

Date of Publication  
March 3, 2025



HiveForce Labs  
WEEKLY  
**THREAT DIGEST**

**Attacks, Vulnerabilities and Actors**

24 FEBRUARY to 02 MARCH 2025

# Table Of Contents

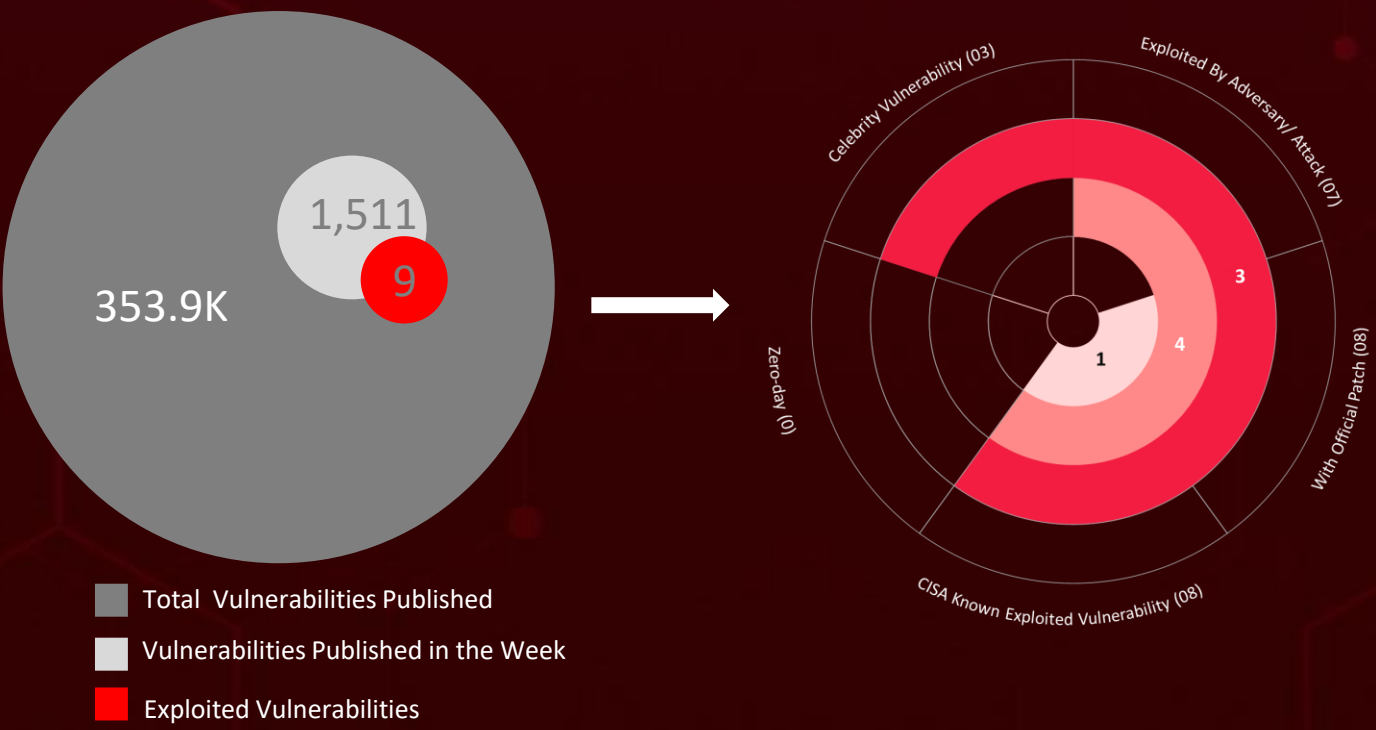
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&amp;CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	17
<u>Recommendations</u>	18
<u>Threat Advisories</u>	19
<u>Appendix</u>	20
<u>What Next?</u>	23

# Summary

HiveForce Labs has identified a surge in cyber threats, with **six** attacks executed, **nine** vulnerabilities uncovered in the past week highlighting the relentless nature of cyberattacks.

HiveForce Labs has uncovered a critical vulnerability in Microsoft Power Pages (**CVE-2025-24989**) that is already being actively exploited. This flaw, caused by improper access controls, allows attackers to escalate privileges remotely and bypass user registration restrictions. With hackers taking advantage of this weakness, organizations using Power Pages must apply the patch immediately to prevent unauthorized access and potential system compromise.

