

Date of Publication
June 18, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

10 to 16 JUNE 2024

Table Of Contents

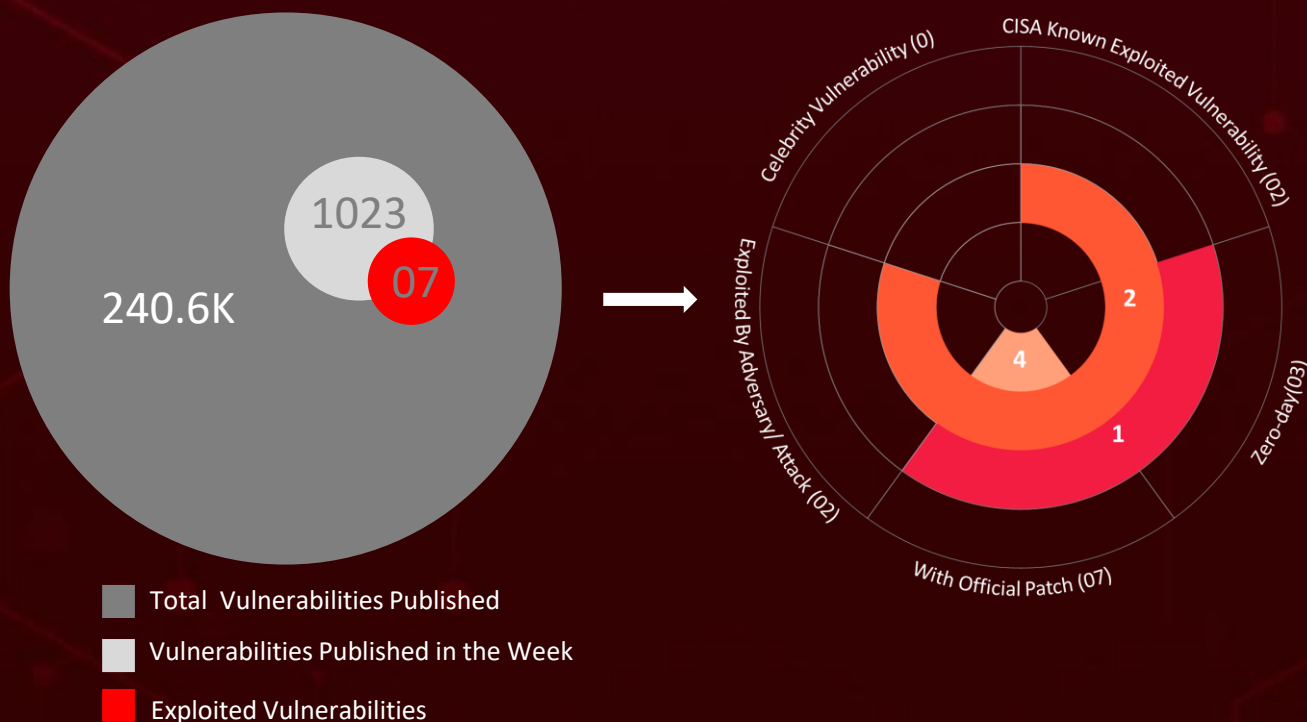
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	15
<u>Recommendations</u>	16
<u>Threat Advisories</u>	17
<u>Appendix</u>	18
<u>What Next?</u>	21

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week alone, HiveForce Labs has detected **five** executed attacks, reported **seven** vulnerabilities, and identified **one** active adversary. These findings highlight the relentless and escalating danger of cyber intrusions.

Additionally, a new Windows malware '**WARMCOOKIE**' disseminated in the "REF6127" email campaign targeting job seekers, functioning as a backdoor to explore networks, deploy additional payloads, and capture screenshots.

Furthermore, the Cardinal Threat Group, associated with **Black Basta ransomware**, is believed to have exploited Windows **CVE-2024-26169** as a zero-day, granting attackers the highest-level system access. These rising threats pose significant and immediate danger to users worldwide.



