64d071542f01b
	SHA256	9faeb1c8a4b9827f025a63c086d87c409a369825428634b2b01314460a332c6c
BeardShell	SHA1	6d39f49aa11ce0574d581f10db0f9bae423ce3d5
	SHA256	2eabe990f91bfc480c09db02a4de43116b40da2d6eaad00a034adf4214dac4d1

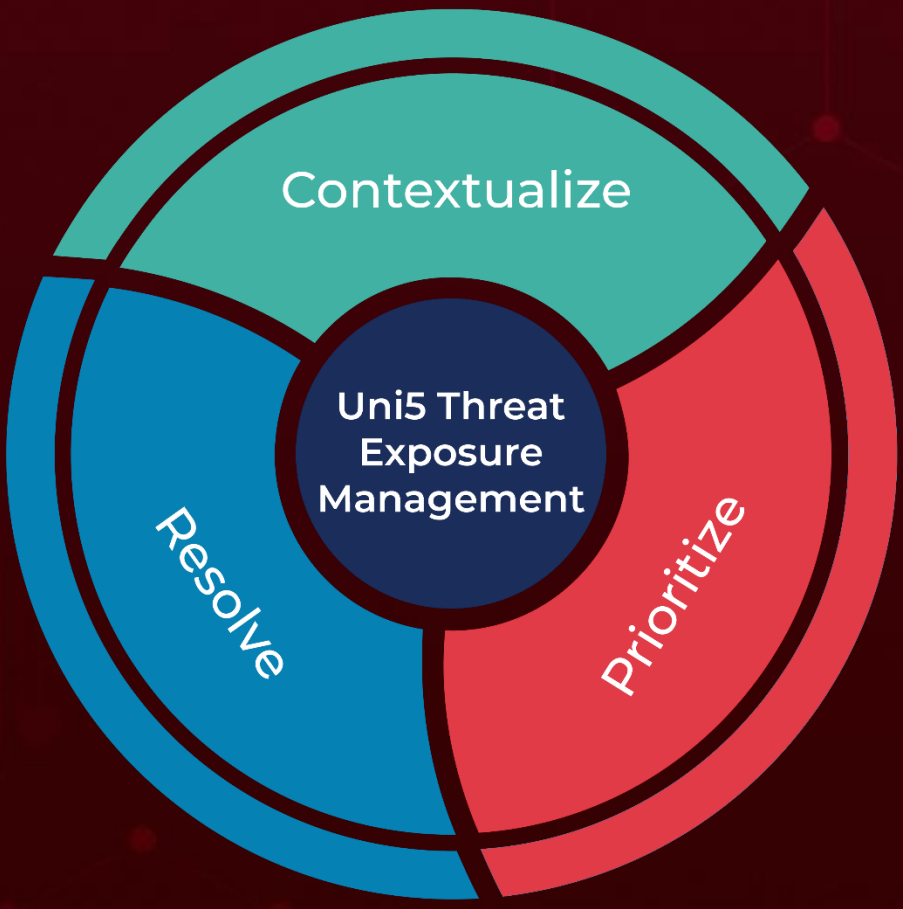
Attack Name	TYPE	VALUE
Covenant	SHA256	27a331384cfca9a4d2aa45afdc12c7156cfb4da775f1380d4870f06fbb77ccf2, 62d3b82ac3688b1c00adce7cd241de2a50c24caac4ed6b8e46b16da1266457eb, 1b2b83d462493eb63d6655103cf968d396ee7bdf7dd317f8cb5a5eadee6b560f
VENON	IPv4	206[.]0[.]29[.]58, 51[.]222[.]75[.]250, 51[.]222[.]75[.]248, 192[.]99[.]226[.]117, 212[.]69[.]5[.]84, 34[.]227[.]229[.]85
	SHA256	c482286a7fdfb64d308c197a4deabcd773b8b62d9e74d1d08fcfd02568d75d72, d61be2b21e135726c547a388ecb47552559e5221894f5005ce35bdb24efc0c26
Slopoly	SHA256	0884e5590bdf3763f8529453fbd24ee46a3a460bba4c2da5b0141f5ec6a35675
	Domain	plurfestivalgalaxy[.]com
	IPv4	94[.]156[.]181[.]89

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 16, 2026 • 11:00 PM

More at www.hivepro.com