Meanwhile, cybercriminals continue to evolve their tactics. **Ghost ransomware**, first spotted in early 2021, has infiltrated organizations in over 70 countries by exploiting unpatched vulnerabilities. Believed to be operated by China-based threat actors, Ghost employs payload rotation, detection evasion, and high-profile exploits like ProxyShell to maximize damage. Adding to the growing threat landscape, a newly discovered Linux backdoor, **Auto-Color**. This stealthy malware provides attackers with persistent remote access, making it exceptionally difficult to detect and remove. As cyber threats grow more sophisticated, organizations must prioritize proactive security, continuous monitoring, and timely patching to stay ahead.



# High Level Statistics

6

Attacks  
Executed

9

Vulnerabilities  
Exploited

0

Adversaires in  
Action

- Ghost
- FatalRAT
- Auto-color
- AsyncRAT
- Quasar RAT
- Winos4.0
- CVE-2025-24989
- CVE-2018-13379
- CVE-2010-2861
- CVE-2009-3960
- CVE-2021-34473
- CVE-2021-34523
- CVE-2021-31207
- CVE-2019-0604
- CVE-2024-34331



# Insights

A stealthy campaign is hitting APAC, using **FatalRAT** for persistent access. Attackers exploit Chinese cloud services like myqcloud and Youdao Cloud Notes to blend in and evade detection.

**Auto-color**, a stealthy new Linux malware, grants attackers' full remote control while resisting deletion.

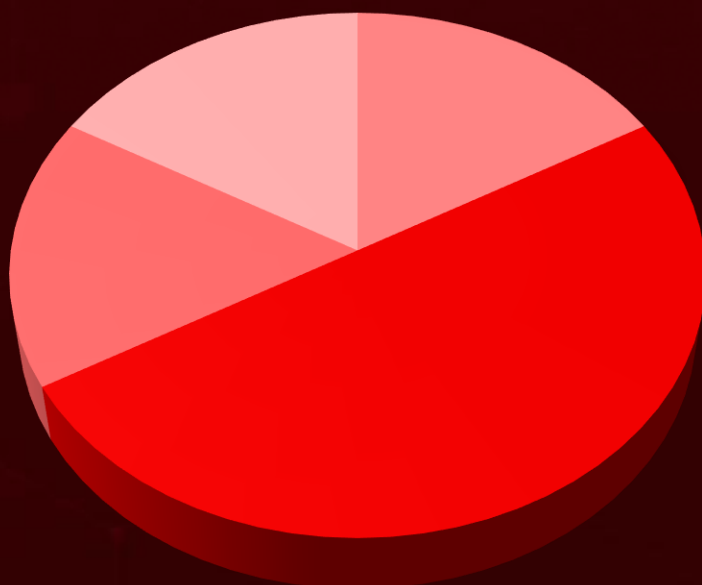
**CVE-2025-24989** flaw in Power Pages is under active exploitation, letting attackers bypass registration restrictions and escalate privileges remotely—patch immediately.

**Ghost Ransomware** surges globally, breaching critical infrastructure in 70+ countries by exploiting unpatched flaws.

**GitVenom** exploits fake GitHub repos to infect developers and crypto users, deploying Node.js Stealer, AsyncRAT, and clipboard hijackers to steal credentials and funds. With attackers amassing nearly 5 BTC in a month, vigilance is key—verify repos and inspect code before use.

**CVE-2024-34331** in Parallels Desktop lets attackers gain root on macOS via flawed installer signature checks. Despite patches, bypasses exist—making all versions vulnerable.