High Level Statistics

5

Attacks
Executed

- [Fog Ransomware](#)
- [ValleyRAT](#)
- [WARMCOOKIE](#)
- [TellYouThePass](#)
- [Black Basta](#)

7

Vulnerabilities
Exploited

- [CVE-2024-27348](#)
- [CVE-2024-29849](#)
- [CVE-2024-4577](#)
- [CVE-2023-50868](#)
- [CVE-2024-4610](#)
- [CVE-2024-26169](#)
- [CVE-2024-29855](#)

1

Adversaries in
Action

- [Cardinal Threat Group](#)



Insights

Microsoft's June 2024

Patch Tuesday
Addresses 49
Vulnerabilities

Fog Ransomware

targeting educational organizations and the recreation sector in the US

ValleyRAT

China-linked RAT that enables unauthorized remote access to compromised systems

ARM's 0-day CVE-2024-4610

impacting Bifrost and Valhall GPU kernel drivers, allows improper GPU memory processing, potentially granting access to freed memory

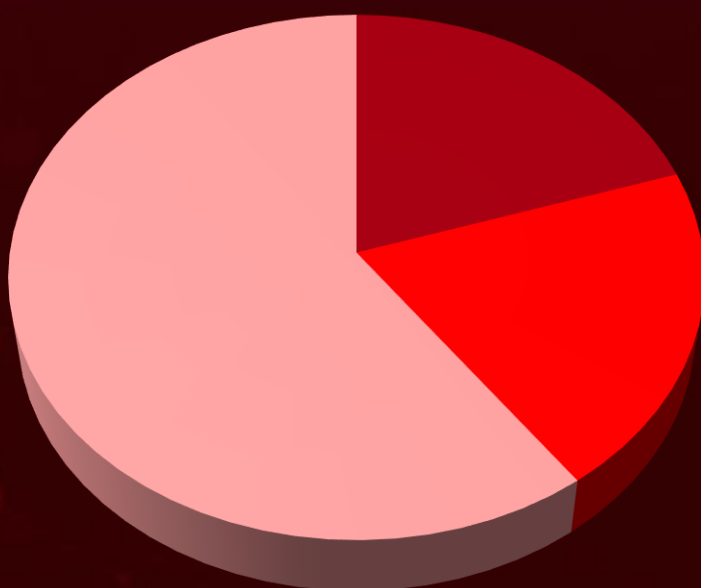
TellYouThePass ransomware gang

is actively exploiting this **CVE-2024-4577** PHP vulnerability, leading to arbitrary code execution on affected servers and potentially compromising entire systems

