Date of Publication
October 15, 2024

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

7 to 13 October 2024

Table Of Contents

Summary 03

High Level Statistics 04

Insights 05

Targeted Countries 06

Targeted Industries 07

Top MITRE ATT&CK TTPs 07

Attacks Executed 08

Vulnerabilities Exploited 15

Adversaries in Action 21

Recommendations 24

Threat Advisories 25

Appendix 26

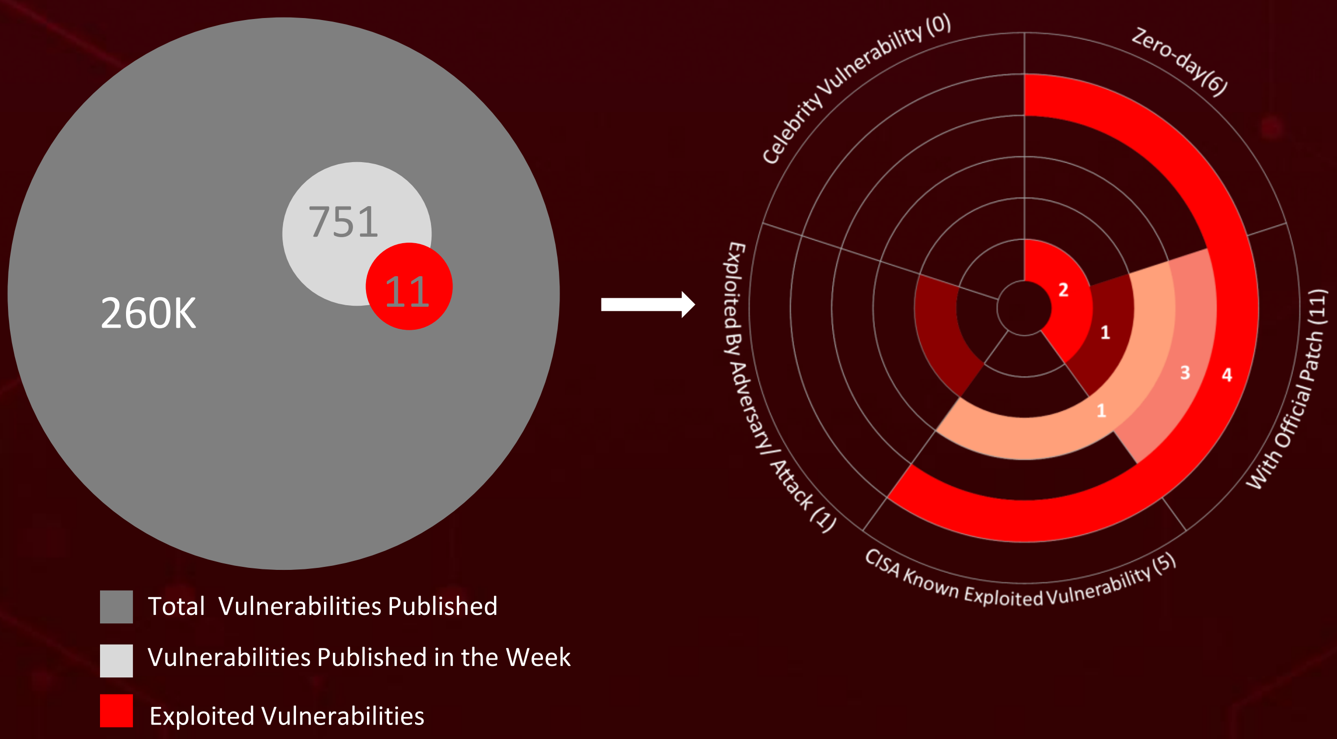
What Next? 29

Summary

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

Additionally, **GorillaBot**, an advanced botnet, executed 300,000+ DDoS attacks across 113 countries in September 2024, using diverse vectors and encryption, posing a severe global threat. **Microsoft's October 2024 Patch** Tuesday addresses 117 vulnerabilities, including 3 critical and 2 actively exploited zero-day flaws (**CVE-2024-43572 and CVE-2024-43573**).