## Threat Distribution



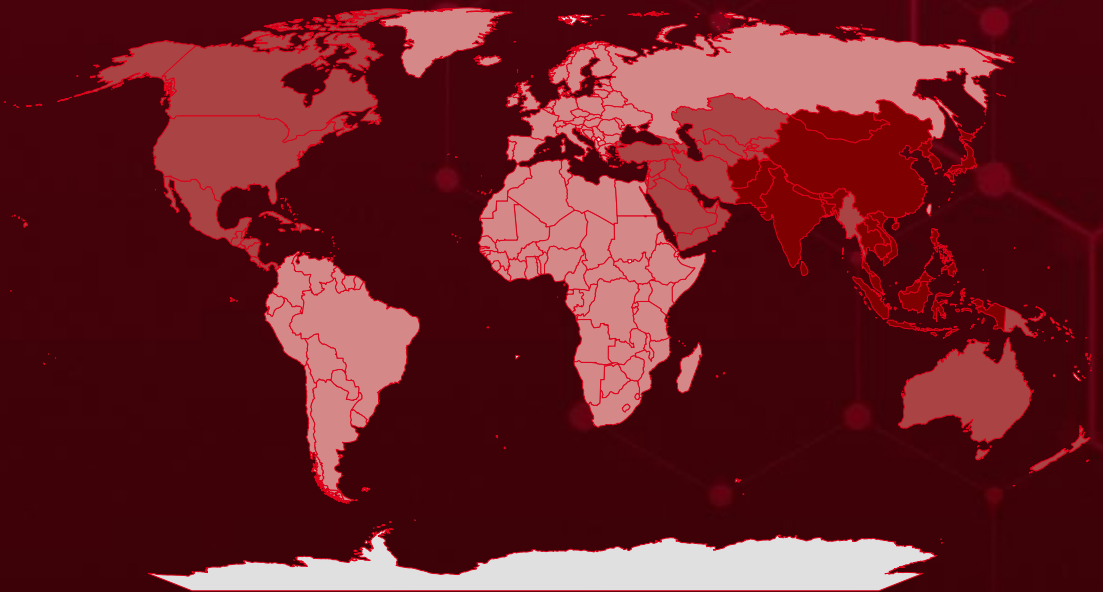
■ Ransomware ■ RAT ■ Backdoor ■ Malware Framework



# Targeted Countries

Most

Least



Powered by Bing

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

Countries
North Korea
Malaysia
South Korea
Bangladesh
Mongolia
Bhutan
Philippines
Brunei
Thailand
Cambodia
Maldives
China
Nepal
India
Pakistan
Indonesia
Singapore
Japan
Sri Lanka
Vietnam
Timor-Leste
Afghanistan

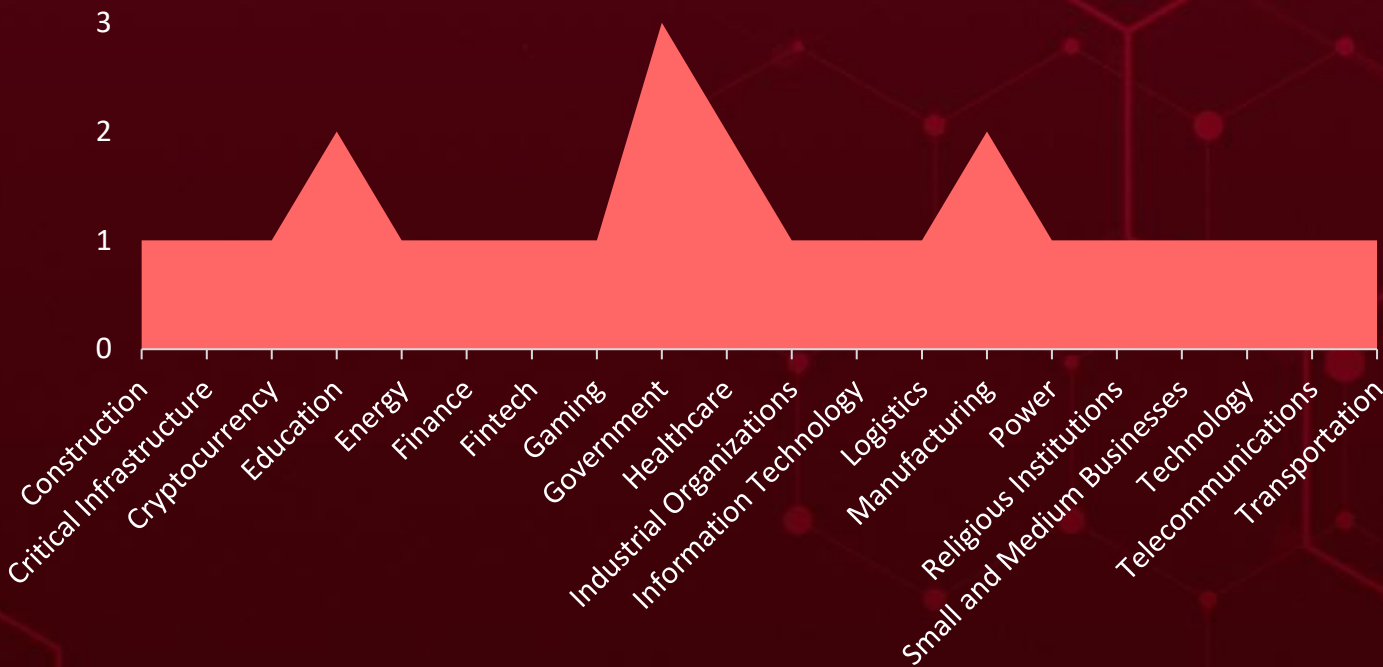
Countries
Laos
Cuba
Georgia
Dominica
Guatemala
Uzbekistan
Haiti
Cyprus
Honduras
State of Palestine
Bahrain
Turkmenistan
Antigua and Barbuda
Costa Rica
Iran
Panama
Iraq
Saint Lucia
Israel
Dominican Republic
Jamaica
Tajikistan