Black Basta ransomware

believed to have exploited a Windows **CVE-2024-26169** vulnerability as a 0-day

Threat Distribution



■ Backdoor

■ Remote Access Trojan

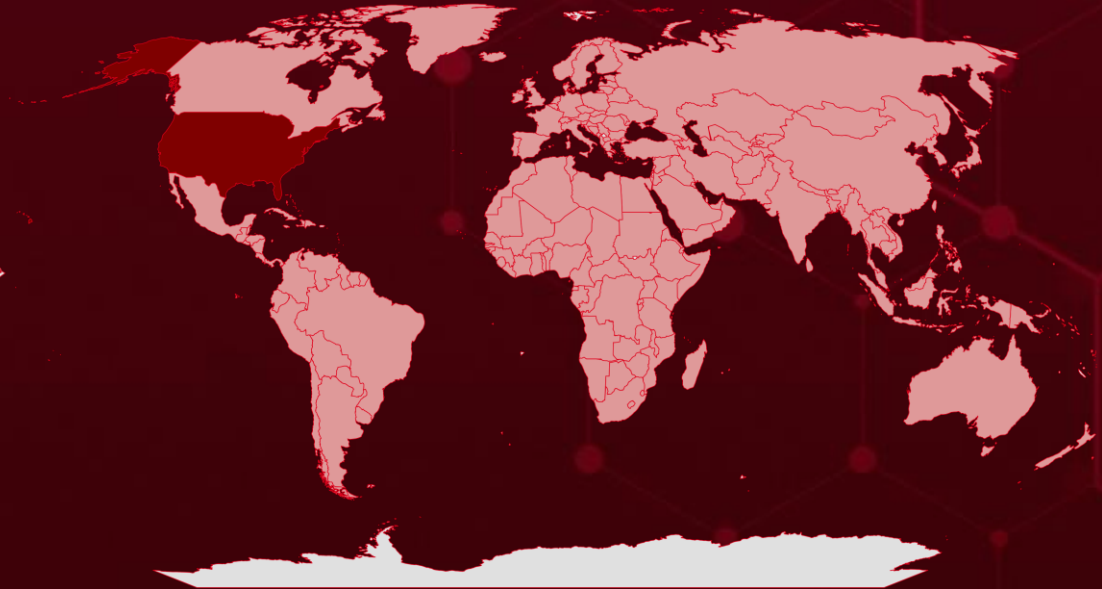
■ Ransomware



Targeted Countries

Most

Least



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Countries	Countries	Countries	Countries
United States	Morocco	Mexico	Côte d'Ivoire
Netherlands	Barbados	Burundi	Sudan
Canada	Nicaragua	Mongolia	Croatia
South Korea	Belarus	Cabo Verde	Syria
Algeria	Palau	Myanmar	Cuba
Moldova	Belgium	Cambodia	Timor-Leste
Andorra	Qatar	North Macedonia	Cyprus
Saint Kitts & Nevis	Belize	Cameroon	Tunisia
Angola	Sao Tome & Principe	Nigeria	Czech Republic (Czechia)
Tonga	Benin	Zambia	Uganda
Antigua and Barbuda	Slovenia	Oman	Denmark
Maldives	Bhutan	Central African Republic	Uruguay
Argentina	St. Vincent & Grenadines	Papua New Guinea	Djibouti
Nauru	Bolivia	Chad	Vietnam
Armenia	Tanzania	Poland	Dominica
Peru	Bosnia and Herzegovina	Chile	Afghanistan
Australia	Turkmenistan	Russia	Dominican Republic
Seychelles	Botswana	China	Lithuania
Austria	Vanuatu	Samoa	DR Congo
Sweden	Brazil	Colombia	Madagascar
Azerbaijan	Liechtenstein	Senegal	Ecuador
United Arab Emirates	Brunei	Comoros	Malaysia
Bahamas	Malawi	Singapore	Egypt
Luxembourg	Bulgaria	Congo	Mali
Bahrain	Malta	Somalia	El Salvador
	Burkina Faso	Costa Rica	Marshall Islands
		Spain	Equatorial Guinea

Targeted Industries



TOP MITRE ATT&CK TTPs

T1190

Exploit Public-Facing Application

T1588

Obtain Capabilities

T1059

Command and Scripting Interpreter

T1588.006

Vulnerabilities

T1055

Process Injection

T1588.005

Exploits

T1027

Obfuscated Files or Information

T1498

Network Denial of Service

T1105

Ingress Tool Transfer

T1068

Exploitation for Privilege Escalation

T1486

Data Encrypted for Impact

T1036

Masquerading

T1082

System Information Discovery

T1204.002

Malicious File

T1566

Phishing

T1547

Boot or Logon Autostart Execution

T1070

Indicator Removal

T1587.001

Malware

T1204

User Execution

T1057

Process Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Fog Ransomware	Fog ransomware, a new threat discovered in May 2024, has been targeting educational and recreational institutions in the United States. This ransomware attacks virtual environments within organizations, potentially causing significant disruption.	Exploiting compromised VPN credentials	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data Theft, Data encryption, Financial loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA1	7c8c60172f9ae4dab9f61c28ccae7084da90a06, 507b26054319ff31f275ba44ddc9d2b5037bd295, e1fb7d15408988df39a80b8939972f7843f0e785, 83f00af43df650fda2c5b4a04a7b31790a8ad4cf, 44a76b9546427627a8d88a650c1bed3f1cc0278c		