Furthermore, this week, **GoldenJackal**, a skilled APT group, launched advanced cyberattacks on government and diplomatic targets in Europe, aiming to breach air-gapped systems and steal sensitive data. Mozilla fixed the critical zero-day flaw **CVE-2024-9680** in Firefox, which is actively exploited to execute arbitrary code. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

13

Attacks Executed

11

Vulnerabilities Exploited

3

Adversaries in Action

- VeilShell
- GorillaBot
- JackalWorm
- GoldenDealer
- GoldenHowl
- GoldenRobo
- GoldenAce
- GoldenUsbCopy
- GoldenBlacklist
- GoldenMailer
- GoldenDrive
- Akira ransomware
- Fog ransomware

- CVE-2024-45519
- CVE-2024-43573
- CVE-2024-43572
- CVE-2024-6197
- CVE-2024-20659
- CVE-2024-43583
- CVE-2024-9680
- CVE-2024-9379
- CVE-2024-9380
- CVE-2024-9381
- CVE-2024-40711

- APT37
- GoldenJackal
- Awaken Likho

Insights

Awaken Likho, intensified its operations post-Russo-Ukrainian conflict by switching from UltraVNC to MeshAgent to target government and industrial networks.

Ivanti, fixed three actively exploited zero-day vulnerabilities in its Cloud Services Appliance that could enable remote code execution and SQL command execution.

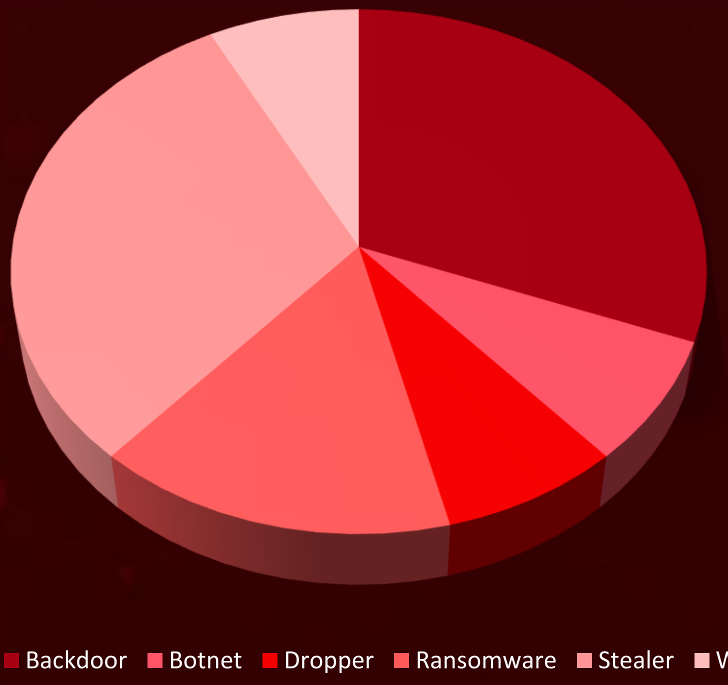
Mozilla has patched the critical zero-day vulnerability CVE-2024-9680, which is actively exploited to run arbitrary code.

Microsoft's October 2024 Patch Tuesday addresses two actively exploited zero-day flaws, **CVE-2024-43572** and CVE-2024-43573.