Countries
Barbados
Trinidad and Tobago
Jordan
United Arab Emirates
Kazakhstan
Nicaragua
Kiribati
Oman
Kuwait
Palau
Kyrgyzstan
Papua New Guinea
Vanuatu
Qatar
Lebanon
Saudi Arabia
Belize
Solomon Islands
Armenia
El Salvador
Australia
Syria

Countries
Azerbaijan
Fiji
Marshall Islands
Tonga
Mexico
Turkey
Canada
Tuvalu
Myanmar
United States
Bahamas
Grenada
New Zealand
Yemen
Russia
Albania
Somalia
Cameroon
Cabo Verde
Ireland
Senegal
Algeria



# Targeted Industries



# TOP MITRE ATT&CK TTPs

## T1059

Command and Scripting Interpreter

## T1068

Exploitation for Privilege Escalation

## T1036

Masquerading

## T1140

Deobfuscate/Decode Files or Information

## T1027

Obfuscated Files or Information

## T1057

Process Discovery

## T1190

Exploit Public-Facing Application

## T1056

Input Capture

## T1083

File and Directory Discovery

## T1548.002

Bypass User Account Control

## T1204.002

Malicious File

## T1566

Phishing

## T1056.00

1  
Keylogging

## T1547

Boot or Logon Autostart Execution

## T1071

Application Layer Protocol

## T1562

Impair Defenses

## T1071.001

Web Protocols

## T1059.003

Windows Command Shell

## T1082

System Information Discovery

## T1497

Virtualization/Sandbox Evasion

# ✂ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Ghost Ransomware</u>	<p>Ghost ransomware surfaced in early 2021, rapidly gaining attention for targeting exposed internet services by exploiting known security vulnerabilities. The group behind it, suspected to be based in China, frequently modified their ransomware payloads, changed file extensions for encrypted files, altered ransom note texts, and used various email addresses to avoid identification.</p>	Exploiting Vulnerabilities in internet-facing services	CVE-2018-13379 CVE-2010-2861 CVE-2009-3960 CVE-2021-34473 CVE-2021-34523 CVE-2021-31207 CVE-2019-0604
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Financial Losses, Operational Disruption, Reputational Damage	Fortinet FortiOS, Adobe ColdFusion 9.0.1 and earlier, Adobe BlazeDS 3.2 and earlier, Microsoft Exchange Server, Microsoft SharePoint
ASSOCIATED ACTOR			PATCH LINK
-			<a href="https://www.fortiguard.com/p/sirt/FG-IR-18-384">https://www.fortiguard.com/p/sirt/FG-IR-18-384</a> , <a href="https://helpx.adobe.com/coldfusion/kb/coldfusion-security-hot-fix-bulletin.html">https://helpx.adobe.com/coldfusion-security-hot-fix-bulletin.html</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34523">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34523</a> , <a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207</a> , <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0604">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0604</a> , <a href="https://helpx.adobe.com/security/security-bulletin.html">https://helpx.adobe.com/security/security-bulletin.html</a>
IOC TYPE	VALUE		
MD5	c5d712f82d5d37bb284acd4468ab3533, 34b3009590ec2d361f07cac320671410, d9c019182d88290e5489cdf3b607f982		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<a href="#">FatalRAT</a>	FatalRAT, a remote access Trojan (RAT), enables persistent access for attackers. They exploit legitimate Chinese cloud services, such as myqcloud CDN and Youdao Cloud Notes, to conceal their infrastructure and avoid detection. Through a multi-stage payload delivery, they silently deploy malware, bypassing security defenses. FatalRAT provides attackers with full control over compromised systems, allowing keystroke logging, data theft, and remote command execution.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Persistent Access, Data Theft, Bypassing Security Defenses	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
MD5	2477e031f776539c8118b8e0e6663b0, 02d8c59e5e8a85a81ee75ce517609739		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<a href="#">Auto-color</a>	A new Linux malware strain, Auto-color, is named after the filename it adopts upon installation. Auto-color provides attackers with complete remote control over compromised systems. The malware integrates seamlessly into the system, resisting deletion. If the user lacks root privileges, it halts installation to avoid detection. However, when executed with elevated privileges, it installs a malicious library that mimics a legitimate system library to remain undetected.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Remote Control, Persistent Presence	Linux
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d4c43, 65a84f6a9b4ccddcdade812ab8783938e3f4c12cfba670131b1a80395710c6fb4		