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 CVEs
<u>ValleyRAT</u>	ValleyRAT, discovered in 2023 and linked to a China-based threat actor, is a Remote Access Trojan (RAT). This sophisticated malware employs a multi-stage infection process to execute various malicious activities.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR		Infiltrate and compromise systems	-
-			PATCH LINK
-	-		
IOC TYPE	VALUE		
SHA256	46ea0173f8f8ee07575c1ab440f7b06c9519cfc85c9094cde05497c0adeb73c5, a5c7dd4e3b2113a51c5c031a3e5f37a0783e41d983ccdc9dbfd6735018a39338, a5d96982f492aeaa3461f397c58f5ea90be6b6087550dd01a0b43c76dd675f2b, a245d1f716919f561df98c5df164652ee76e6201cc6d12287a07b98f821b5aef, d404c0f796c73159e5cd95b976cb79134b27e567917ce0026965074a8c79c154		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>WARMCOOKIE</u>	WARMCOOKIE functions as an initial backdoor tool, used to explore victim networks and deploy further malicious payloads. Each instance is compiled with a hard-coded C2 IP address and an RC4 key.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Steal information, install other malware,	-
-			PATCH LINK
-	-		
IOC TYPE	VALUE		
SHA1	ccde1ded028948f5cd3277d2d4af6b22fa33f53abde84ea2aa01f1872fad1d13		




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 CVEs
<u>TellYouThePass</u>	TellYouThePass is a ransomware threat that's been active since 2019. It encrypts files on a victim's computer and demands a ransom payment to restore them. It exploits vulnerabilities in software to gain access to systems. Recently, it's been seen targeting a new vulnerability (CVE-2024-4577) that impacts PHP.	Exploiting vulnerabilities	CVE-2024-4577
		IMPACT	AFFECTED PRODUCTS
		Data Theft, Data encryption, Financial loss	PHP
			PATCH LINK
			https://www.php.net/downloads
TYPE			
Ransomware			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
SHA256	d18453e564ca27514227478f225d85811fe15d08aa5fb1f613022c43155c5c54, 170d654b61810992fef6f18dbce5b4c7f5762cf36c9b41c36a14c9f6609f6e7d, f572898ab9f9a0fabac77d5d388680f84f85f9eb2c01b4e5de426430c6b5008f, 9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53, ea59d6a130a279dfde4df53640bd720419c7b5d9711a21a78af9453b1b3b5805		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Black Basta</u>	Black Basta is a ransomware-as-a-service (RaaS) group that emerged in early 2022. Cardinal Threat Group, known to be associated with Black Basta ransomware group, is believed to have exploited a Windows CVE-2024-26169 as zero-day.	Exploiting vulnerabilities	CVE-2024-26169
		IMPACT	AFFECTED PRODUCTS
		Data Theft, Data encryption, Financial loss	Microsoft Windows
			PATCH LINK
			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26169
TYPE			
Ransomware			
ASSOCIATED ACTOR			
Cardinal Threat Group			
IOC TYPE	VALUE		
SHA256	7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a, d9d2838327c081a6daf9528c77ff3a8ac88e8ff73521b97d34af0d3da5807e7c, a6fbbdf8efe0ea129636bb5b3d6d6faec298272a2afded7e7516f2491844abc7, e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757, df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415		




Vulnerabilities Exploited




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-27348		Apache HugeGraph-Server from version 1.0.0 to before 1.3.0 in Java8 & Java11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:apache:hugegraph-server:*:*:*:*:*	-
Apache HugeGraph-Server Remote Command Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1190 : Exploit Public-Facing Application	https://hugegraph.apache.org/docs/download/download/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29849		Veeam Backup Enterprise Manager versions before prior to 12.1.2.172	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*	-
Veeam Backup Enterprise Manager Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://www.veeam.com/kb4510

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-4577</u>		PHP versions: 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:php:php:*:*:*:*:*:*:*	TellYouThePass ransomware
PHP-CGI Argument Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.php.net/downloads


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-50868</u>		Windows Server: 2012 – 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
NSEC3 Closest Encloser Proof DoS Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-400	T1498 : Network Denial of Service	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-50868

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-4610</u>		Bifrost GPU Kernel Driver: All versions from r34p0 to r40p0	-
	ZERO-DAY	Valhall GPU Kernel Driver: All versions from r34p0 to r40p0	
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:arm:bifrost_gpu_kernel_driver:*:*:*:*:*:* cpe:2.3:a:arm:valhall_gpu_kernel_driver:*:*:*:*:*:*	-
Arm Mali GPU Kernel Driver Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter	https://developer.arm.com/downloads/-/mali-drivers/bifrost-kernel ; https://developer.arm.com/downloads/-/mali-drivers/valhall-kernel