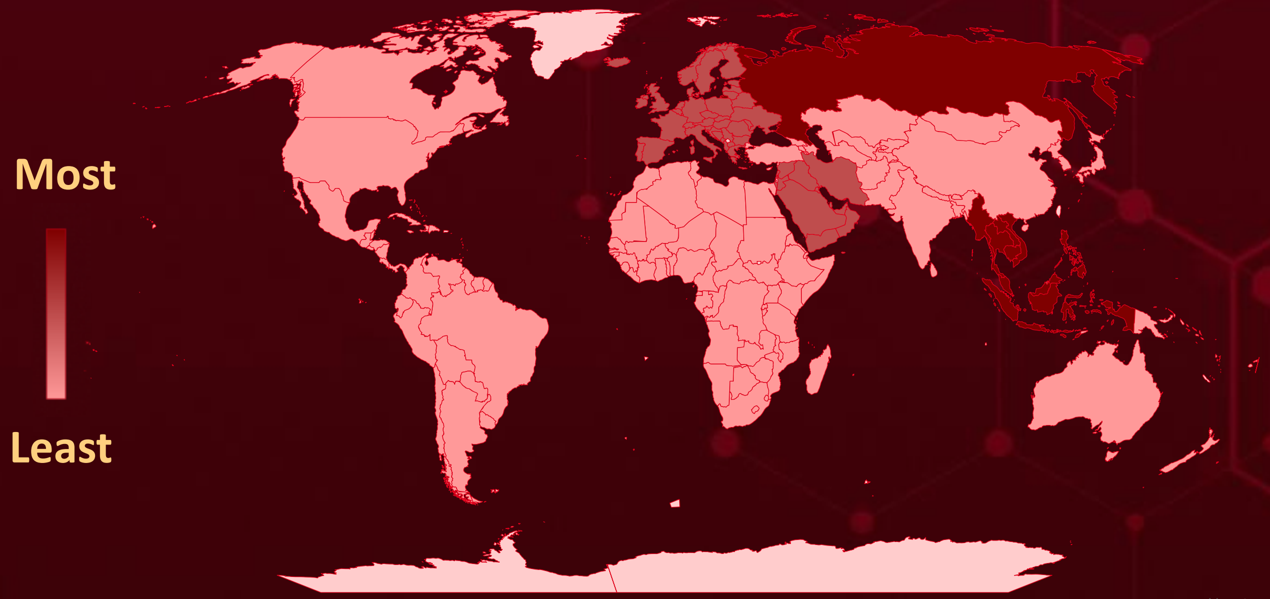
CVE-2024-45519, is a critical vulnerability in Zimbra Collaboration Suite that allows unauthenticated remote command execution via an OS command injection flaw in the postjournal service.

CVE-2024-40711 is a critical RCE flaw in Veeam Backup & Replication that allows unauthenticated attackers to execute arbitrary code, exploited in ransomware attacks like Fog and Akira.