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>AsyncRAT</u>	AsyncRAT is a remote access tool (RAT) that allows users to monitor and control computers from a distance using an encrypted connection. It comes with features like keylogging, remote desktop access, and other functions that can compromise a victim's system.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
IPv4	138[.]68[.]81[.]155		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Quasar RAT</u>	Quasar RAT is a .NET-based malware family employed by various threat actors. Fully functional and open-source, it is frequently packed to complicate source code analysis.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Remote Control and Surveillance, System Disruption	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
-			

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>Winos 4.0</u>	Winos4.0 malware steals sensitive data, which can be used for subsequent attacks. A secondary attack chain has been discovered, deploying an online module capable of capturing screenshots from WeChat and online banking platforms.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data Theft, Compromise of Sensitive Platforms	Microsoft Windows
Malware framework			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	f519802d1abc6f364b519e6c9a108edfb688d42d438167c1524387cfbdf066ef, 8b1b9a789136ca3abe25938204845c351aaf0c97c0708ade8d4d8ba4ded95ba7		




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
<u>CVE-2025-24989</u>		Microsoft Power Pages	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:microsoft:power_pages:*:*:*:*:*:*	-
Microsoft Power Pages Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24989">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24989</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2018-13379</u>		Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 and FortiProxy 2.0.0, 1.2.0 to 1.2.8, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 under SSL VPN web portal	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*	Ghost Ransomware
Fortinet FortiOS SSL VPN Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application; T1083: File and Directory Discovery	<a href="https://www.fortiguard.com/psirt/FG-IR-20-233">https://www.fortiguard.com/psirt/FG-IR-20-233</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2010-2861</u>		Adobe ColdFusion 9.0.1 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:coldfusion:*:*:*:*:*:*	Ghost Ransomware
Adobe ColdFusion Directory Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application; T1083: File and Directory Discovery	<a href="https://helpx.adobe.com/security/security-bulletin.html">https://helpx.adobe.com/security/security-bulletin.html</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2009-3960</u>		Adobe BlazeDS 3.2 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:blazeds:*:*:*:*:*:*	Ghost Ransomware
Adobe BlazeDS Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1190: Exploit Public-Facing Application; T1005: Data from Local System	<a href="https://helpx.adobe.com/security/security-bulletin.html">https://helpx.adobe.com/security/security-bulletin.html</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-34473</u>		Microsoft Exchange Server	-
	ZERO-DAY		
			
	CISA KEV		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	Ghost Ransomware
PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-34523</u>		Microsoft Exchange Server	-
	ZERO-DAY		
			
	CISA KEV		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	Ghost Ransomware
PROXYSHELL (Microsoft Exchange Server Privilege Escalation Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34523">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34523</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-31207</u>		Microsoft Exchange Server	-
	ZERO-DAY		
			
	CISA KEV		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME		cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*	Ghost Ransomware
PROXYSHELL (Microsoft Exchange Server Security Feature Bypass Vulnerability)	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-434	T1190: Exploit Public-Facing Application; T1556: Modify Authentication Process	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-31207</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2019-0604</u>		Microsoft SharePoint	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*	Ghost Ransomware
Microsoft SharePoint Remote Code Execution Vulnerability		ASSOCIATED TTPs	PATCH LINK
	CWE ID		
	CWE-20	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	<a href="https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0604">https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0604</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-34331</u>		Parallels Desktop: All versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:parallels:desktop:19.0:*:*:*:*:*:*	-
Parallels Desktop Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	MITIGATION LINK
	CWE-269	T1068: Exploitation for Privilege Escalation; T1553: Subvert Trust Controls; T1059: Command and Scripting Interpreter	<a href="https://www.parallels.com/products/desktop/download/">https://www.parallels.com/products/desktop/download/</a> <a href="https://kb.parallels.com/129860">https://kb.parallels.com/129860</a>

# Adversaries in Action

No Active Adversaries tracked this week.

