

Date of Publication  
March 10, 2025



HiveForce Labs

WEEKLY

# THREAT DIGEST

**Attacks, Vulnerabilities and Actors**

03 to 09 MARCH 2025

# Table Of Contents

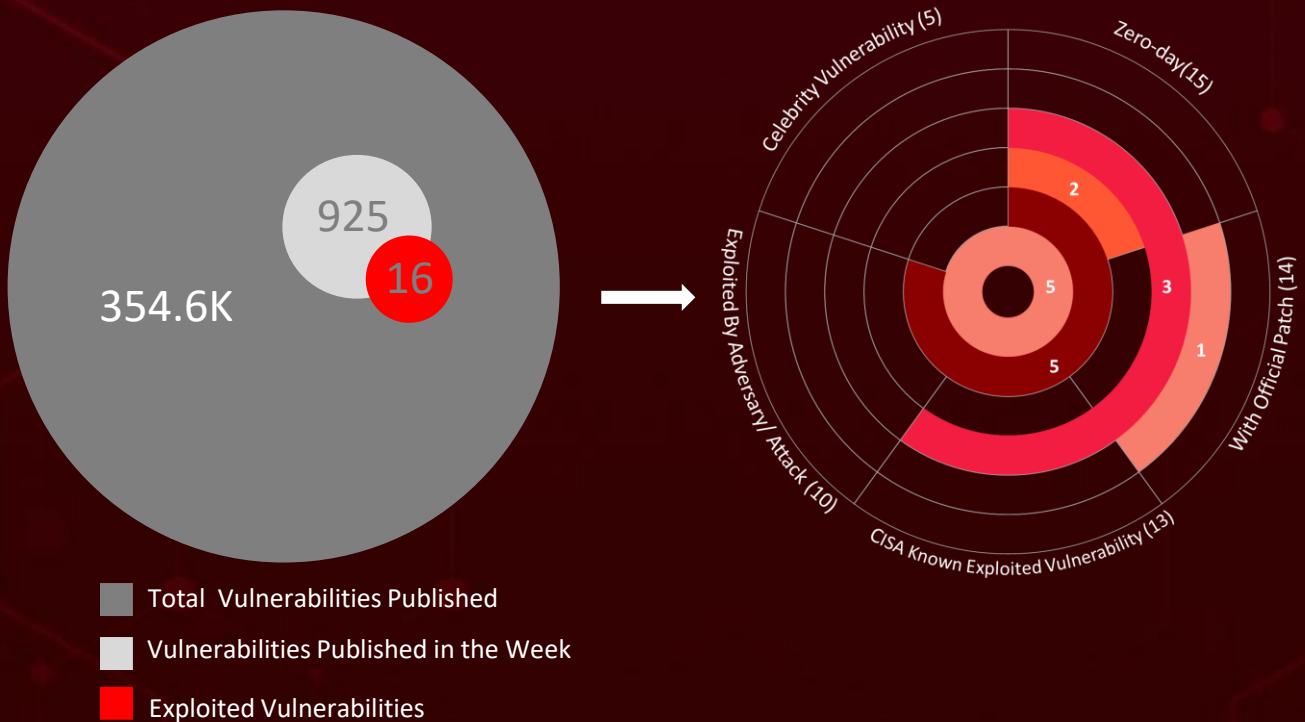
<a href="#"><u>Summary</u></a>	03
<a href="#"><u>High Level Statistics</u></a>	04
<a href="#"><u>Insights</u></a>	05
<a href="#"><u>Targeted Countries</u></a>	06
<a href="#"><u>Targeted Industries</u></a>	07
<a href="#"><u>Top MITRE ATT&amp;CK TTPs</u></a>	07
<a href="#"><u>Attacks Executed</u></a>	08
<a href="#"><u>Vulnerabilities Exploited</u></a>	11
<a href="#"><u>Adversaries in Action</u></a>	22
<a href="#"><u>Recommendations</u></a>	25
<a href="#"><u>Threat Advisories</u></a>	26
<a href="#"><u>Appendix</u></a>	27
<a href="#"><u>What Next?</u></a>	29

# Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, detected **four** attacks, reported **sixteen** vulnerabilities, and identified **three** active adversaries. These findings underscore the relentless and escalating danger of cyber intrusions.