Threat Distribution



Targeted Countries



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

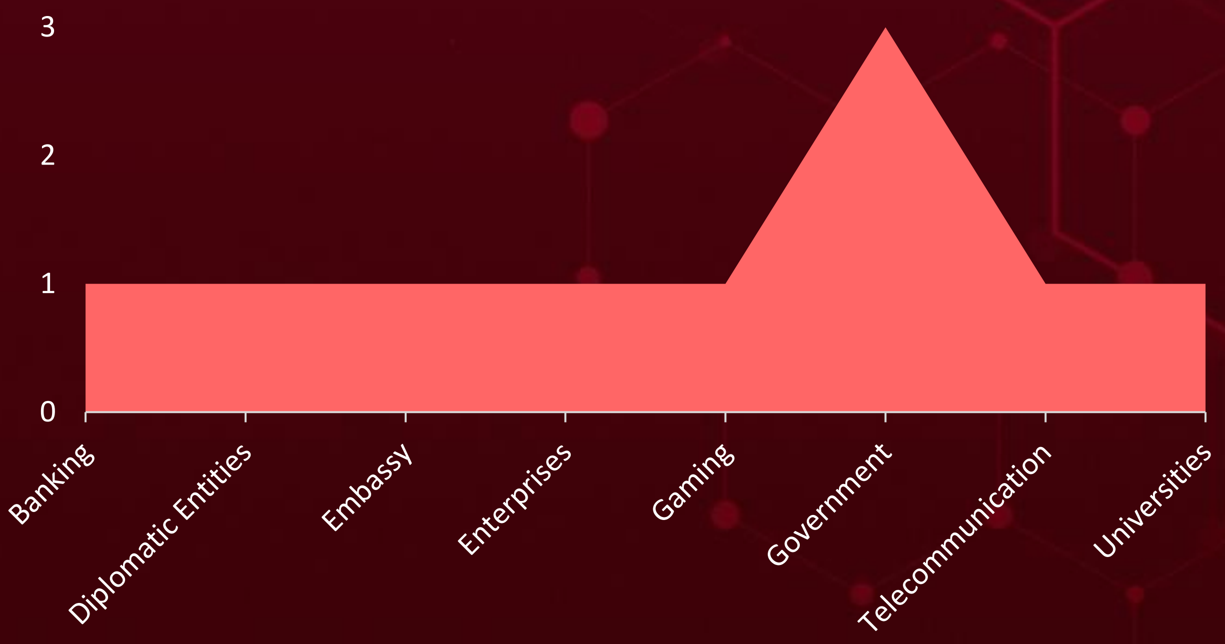
	Countries
■	Russia
■	Myanmar
■	Thailand
■	Cambodia
■	Philippines
■	Indonesia
■	Singapore
■	Laos
■	Malaysia
■	Vietnam
▨	Montenegro
▨	Slovakia
▨	Portugal
▨	Croatia
▨	United Arab Emirates
▨	Czech Republic
▨	Norway
▨	Denmark
▨	San Marino
▨	Estonia
▨	Switzerland
▨	Finland
▨	Moldova
▨	France
▨	Netherlands
▨	Germany

	Countries
▨	Greece
▨	Romania
▨	Holy See
▨	Serbia
▨	Hungary
▨	Spain
▨	Iceland
▨	Bulgaria
▨	Andorra
▨	Malta
▨	Iran
▨	Monaco
▨	Iraq
▨	Belarus
▨	Ireland
▨	North Macedonia
▨	Israel
▨	Oman
▨	Italy
▨	Poland
▨	Jordan
▨	Qatar
▨	Kuwait
▨	Bosnia and Herzegovina
▨	Austria
▨	Saudi Arabia
▨	Latvia

	Countries
▨	Belgium
▨	Brunei Darussalam
▨	United Kingdom
▨	Slovenia
▨	Yemen
▨	Sweden
▨	Liechtenstein
▨	Syria
▨	Lithuania
▨	Ukraine
▨	Luxembourg
▨	Albania
▨	Bahrain
▨	Lebanon
□	Ghana
□	South Africa
□	Rwanda
□	Benin
□	Togo
□	Grenada
□	Peru
□	Guatemala
□	Eritrea
□	Guinea
□	Suriname
□	Guinea-Bissau
□	Gambia
□	Guyana
□	Palau

	Countries
□	Haiti
□	DR Congo
□	Bhutan
□	El Salvador
□	Honduras
□	Eswatini
□	Bolivia
□	Sri Lanka
□	Armenia
□	Tajikistan
□	India
□	Turkey
□	Botswana
□	Uruguay
□	Brazil
□	Bangladesh
□	Brunei
□	Papua New Guinea
□	Australia
□	Dominica
□	Algeria
□	Ecuador
□	Burkina Faso
□	Saint Lucia
□	Jamaica
□	Equatorial Guinea
□	Japan
□	Sierra Leone

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1588** Obtain Capabilities	**T1068** Exploitation for Privilege Escalation	**T1588.006** Vulnerabilities
T1588.001 Malware	**T1041** Exfiltration Over C2 Channel	**T1204.002** Malicious File	**T1203** Exploitation for Client Execution	**T1204** User Execution
T1070 Indicator Removal	**T1574** Hijack Execution Flow	**T1027** Obfuscated Files or Information	**T1082** System Information Discovery	**T1566** Phishing
T1055 Process Injection	**T1059.003** Windows Command Shell	**T1057** Process Discovery	**T1083** File and Directory Discovery	**T1105** Ingress Tool Transfer