# Recommendations

## Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the malware **Ghost, FatalRAT, Auto-color, AsyncRAT, Quasar RAT, Winos4.0**.

## 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 **nine exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the malware **Ghost, FatalRAT** and **Winos4.0** in Breach and Attack Simulation(BAS).

# Threat Advisories

[Microsoft Fixes Power Pages Critical Flaw Exploited in Active Attacks](#)

[Ghost Ransomware's Brutal Reminder: Patching Isn't Optional](#)

[FatalRAT Malware Targets APAC Industries via Chinese Cloud Services](#)

[Patch Bypassed! Parallels Desktop Vulnerability Still Open to Attack](#)

[Auto-Color: The Stealthy Linux Malware Lurking in the Shadows](#)

[GitVenom Campaign Exploits GitHub to Target Crypto Users](#)

[Winos4.0: Stealthy Malware Campaign Targets Taiwanese Enterprises](#)

# 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
<u>Ghost</u>	MD5	c5d712f82d5d37bb284acd4468ab3533, 34b3009590ec2d361f07cac320671410, d9c019182d88290e5489cdf3b607f982, 29e44e8994197bdb0c2be6fc5dfc15c2, c9e35b5c1dc8856da25965b385a26ec4, d1c5e7b8e937625891707f8b4b594314, ef6a213f59f3fbee2894bd6734bbaed2, ac58a214ce7deb3a578c10b97f93d9c3, c3b8f6d102393b4542e9f951c9435255, 0a5c4ad3ec240fbfd00bdc1d36bd54eb, ff52fdf84448277b1bc121f592f753c5, a2fd181f57548c215ac6891d000ec6b9, 625bd7275e1892eac50a22f8b4a6355d, db38ef2e3d4d8cb785df48f458b35090
	SHA256	f7d270ca0f2b4d21830787431f881cd004b2eb102cc3048c6b4d69cb775511c8, c8acd8e65b46c86d0d01e961358bc6ab9aec70f90a57829aa15e39add536b5c8
<u>FatalIRAT</u>	MD5	2477e031f776539c8118b8e0e6663b0, 02d8c59e5e8a85a81ee75ce517609739, 05c528a2b8bb20aad901c733d146d595, 15962f79997a308ab3072c10e573e97c, 17278c3f4e8bf56d9c1054f67f19b82c, 172ee543d8a083177fc1832257f6d57d, 1fe3885dea6be2e1572d8c61e3910d19, 249f568f8b8709591e7afd934ebea299, 266bb19f9ceb1a4ccbf45577bbeaac1a,