Additionally, the newly identified **CVE-2025-27218** in Sitecore XM/XP allows remote code execution via insecure deserialization. **VMware** has patched three zero-day flaws (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226) that let attackers escape VM sandboxes, risking host system compromise.

Furthermore, this week, **Silk Typhoon** leverages unpatched vulnerabilities in IT tools to steal credentials, infiltrate networks, and escalate privileges. These rising threats pose significant and immediate dangers to users worldwide.



# High Level Statistics

4

Attacks  
Executed

16

Vulnerabilities  
Exploited

3

Adversaries in  
Action

- [Havoc Demon](#)
- [KaynLdr](#)
- [Sosano](#)
- [Poco RAT](#)

- [CVE-2025-22224](#)
- [CVE-2025-22225](#)
- [CVE-2025-22226](#)
- [CVE-2025-0364](#)
- [CVE-2024-54761](#)
- [CVE-2025-0282](#)
- [CVE-2024-12356](#)
- [CVE-2024-12686](#)
- [CVE-2024-3400](#)
- [CVE-2023-3519](#)
- [CVE-2021-26855](#)
- [CVE-2021-26857](#)
- [CVE-2021-26858](#)
- [CVE-2021-27065](#)
- [CVE-2021-44228](#)
- [CVE-2025-27218](#)

- [UNK CraftyCamel](#)
- [Silk Typhoon](#)
- [Dark Caracal](#)



# Insights

A **ClickFix phishing campaign** uses PowerShell to deploy Havoc via SharePoint, enabling stealthy remote control.

**UNK\_CraftyCamel** targets UAE aviation and satellite firms with the Sosano backdoor, leveraging a compromised Indian company.

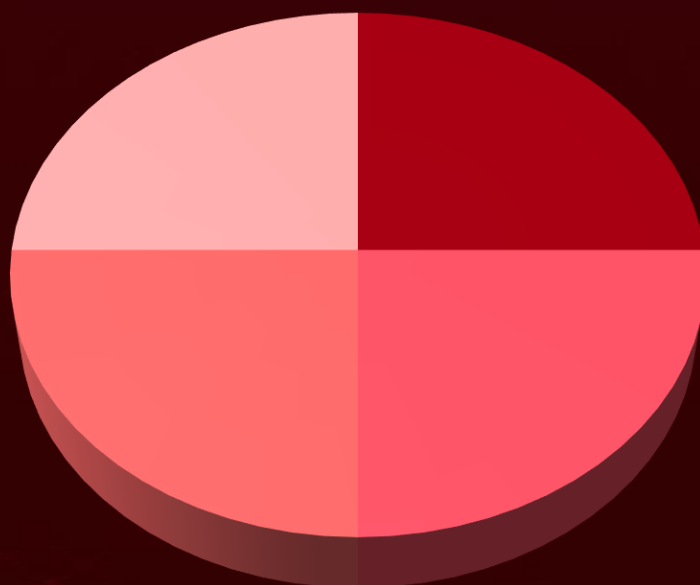
**Critical BigAnt Server flaws**, CVE-2025-0364 and CVE-2024-54761, allow admin creation and code execution; no patch exists, urging immediate mitigation.

**VMware patches three zero-day flaws** (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226) that let attackers escape the VM sandbox and compromise the host.

**Silk Typhoon** exploits IT tools and unpatched flaws to steal credentials, escalate privileges, and exfiltrate data across cloud and on-prem networks.

**Dark Caracal** deploys **Poco RAT** in phishing attacks targeting Spanish-speaking corporate networks, enabling full system control and data exfiltration.