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
VeilShell	VeilShell is a stealthy PowerShell-based malware used by North Korea's APT37. It's designed to evade detection and maintain persistence on compromised systems. The malware is often used as a backdoor to allow attackers to remotely access and control infected systems.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Stealthy access and Data exfiltration	-
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
APT37			-

IOC TYPE	VALUE
SHA256	BEAF36022CE0BD16CAAEE0EBFA2823DE4C46E32D7F35E793AF4E1538E705379F, 9D0807210B0615870545A18AB8EAE8CECF324E89AB8D3B39A461D45CAB9EF957, 106C513F44D10E6540E61AB98891AEE7CE1A9861F401EEE2389894D5A9CA96EF, 6B95BC32843A55DA1F8186AEC06C0D872CAC13D9DF6D87114C5F8B7277C72A4F, AF74D416B65217D0B15163E7B3FD5D0702D65F88B260C269C128739E7E7A4C4D

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 CVEs</th></tr>
<tr><td rowspan="2">GorillaBot</td><td rowspan="6">GorillaBot is a new and advanced botnet that has executed over 300,000 DDoS attacks between September 4 to 27, 2024, targeting over 113 countries, including China and the U.S. It uses a variety of attack vectors, including UDP and TCP ACK floods, and exploits vulnerabilities in devices and systems.</td><td>Exploit vulnerabilities</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><th>TYPE</th><td rowspan="4">Massive DDoS attacks</td><td rowspan="2">-</td></tr>
<tr><td>Botnet</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>-</td><td>-</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">22a545fdb6ebbc5ba351c97d32cd008a1550a49891ae6112ddc8a6370376f053,
4cac6023b760e1fdae8c096a4db425eae3bbfe0d2554551efb76fc2f2d3a6b1b,
e8320657b9ff24198170e6b30188304555b43281b654075052721717f66fb4df,
42845557a515bc05c290b3ab9d1ad291303691d472db9e09863bfc782b803ed2,
d99d10559f1ad6bba1b59913604e261a613daa94af01ade8276effd692b5c03f</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">JackalWorm</td><td rowspan="6">JackalWorm is a sophisticated piece of malware utilized by the GoldenJackal APT group. It detects presence of USB devices and replicates through them. Its primary function is to facilitate the spread of other malicious tools, notably the JackalControl trojan, across both air-gapped and connected systems.</td><td>Infected USB Drives</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><th>TYPE</th><td rowspan="4">Data Exfiltration</td><td rowspan="2">-</td></tr>
<tr><td>Worm</td></tr>
<tr><th>ASSOCIATED ACTOR</th><th>PATCH LINK</th></tr>
<tr><td>GoldenJackal</td><td>--</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA1</td><td colspan="3">a87ceb21ef88350707f278063d7701bde0f8b6b7</td></tr>
</table>

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
GoldenDealer	GoldenDealer is a malicious component developed by the GoldenJackal APT group, designed to infiltrate air-gapped systems via USB drives. It monitors for USB insertion on compromised internet-connected machines and automatically copies itself and additional payloads onto the drives.	Infected USB Drives	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Install other malware and Data exfiltration	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
GoldenJackal			--

IOC TYPE	VALUE
SHA1	da9562f5268fa61d19648dff9c6a57fb8ab7b0d7

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GoldenHowl	GoldenHowl is a modular backdoor malware developed by the GoldenJackal APT group, written in Python and designed to maintain control over infected systems. It is distributed as a self-extracting archive that contains both legitimate Python binaries and malicious scripts, allowing it to operate on internet-connected machines.	Infected USB Drives	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data exfiltration	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
GoldenJackal			-