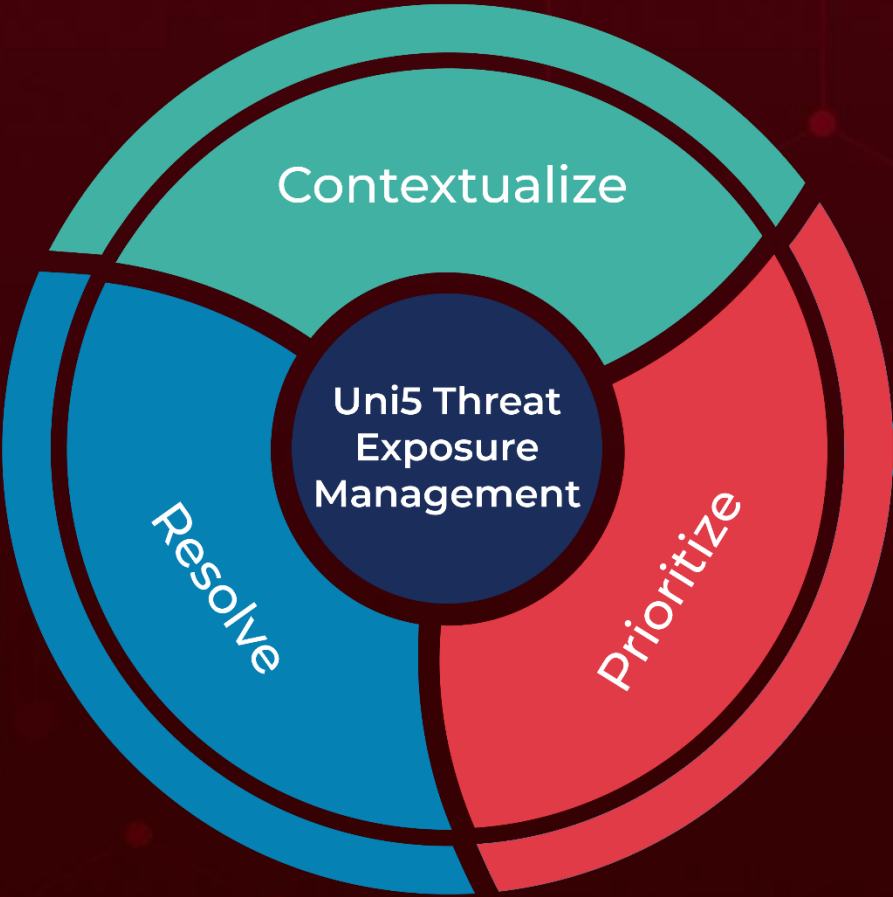
Attack Name	TYPE	VALUE
<u>FatalRAT</u>	MD5	3c583e01eddd0ea6fe59a89aea4503b4, 3ec20285d88906336bd4119a74d977a0, 43156787489e6aa3a853346cded3e67b, 46630065be23c229adff5e0ae5ca1f48, 577e1a301e91440b920f24e7f6603d45, 5be46b50cac057500ea3424be69bf73a, 60a92d76e96aaa0ec79b5081ddcc8a24, 60dbc3ef17a50ea7726bdb94e96a1614, 635f3617050e4c442f2cbd7f147c4dcf, 675a113cdbcce171e1ff172834b5f740, 68a27f7ccbfa7d3b958fad078d37e299, 73e49ddf4251924c66e3445a06250b10, 787f2819d905d3fe684460143e01825c, 7ac3ebac032c4afd09e18709d19358ed, 8f67a7220d36d5c233fc70d6ecf1ee33, 9b4d46177f24ca0a4881f0c7c83f5ef8, 9c3f469a5b54fb2ec29ac7831780ed6d, 9d34d83e4671aaf23ff3e61cb9daa115, a935ef1151d45c7860bfe799424bea4b, bcec6b78adb3cf966fab9025dacb0f05, d0d3efcff97ef59fe269c6ed5ebb06c9, ebc0809580940e384207aa1704e5cc8e, eca08239da3acaf0d389886a9b91612a, ed6837f0e351aff09db3c8ee93fbcf06, fb8dc76a0cb0a5d32e787a1bb21f92d2, feb49021233524bd64eb6ce37359c425
	SHA256	013a681ff8c09b5fab6218f4aa493627652c9ec7c6ba88291980b6e00e1 51201, 20a418e0de5890e79c9a628eebe1208244f5d90d12cf8124f4424c8720 299ce
<u>Auto-color</u>	SHA256	270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d 4c43, 65a84f6a9b4ccddcdade812ab8783938e3f4c12cfba670131b1a80395710 c6fb4, 83d50fcf97b0c1ec3de25b11684ca8db6f159c212f7ff50c92083ec5fbd3a 633, a1b09720edcab4d396a53ec568fe6f4ab2851ad00c954255bf1a0c04a9d 53d0a, bace40f886aac1bab03bf26f2f463ac418616bacc956ed97045b7c3072f0 2d6b, e1c86a578e8d0b272e2df2d6dd9033c842c7ab5b09cda72c588e0410dc 3048f7, 85a77f08fd66aeabc887cb7d4eb8362259afa9c3699a70e3b81efac9042b b255, bf503b5eb456f74187a17bb8c08bccc9b3d91a7f0f6fd50110540b05151 0d1ca

Attack Name	TYPE	VALUE
<u>AsyncRAT</u>	IPv4	138[.]68[.]81[.]155
<u>Winos4.0</u>	SHA256	f519802d1abc6f364b519e6c9a108edfb688d42d438167c1524387cfbdf066ef, 8b1b9a789136ca3abe25938204845c351aaf0c97c0708ade8d4d8ba4ded95ba7

# 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 03, 2025 • 4:30 AM**

© 2025 All Rights are Reserved by Hive Pro



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