## Threat Distribution



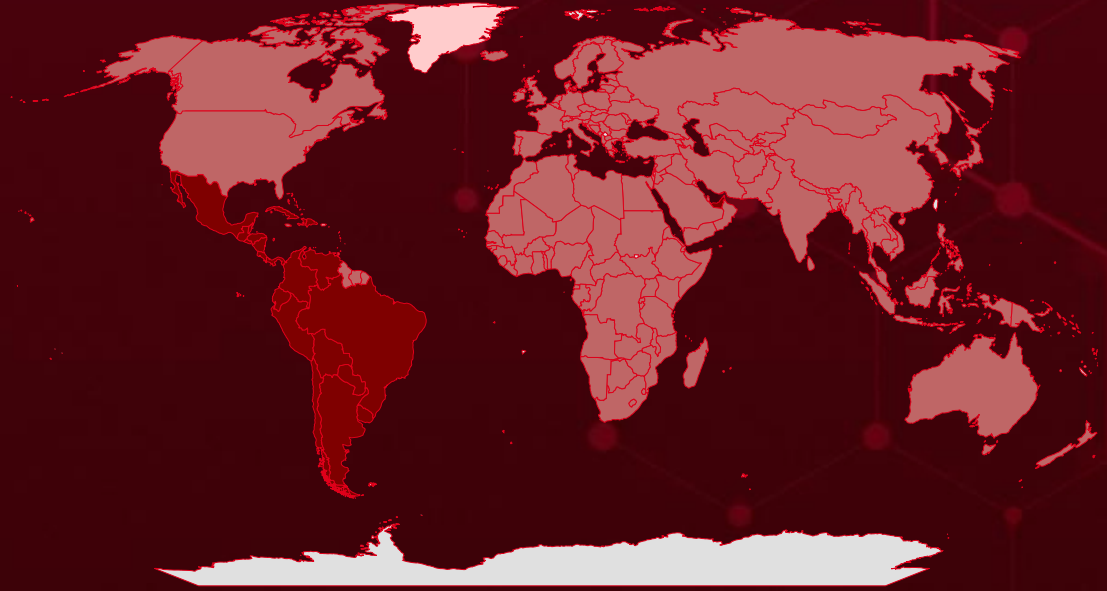
■ Backdoor   ■ Hack tool   ■ Loader   ■ RAT