IOC TYPE	VALUE
SHA1	5f12ffd272aabc0d5d611d18812a196a6ea2faa9

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
GoldenRobo	GoldenRobo is a malware tool utilized by the GoldenJackal APT group for file collection and data exfiltration from compromised systems. Operating on internet-connected PCs, it extracts files from USB drives and transmits them to an attacker-controlled server. Written in Go, GoldenRobo employs the legitimate Windows utility robocopy to facilitate its file-copying functions.	Infected USB Drives	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			--
IOC TYPE	**VALUE**		
SHA1	6de7894f1971fdc1df8c4e4c2edcc4f4489353b6		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GoldenAce	GoldenAce is a malware component used by the GoldenJackal APT group to propagate malicious software through USB drives targeting air-gapped systems. It operates by hiding malware on USB devices and automatically installing it on connected systems, facilitating the spread of other malicious components. GoldenAce employs a lightweight worm variant known as JackalWorm to enhance its distribution capabilities.	Infected USB Drives	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		Install other malware	-
ASSOCIATED ACTOR			**PATCH LINK**
GoldenJackal			-
IOC TYPE	**VALUE**		
SHA1	24fbcec23e8b4b40fea188132b0e4a90c65e3ffb		

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
GoldenUsbCopy	GoldenUsbCopy is a malware component developed by the GoldenJackal APT group, designed to monitor USB drives and facilitate the theft of sensitive files. It operates by exfiltrating recently modified files that meet specific criteria, such as size and content type, without relying on AES encryption.	Infected USB Drives	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data theft	-
Stealer			
ASSOCIATED ACTOR			PATCH LINK
GoldenJackal			--

IOC TYPE	VALUE
SHA1	7cb7c3e98cab2226f48ba956d3be79c52ab62140

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GoldenBlacklist	GoldenBlacklist is a malware component utilized by the GoldenJackal APT group to filter and archive specific email messages from compromised systems. It processes emails of interest before preparing them for exfiltration, ensuring that only valuable data is captured.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Data exfiltration	-
Stealer			
ASSOCIATED ACTOR			PATCH LINK
GoldenJackal			-

IOC TYPE	VALUE
SHA1	9cbe8f7079da75d738302d7db7e97a92c4de5b71

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 CVEs</th></tr>
<tr><td rowspan="3">GoldenMailer</td><td rowspan="7">GoldenMailer is a malware component used by the GoldenJackal APT group to exfiltrate stolen information via email. It automates the process of sending collected files as email attachments to accounts controlled by the attackers, thereby facilitating data theft from compromised systems.</td><td>Phishing</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td rowspan="5">Data exfiltration</td><td rowspan="3">-</td></tr>
<tr><td><b>TYPE</b></td></tr>
<tr><td>Stealer</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>GoldenJackal</td><td>--</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA1</td><td colspan="3">c830efd843a233c170285b4844c5960ba8381979</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="3">GoldenDrive</td><td rowspan="7">GoldenDrive is a malware component used by the GoldenJackal APT group to exfiltrate sensitive data by uploading it to Google Drive. This tool automates the process of transferring stolen files from compromised systems, enabling attackers to bypass traditional data transfer methods that might trigger security alerts.</td><td>-</td><td>-</td></tr>
<tr><td><b>IMPACT</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td rowspan="5">Data exfiltration</td><td rowspan="3">-</td></tr>
<tr><td><b>TYPE</b></td></tr>
<tr><td>Stealer</td></tr>
<tr><td><b>ASSOCIATED ACTOR</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>GoldenJackal</td><td>-</td></tr>
<tr><td><b>IOC TYPE</b></td><td colspan="3"><b>VALUE</b></td></tr>
<tr><td>SHA1</td><td colspan="3">f7192914e00dd0ce31df0911c073f522967c6a97</td></tr>
</table>

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
Akira	Akira ransomware, first identified in March 2023, targets both Windows and Linux systems, employing a hybrid encryption method using ChaCha20 and RSA. This ransomware utilizes a double extortion tactic, encrypting files and exfiltrating sensitive data before demanding large ransoms, often in the millions.	Exploiting Vulnerabilities	CVE-2024-40711
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data encryption and exfiltration	Veeam Backup & Replication
ASSOCIATED ACTOR			PATCH LINK
-			https://www.veeam.com/kb4600