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-26169</u>		Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	Cardinal Threat Group
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	Black Basta ransomware
Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability			
	CWE ID	ASSOCIATED TTPs	
	CWE-269	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26169

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-29855</u>		Veeam Recovery Orchestrator (VRO) version 7.0.0.337	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:recovery_orchestrator:*:*:*:*:*:* *	-
Veeam Recovery Orchestrator Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation, T1591 : Gather Victim Org Information	https://www.veeam.com/kb4585

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Cardinal Threat Group (aka Storm-1811, UNC4393)</u>	-	-	Worldwide
	MOTIVE Information Theft, Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-26169	Black Basta ransomware (aka no_name_software)	-
TTPs			
TA0002: Execution, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0003: Persistence, TA0040: Impact, TA0042: Resource Development, 1588.006: Vulnerabilities, T1588.005: Exploits, T1588: Obtain Capabilities, T1068: Exploitation for Privilege Escalation, T1486: Data Encrypted for Impact, T1036: Masquerading, T1059: Command and Scripting Interpreter			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seven exploited vulnerabilities** and block the indicators related to the threat actors **Cardinal Threat Group**, and malware **Fog Ransomware, ValleyRAT, WARMCOOKIE, TellYouThePass, Black Basta**.

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 **seven exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Cardinal Threat Group**, and malware **Fog Ransomware, ValleyRAT, WARMCOOKIE** in Breach and Attack Simulation(BAS).

Threat Advisories

[Fog Ransomware Targets US Sectors Via Compromised VPN Credentials](#)

[POC Exploit Code Released for Apache HugeGraph RCE Vulnerability](#)

[Veeam Addresses Critical Flaws, Urges Admins to Patch](#)

[New Face of ValleyRAT: Enhanced Commands and Infiltration Tactics](#)

[WARMCOOKIE Backdoor: Rising via Recruitment-Themed Phishing](#)

[PHP RCE Flaw Opens a Gateway for TellYouThePass Ransomware](#)

[Microsoft's June 2024 Patch Tuesday Addresses 49 Vulnerabilities](#)

[ARM's Zero-Day Flaw Leads to Improper GPU Memory Processing](#)

[Black Basta Ransomware Linked to Zero-Day Windows Exploit](#)

[Veeam Recovery Orchestrator Flaw Enables Forge of Valid JWT Tokens](#)

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>Fog Ransomware</u>	SHA1	f7c8c60172f9ae4dab9f61c28ccae7084da90a06, 507b26054319ff31f275ba44ddc9d2b5037bd295, e1fb7d15408988df39a80b8939972f7843f0e785, 83f00af43df650fda2c5b4a04a7b31790a8ad4cf, 44a76b9546427627a8d88a650c1bed3f1cc0278c
<u>ValleyRAT</u>	SHA256	46ea0173f8f8ee07575c1ab440f7b06c9519cfc85c9094cde05497c0 adeb73c5, a5c7dd4e3b2113a51c5c031a3e5f37a0783e41d983ccdc9dbfd6735 018a39338, a5d96982f492aeaa3461f397c58f5ea90be6b6087550dd01a0b43c7 6dd675f2b, a245d1f716919f561df98c5df164652ee76e6201cc6d12287a07b98f 821b5aef, d404c0f796c73159e5cd95b976cb79134b27e567917ce002696507 4a8c79c154, 8c4de69e89dcc659d2fff52d695764f1efd7e64e0a80983ce6d0cb9e eddb806c, 9763543f309b96bd89953245dec616a0777399f389f128e5334cf58 167bd12a9, 1ddd09c086a9626426885916af78201429528a20d1ef6bb133aec3 b25223b519, 880a51fc964a355cf8b4bcc985f315ffb1d4ac0394e8043706e9c9d1 87784564, c70e8867fe9a63a147588a53e26c6e68753157326c5e759742333a d6d5c5dcc2, c017974a8b52d728763d8c4ed2112809c76271eb9e3c1d64d7ab7e 8a60d29217, b8637cecec68d2275fa7ac89782467053d92621577e46c741a136a3 50a14fe99,