# Targeted Countries

Most

Least

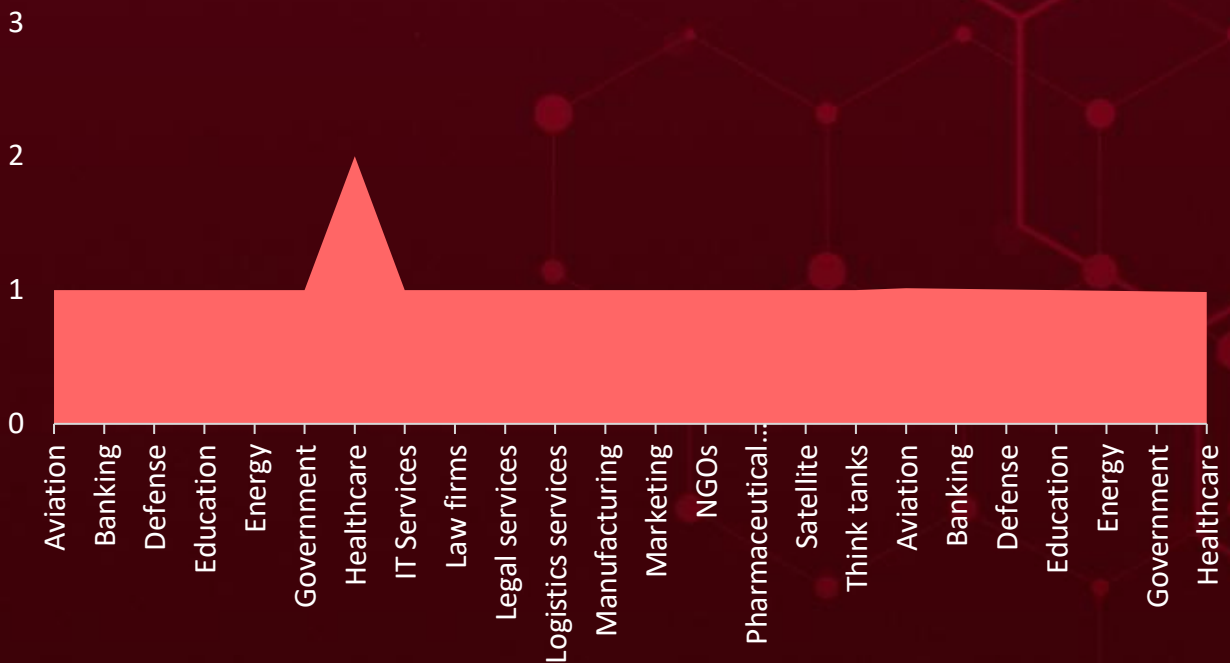


Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

Countries	Countries	Countries	Countries
Mexico	Angola	Turkey	Nigeria
El Salvador	Palau	Bhutan	Dominica
Peru	Brunei	China	Oman
Argentina	Sri Lanka	Rwanda	Austria
Haiti	Bulgaria	Albania	Papua New Guinea
Belize	Mauritania	Serbia	DR Congo
Panama	Burkina Faso	Comoros	Poland
Bolivia	Belgium	South Africa	Azerbaijan
Uruguay	Burundi	Congo	Romania
Brazil	Qatar	Suriname	Egypt
Guatemala	Cabo Verde	Armenia	Saint Lucia
Chile	Slovakia	Togo	Bahamas
Honduras	Cambodia	Côte d'Ivoire	Saudi Arabia
Colombia	Tajikistan	Ukraine	Equatorial Guinea
Nicaragua	Cameroon	Croatia	Sierra Leone
Costa Rica	Bosnia and Herzegovina	Malta	Eritrea
Paraguay	Canada	Australia	Solomon Islands
Cuba	Moldova	Belarus	Estonia
United Arab Emirates	Central African Republic	Cyprus	South Sudan
Dominican Republic	Nauru	Mongolia	Eswatini
Ecuador	Chad	Czech Republic	State of Palestine
Venezuela	North Macedonia	Myanmar	Ethiopia
San Marino	Antigua and Barbuda	Denmark	Switzerland
Morocco		Netherlands	Fiji
		Djibouti	Thailand
			Finland

# Targeted Industries



## TOP MITRE ATT&CK TTPs

### T1059

Command and Scripting Interpreter

### T1190

Exploit Public-Facing Application

### T1566

Phishing

### T1588.005

Exploits

### T1588

Obtain Capabilities

### T1588.006

Vulnerabilities

### T1204

User Execution

### T1105

Ingress Tool Transfer

### T1068

Exploitation for Privilege Escalation

### T1036

Masquerading

### T1195

Supply Chain Compromise

### T1140

Deobfuscate/Decode Files or Information

### T1204.001

Malicious Link

### T1204.002

Malicious File

### T1041

Exfiltration Over C2 Channel

### T1203

Exploitation for Client Execution

### T1027

Obfuscated Files or Information

### T1566.001

Spearpishing Attachment

### T1133

External Remote Services

### T1547

Boot or Logon Autostart Execution



# Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<a href="#"><u>Havoc Demon</u></a>	<p>The Havoc Demon is part of the Havoc C2 framework, a sophisticated post-exploitation tool used by threat actors to control infected systems. It is delivered via a ZIP archive containing a malicious screen saver and a decoy document. The malware employs advanced evasion techniques like sleep obfuscation and indirect syscalls to bypass security measures. Recent campaigns have used Havoc Demon in phishing attacks, leveraging platforms like SharePoint and Microsoft Graph API for stealthy operations</p>	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>  Remote Access, System Compromise	<b>AFFECTED PRODUCTS</b>
Hack tool			Windows
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
-		-	
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	cc151456cf7df7ff43113e5f82c4ce89434ab40e68cd6fb362e4ae4f70ce65b3		

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
<u>KaynLdr</u>	KaynLdr is a shellcode loader that loads malware like Havoc Demon DLL, using a modified DJB2 hashing algorithm to evade detection. It executes the DLL's entry point, initiating malicious activities.	Phishing	-
		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
<b>TYPE</b>		Windows	
Loader		<b>PATCH LINK</b>	
<b>ASSOCIATED ACTOR</b>		-	
-		-	
<b>IOC TYPE</b>	<b>VALUE</b>		
SHA256	A5210aaa9eb51e866d9c2ef17f55c0526732each1a412b910394b6b51246b7da		





NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Sosano</u>	Sosano is a sophisticated Golang-based backdoor malware used in highly targeted phishing campaigns, particularly against UAE's aviation and satellite sectors. It employs advanced obfuscation techniques, including unnecessary libraries to complicate analysis, and establishes communication with a command-and-control server to execute commands.	Phishing	-
<b>TYPE</b>		<b>IMPACT</b>	<b>AFFECTED PRODUCTS</b>
Backdoor		Data theft and Espionage	-
<b>ASSOCIATED ACTOR</b>			<b>PATCH LINK</b>
UNK_CraftyCame			-
<b>IOC TYPE</b>		<b>VALUE</b>	
SHA256	0ad1251be48e25b7bc6f61b408e42838bf5336c1a68b0d60786b8610b82bd94c		





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
<u>Poco RAT</u>	Poco RAT is a sophisticated Remote Access Trojan (RAT) attributed to the Dark Caracal threat group, designed to provide attackers with full control over infected systems. It is delivered via phishing campaigns targeting Spanish-speaking users, often using PDF attachments or links to cloud-hosted malicious archives.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			PATCH LINK
ASSOCIATED ACTOR			-
Dark Caracal			-
IOC TYPE		VALUE	
SHA256	05bf7db7debfeb56702ef1b421a336d8431c3f7334187d2ccd6ba34816a3fd5a, 08552f588eafceb0fa3117c99a0059fd06882a36cc162a01575926736d4a80eb, 0d6822c93cb78ad0d2ad34ba9057a6c9de8784f55caa6a8d8af77fed00f0da0a, 0fe11d78990590652f4d0f3afba5670e030b8ab714db9083fd0a981e0f1f48f3, 0ffc7ae741bb90c7f8e442d89b985def9969ebf293442f751ab2e69f4df226a8		




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
<a href="#"><u>CVE-2025-0364</u></a>		BigAnt Server 5.6.06 and below	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:bigantsoft:bigant_server:*.:*:*:*:*:*	-
BigAntSoft BigAnt Server Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1068 : Exploitation for Privilege, T1190: Exploit Public-Facing Application	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-54761</u></a>		BigAnt Server 5.6.06 and below	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:bigantsoft:bigant_server:*.:*:*:*:*:*	-
BigAntSoft BigAnt Office Messenger SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-22224</u>		VMware ESXi Versions 7.0 and 8.0, VMware Cloud Foundation Version 4.5.x and 5.x, VMware Telco Cloud Platform Version 5.x, 4.x, 3.x, and 2.x, VMware Telco Cloud Infrastructure Version 3.x and 2.x, VMware Workstation Version 17.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:vmware:esxi:- :*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* :*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:* :* cpe:2.3:a:vmware:workstation:*:*:*:*:*:*	-
VMware ESXi and Workstation TOCTOU Race Condition Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-367	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	<a href="https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390">https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-22225</u>		VMware ESXi Versions 7.0 and 8.0, VMware Cloud Foundation Version 4.5.x and 5.x, VMware Telco Cloud Platform Version 5.x, 4.x, 3.x, and 2.x, VMware Telco Cloud Infrastructure Version 3.x and 2.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
VMware ESXi Arbitrary Write Vulnerability		cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-123	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	<a href="https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390">https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<b><u>CVE-2025-22226</u></b>		VMware ESXi Versions 7.0 and 8.0, VMware Cloud Foundation Version 4.5.x and 5.x, VMware Telco Cloud Platform Version 5.x, 4.x, 3.x, and 2.x, VMware Telco Cloud Infrastructure Version 3.x and 2.x, VMware Workstation Version 17.x, VMware Fusion Version 13.x	-
	<b>ZERO-DAY</b>		
		<b>AFFECTED CPE</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>
<b>NAME</b>	<b>CISA KEY</b>	cpe:2.3:o:vmware:esxi:-:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:* cpe:2.3:a:vmware:workstation:*:*:*:*:*:* cpe:2.3:a:vmware:fusion:*:*:*:*:*:*	-
VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability			
	<b>CWE ID</b>	<b>ASSOCIATED TTPs</b>	<b>PATCH LINK</b>
	CWE-125	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	<a href="https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390">https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-0282</u>		Ivanti Connect Secure: 22.7R2 through 22.7R2.4 Ivanti Policy Secure: 22.7R1 through 22.7R1.2 Ivanti Neurons for ZTA gateways: 22.7R2 through 22.7R2.3	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*	-
Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1059: Command and Scripting Interpreter; T1210: Exploitation of Remote Services	<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283</a>







CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-12356</a>		BeyondTrust Privileged Remote Access (PRA) Versions 24.3.1 and earlier, BeyondTrust Remote Support (RS) Versions 24.3.1 and earlier	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*	
BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability		cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation, T1133 : External Remote Services	<a href="https://www.beyondtrust.com/trust-center/security-advisories/bt24-10">https://www.beyondtrust.com/trust-center/security-advisories/bt24-10</a>



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-12686</a>		BeyondTrust Privileged Remote Access (PRA) Versions 24.3.1 and earlier, BeyondTrust Remote Support (RS) Versions 24.3.1 and earlier	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*	
BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability		cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation, T1133 : External Remote Services	<a href="https://www.beyondtrust.com/trust-center/security-advisories/bt24-11">https://www.beyondtrust.com/trust-center/security-advisories/bt24-11</a>



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u><b>CVE-2024-3400</b></u>		Palo Alto PAN-OS: 10.2 < 10.2.9-h1 Palo Alto PAN-OS: 11.0 < 11.0.4-h1 Palo Alto PAN-OS: 11.1 < 11.1.2-h3 11.1.2-h2	Silk Typhoon
	<b>ZERO-DAY</b>		
		<b>AFFECTED CPE</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>
<b>NAME</b>	<b>CISA KEY</b>	cpe:2.3:a:paloaltonetworks:pan-os:*:*:*:*:*	-
Palo Alto Networks PAN-OS Command Injection Vulnerability			
	<b>CWE ID</b>	<b>ASSOCIATED TTPs</b>	<b>PATCH LINK</b>
	<b>CWE-77</b>	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	<a href="https://security.paloaltonetworks.com/CVE-2024-3400">https://security.paloaltonetworks.com/CVE-2024-3400</a>



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u><a href="#">CVE-2023-3519</a></u>		NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13; NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13; NetScaler ADC and NetScaler Gateway version 12.1, now end of life; NetScaler ADC 13.1-FIPS before 13.1-37.159; NetScaler ADC 12.1-FIPS before 12.1-55.297; NetScaler ADC 12.1-NDcPP before 12.1-55.297	Silk Typhoon
	<b>ZERO-DAY</b>		
		<b>AFFECTED CPE</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>
<b>NAME</b>	<b>CISA KEY</b>	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability			
	<b>CWE ID</b>	<b>ASSOCIATED TTPs</b>	<b>PATCH LINK</b>
	CWE-94	T1190 : Exploit Public-Facing Application, T1059 : Command and Scripting Interpreter	<a href="https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467">https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2021-26855</u></a>	ProxyLogon	Microsoft Exchange Server	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*	-
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application; T1078: Valid Accounts	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2021-26857</u></a>	ProxyLogon	Microsoft Exchange Server	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	-
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26857</a>


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2021-26858</a>	ProxyLogon	Microsoft Exchange Server	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	-
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1505.003: Web Shell	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2021-27065</a>	ProxyLogon	Microsoft Exchange Server	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	-
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1505.003: Web Shell	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-44228</u>	Log4shell	Apache Log4j2	Silk Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
Apache Log4j2 Remote Code Execution Vulnerability		cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-917	T1059: Command and Scripting Interpreter	<a href="https://logging.apache.org/log4j/2.x/security.html">https://logging.apache.org/log4j/2.x/security.html</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-27218</u>		Sitecore Experience Manager (XM) and Experience Platform (XP) prior to 10.4 versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV		
Sitecore XM and XP Deserialization Vulnerability		cpe:2.3:a:sitecore:experience_manager:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190 : Exploit Public-Facing Application, T1203: Exploitation for Client Execution	<a href="https://support.sitecore.com/kb?id=kb_article_view&amp;sysparm_article=KB1003535">https://support.sitecore.com/kb?id=kb_article_view&amp;sysparm_article=KB1003535</a>


# Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <b>UNK_CraftyCamel</b>	-	Aviation and Satellite	United Arab Emirates
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACK S/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
-	Sosano	-	

## TTPs


TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0005: Defense Evasion, TA0007: Discovery, TA0011: Command and Control, T1566: Phishing, T1566.001: Spearphishing Attachment, T1036: Masquerading, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.006: Python, T1027: Obfuscated Files or Information, T1140: Deobfuscate/Decode Files or Information, T1083: File and Directory Discovery, T1070: Indicator Removal, T1586: Compromise Accounts, T1586.002: Email Accounts, T1222: File and Directory Permissions Modification, T1218: System Binary Proxy Execution, T1218.005: Mshta, T1071: Application Layer Protocol



NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Silk Typhoon (aka Hafnium, Red Dev 13, timmy, ATK233, G0125, Operation Exchange Marauder)</u></p>	China	IT Services, Healthcare, Legal services, Higher education, Defense, Government, Non-governmental organizations (NGOs), Energy, Law firms, and Policy think tanks	Worldwide
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
	CVE-2025-0282 CVE-2024-12356 CVE-2024-12686 CVE-2024-3400 CVE-2023-3519 CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065 CVE-2021-44228	-	Windows

**TTPs**

TA0042: Resource Development, TA0006: Credential Access, TA0001: Initial Access, TA0008: Lateral Movement, TA0002: Execution, TA0005: Defense Evasion, TA0003: Persistence, TA0010: Exfiltration, T1078: Valid Accounts, T1027: Obfuscated Files or Information, T1505.003: Web Shell, T1574.010: Services File Permissions Weakness, TA0004: Privilege Escalation, TA0040: Impact, T1190: Exploit Public-Facing Application, T1555: Credentials from Password Stores, T1505, TA0009: Collection, T1110.003: Password Spraying, T1586, TA0007: Discovery, TA0010: Exfiltration, TA0011: Command and Control, T1110: Brute Force, T1068: Compromise Accounts, T1083: File and Directory Discovery, T1106: Server Software Component, T1598: Native API, T1574: Phishing for Information Hijack Execution Flow, T1195.002: Compromise Software Supply Chain, T1195: Supply Chain Compromise, T1567.002: Exfiltration to Cloud Storage: Exploitation for Privilege Escalation, T1041: Exfiltration Over C2 Channel, T1059: Command and Scripting Interpreter, T1584: Compromise Infrastructure, T1584.003: Virtual Private Server

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Dark Caracal (aka ATK 27, TAG-CT3, G0070)</u>	Lebanon	Banking, Manufacturing and distribution, Healthcare and Pharmaceutical services, Logistics services, Marketplaces	Latin America
	<b>MOTIVE</b>		
	Information theft and espionage		
	<b>TARGETED CVEs</b>	<b>ASSOCIATED ATTACKS/RANSOMWARE</b>	<b>AFFECTED PRODUCTS</b>
-	Poco RAT	-	

### TTPs

TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, T1608: Stage Capabilities, T1608.001: Upload Malware, T1583: Acquire Infrastructure, T1583.003: Virtual Private Server, T1588: Obtain Capabilities, T1588.001: Malware, T1566: Phishing, T1566.001: Spearphishing Attachment, T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter, T1059.003: Windows Command Shell, T1055: Process Injection, T1027: Obfuscated Files or Information, T1027.013: Encrypted/Encoded File, T1027.002: Software Packing, T1113: Screen Capture, T1082: System Information Discovery, T1132: Data Encoding, T1132.001: Standard Encoding, T1571: Non-Standard Port, T1665: Hide Infrastructure, T1036: Masquerading

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **sixteen exploited vulnerabilities** and block the indicators related to the threat actors **UNK\_CraftyCamel, Silk Typhoon, Dark Caracal**, and malware **Havoc Demon, KaynLdr, Sosano, Poco RAT**.