IOC TYPE	VALUE
SHA256	8a2d54e3230a4e7656ca760b512a879e0cacbe912a519a1be6916449bd6b5628, 87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d, 58e685695afc3a85d2632777a2b54967dc53d6a6fa1b7e2c110b2023b561bfe9, 1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Fog ransomware (aka Lost in the Fog)	Fog ransomware utilizes techniques such as 'pass-the-hash' attacks to escalate privileges, enabling it to access administrator accounts. Encrypted files typically receive the extensions .FOG or .FLOCKED.	Exploiting Vulnerabilities	CVE-2024-40711
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data encryption and exfiltration	Veeam Backup & Replication
ASSOCIATED ACTOR			PATCH LINK
-			https://www.veeam.com/kb4600

IOC TYPE	VALUE
IPv4	85[.]209[.]11[.]227, 85[.]209[.]11[.]254, 85[.]209[.]11[.]27
SHA256	e67260804526323484f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-45519</td><td>✗</td><td rowspan="2">Zimbra Collaboration (ZCS) before 8.8.15 Patch 46,
9 before 9.0.0 Patch 41,
10 before 10.0.9, and
10.1 before 10.1.1</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:zimbra:collaboration:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Synacor Zimbra Collaboration Command Execution Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-863
CWE-284</td><td>T1059: Command and Scripting Interpreter
T1190: Exploit Public-Facing Application</td><td>https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P46;
https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P41;
https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.9;
https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.1</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43573	✗	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows MSHTML Platform Spoofing Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter, T1204 : User Execution, T1189 : Drive-by Compromise	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43572	✗	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Management Console Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-707	T1059: Command and Scripting Interpreter, T1204 : User Execution, T1204.002: Malicious File	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-6197	⊗	CBL Mariner Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:haxx:libcurl:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Open Source Curl Remote Code Execution Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-590	T1204 : User Execution; T1203 : Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6197

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20659	⊗	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Hyper-V Security Feature Bypass Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1211 : Exploitation for Defense Evasion, T1554 : Compromise Host Software Binary	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20659

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43583	✗	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Winlogon Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-250	T1059: Command and Scripting Interpreter; T1068 : Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43583

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9680	✗	Firefox Version Prior to 131.0.2, Firefox ESR Version Prior to 128.3.1, and Firefox ESR Version Prior to 115.16.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:*	-
Mozilla Firefox and Firefox ESR Use-After- Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1189 : Drive-by Compromise	https://www.mozilla.org/en-US/firefox/enterprise/#download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9379	✗	Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*	-
Ivanti Cloud Services Appliance SQL Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1078 : Valid Accounts, T1190 : Exploit Public-Facing Application	https://forums.ivanti.com/s/article/Ivanti-Cloud-Services-Application-5-0-2-Download-Release-Notes-Patch-History

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9380	✗	Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*	-
Ivanti Cloud Services Appliance OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1190 : Exploit Public-Facing Application, T1078 : Valid Accounts	https://forums.ivanti.com/s/article/Ivanti-Cloud-Services-Application-5-0-2-Download-Release-Notes-Patch-History

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9381	✗	Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:*	-
Ivanti Cloud Services Appliance Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1078 : Valid Accounts, T1190 : Exploit Public-Facing Application	https://forums.ivanti.com/s/article/Ivanti-Cloud-Services-Application-5-0-2-Download-Release-Notes-Patch-History

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-40711	✗	Veeam Backup & Replication before 12.2.0.334 versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*	Akira and Fog ransomware
Veeam Backup & Replication Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter; T1068 : Exploitation for Privilege Escalation	https://www.veeam.com/kb4600

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT37 (aka Reaper, TEMP.Reaper, Ricochet Chollima, ScarCruft, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet)	North Korea	Aerospace, Automotive, Chemical, Education, Financial, Government, Healthcare, High-Tech, Manufacturing, Media, Technology, Transportation	Southeast Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	VeilShell	-