Attack Name	TYPE	VALUE
<u>ValleyRAT</u>	SHA256	b8ebcd9d2621972514d7499cf34ae0e27e825b322baba243d29139 eff70c0ba2, b10c10aa20f008273e0491ec0e6b74e0cddafb15e8b70366e11258b 960a93855, bb8158746f3a8ed8040ca7986c21e3de026e844142685c5c0b7992 2b527fe5d0, a4a6d4257ba42d31c48c812d75de7eeab54a986c31e666c448c74f4 4909a23c8, eac4ef2479304cbf26ca73886871af920f3a857b460352fbf1218fa0f 6a4d469, c6f6c537aa9cce0cfac002034691cad14aad7fbbd7aa3e56b48b83f 502879d8, 86412961d59001ddb6aac7044790324737401d6cd858d03c9baa36 20b26f7cd9, b4f1234da98edeb3876c3aaa01b867a54db91a24a4d90615ddf7a7 b53f959840
	MD5	c563f62191ea363259939a6b3ce7f192
<u>WARMCOKIE</u>	SHA256	ccde1ded028948f5cd3277d2d4af6b22fa33f53abde84ea2aa01f187 2fad1d13
<u>TellYouThePass</u>	SHA256	d18453e564ca27514227478f225d85811fe15d08aa5fb1f613022c4 3155c5c54, 170d654b61810992fef6f18dbce5b4c7f5762cf36c9b41c36a14c9f66 09f6e7d, f572898ab9f9a0fabac77d5d388680f84f85f9eb2c01b4e5de426430 c6b5008f, 9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b 1ec6d41c53, ea59d6a130a279dfde4df53640bd720419c7b5d9711a21a78af9453 b1b3b5805, aa0ef20f9f8ca111b0d8a550daf6651f5b0557f0acb0a26545755c5a 02263a9b
<u>Black Basta</u>	SHA256	7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645 770e1f0b8a, d9d2838327c081a6daf9528c77ff3a8ac88e8ff73521b97d34af0d3d a5807e7c, a6fbd8f8efe0ea129636bb5b3d6d6faec298272a2afded7e7516f249 1844abc7, e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f5 62577fd757, df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857 977a9fb415, d73f6e240766d,dd6c3c16eff8db50794ab8ab95c6a616d4ab2bc967 80f13464d, b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d44 7a96dd9,

Attack Name	TYPE	VALUE
<u>Black Basta</u>	SHA256	<p>69192821f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944</p> <p>62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087</p> <p>462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7</p> <p>5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43</p> <p>58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd</p> <p>51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e</p> <p>05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431</p> <p>3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35</p> <p>350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd</p> <p>0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e</p> <p>892bb04889678134fbdde62d573eef1274c328b4e216ea7dc17ed0065fe8be37</p> <p>58edd2a0980b15f7fc6c892011751a30c134757142a54c2cedcbba4af2cbf855</p> <p>723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224</p> <p>ca0273c55507c3aae95539812c2c5d9bbdc80deb8e714360fe4bcc65d257aeb0</p> <p>0c915ce6cd1676ecc99863f47ed28c6466a2532ce9df7bbd2ae810b7bbf026f7</p> <p>753a66f032d0d7a7c310a2e5f98c54e95e3d404400224d592657a02079c668d5</p> <p>96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be</p> <p>82515c1c5675d68c0f1f7d7572d83819944cc951747879caf1653cf41ce792ba</p> <p>9f948af3a30f125dcd24d8a628b3a18c66b3d72baede8496ee735cbdfd9cf0c7</p> <p>d943a4aabd76582218fd1a9a0a77b2f6a6715b198f9994f0feae6f249b40fdf9</p> <p>ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e</p> <p>7883f01096db9bcf090c2317749b6873036c27ba92451b212b8645770e1f0b8a</p>

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

June 18, 2024 • 4:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com