## 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 **sixteen exploited vulnerabilities**.

Testing the efficacy of their security controls by simulating the attacks related to the threat actors **UNK\_CraftyCamel, Silk Typhoon, Dark Caracal**, and malware **Havoc Demon, Sosano, Poco RAT** in Breach and Attack Simulation(BAS).

# Threat Advisories

[ClickFix Deception: Hackers Use SharePoint and Graph API to Deploy Havoc Malware](#)

[Unpatched Flaws Let Hackers Take Over BigAnt Server](#)

[VMware Fixes Three Actively Exploited Zero-Days - Patch Now!](#)

[UNK CraftyCamel: A New Cyber Threat Lurking in the Satellite Sector](#)

[Silk Typhoon's Strategic Pivot: Exploiting IT Supply Chains for Espionage](#)

[Poco RAT: Dark Caracal's Latest Cyber Espionage Weapon](#)

[Critical Insecure Deserialization Vulnerability in Sitecore XM/XP](#)

# 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
<a href="#"><u>Havoc Demon</u></a>	SHA256	cc151456cf7df7ff43113e5f82c4ce89434ab40e68cd6fb362e4ae4f70ce65b3
<a href="#"><u>KaynLdr</u></a>	SHA256	A5210aaa9eb51e866d9c2ef17f55c0526732eacb1a412b910394b6b51246b7da
<a href="#"><u>Sosano</u></a>	SHA256	0ad1251be48e25b7bc6f61b408e42838bf5336c1a68b0d60786b8610b82bd94c
<a href="#"><u>Poco RAT</u></a>	MD5	a5073df86767ece0483da0316d66c15c, 2a0f523b9e52890105ec6fbccd207dcd, e0bf0aee954fd97457b28c9233253b0a, ec8746a1412d1bd1013dfe51de4b9fd1, fea98ca977d35828e294b7b9cc55fea9, c41645cba3de5c25276650a2013cd32b, 8778b9430947c46f68043666a71a2214, d8ec2df77a01064244f376322ba5aaf1, bbfbd1ece4f4aa43d0c68a32d92b17e5, 32c6c0d29593810f69d7c52047e49373
	SHA1	d0661df945e8e36aa78472d4b60e181769a3f23b, f3a495225dc34cdeba579fb0152e4ccb2e0ad42, ce611811d9200613c1a1083e683faec5187a9280, f719b736ed6b3351d1846127afec8e0c68e54c1d, 63b4d283eaf367122ce0dec9fc0e586e63ef0c78, d8021edcb42b6472dded45f7a028aff6dfe5aaa6, da3ea31e96fba64fcd840e930a99e705eb60c89b, ce60069d5fdef4acced66e6fc049f351c465ee1e, 2ffdf164f6b8e2e403a86bd4d0f6260bf17fb154, 4bf76e731d655f67c9e78a616cf8b21002a53406

Attack Name	TYPE	VALUE
<u>Poco RAT</u>	SHA256	05bf7db7debfeb56702ef1b421a336d8431c3f7334187d2ccd6ba34816a3fd5a, 08552f588eafceb0fa3117c99a0059fd06882a36cc162a01575926736d4a80eb, 0d6822c93cb78ad0d2ad34ba9057a6c9de8784f55caa6a8d8af77fed00f0da0a, 0fe11d78990590652f4d0f3afba5670e030b8ab714db9083fd0a981e0f1f48f3, 0ffc7ae741bb90c7f8e442d89b985def9969ebf293442f751ab2e69f4df226a8, 121d941ba5a6ff8d99558e0919f49b926fbc00e3007aad14ac85e799d55473c, 12e849ffba407d5db756879fd257c4b736eb4b6adac6320d2f1916d6a923fa46, 13306775fdf506b706693deccb44ec364fe04dbf3c471227c2439c2462e19080, 1786f16a50a4255df8aa32f2e21f2829b4f8aaba2ced3e4a7670846205b3ac70, 18ba3612b1f0dbd23f8ab39b2d096bab0ed3438b37932f473c787e24e57e8397

# 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, 2025 • 9:45 PM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)