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.001: Spearphishing Attachment; T1560: Archive Collected Data; T1132: Data Encoding; T1003: OS Credential Dumping; T1555: Credentials from Password Stores; T1027: Obfuscated Files or Information; T1070: Indicator Removal; T1070.004: File Deletion; T1112: Modify Registry; T1574: Hijack Execution Flow; T1574.014: AppDomainManager; T1033: System Owner/User Discovery; T1057: Process Discovery; T1069: Permission Groups Discovery; T1082: System Information Discovery; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.007: JavaScript; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys /Startup Folder; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
GoldenJackal	-	Government, Diplomatic Entities, Embassy	Europe, the Middle East, and South Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	JackalWorm, GoldenDealer, GoldenHowl, GoldenRobo, GoldenAce, GoldenUsbCopy, GoldenBlacklist, GoldenMailer, GoldenDrive	-
TTPs			
TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583: Acquire Infrastructure; T1583.003: Virtual Private Server; T1583.004: Server; T1584: Compromise Infrastructure; T1584.006: Web Services; T1587: Develop Capabilities; T1587.001: Malware; T1585: Establish Accounts; T1585.003: Cloud Accounts; T1588: Obtain Capabilities; T1588.002: Tool; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command: Shell; T1059.006: Python; T1106: Native API; T1569: System Services; T1569.002: Service Execution; T1204: User Execution; T1204.002: Malicious File; T1543: Create or Modify System Process; T1543.003: Windows Service; T1547.001: Registry Run Keys /Startup Folder; T1547: Boot or Logon: Autostart Execution; T1053.005: Scheduled Task; T1564.001: Hidden Files and Directories; T1070.004: File Deletion; T1036.005: Match Legitimate Name or Location; T1036.008: Masquerade File Type; T1112: Modify Registry; T1027.013: Encrypted/Encoded File; T1552.001: Credentials In Files; T1552.004: Private Keys; T1087.001: Local Account; T1083: File and Directory Discovery; T1046: Network Service Discovery; T1120: Peripheral Device Discovery; T1057: Process Discovery; T1018: Remote System Discovery; T1518: Software Discovery; T1082: System Information Discovery; T1016.001: Internet Connection Discovery; T1135: Network Share Discovery; T1210: Exploitation of Remote Services; T1091: Replication Through Removable Media; T1560.002: Archive via Library; T1119: Automated Collection; T1005: Data from Local System; T1025: Data from Removable: Media; T1074.001: Local Data Staging; T1114.001: Local Email Collection; T1071.001: Web Protocols; T1092: Communication Through Removable Media; T1132.001: Standard Encoding; T1572: Protocol Tunneling; T1090.001: Internal Proxy; T1041: Exfiltration Over C2 Channel; T1052.001: Exfiltration over USB; T1132: Data Encoding; T1567.002: Exfiltration to Cloud Storage; T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol; T1016: System Network Configuration Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Awaken Likho (aka Core Werewolf, PseudoGamaredon)	-	Enterprises, Government	Russia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	-	-

TTPs

TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; T1593: Search Open Websites/Domains; T1593.002: Search Engines; T1566: Phishing; T1566.001: Spearphishing Attachment; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1053: Scheduled Task/Job; T1053.005: Scheduled Task; T1204: User Execution; T1204.002: Malicious File; T1543: Create or Modify System Process; T1055: Process Injection; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1036.007: Double File Extension; T1083: File and Directory Discovery; T1057: Process Discovery; T1005: Data from Local System; T1070: Indicator Removal; T1027: Obfuscated Files or Information; T1027.002: Software Packing; T1133: External Remote Services; T1564.003: Hidden Window; T1059.010: AutoHotKey & AutoIT

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **eleven exploited vulnerabilities** and block the indicators related to the threat actors **APT37, GoldenJackal, Awaken Likho** and malware **VeilShell, GorillaBot, JackalWorm, GoldenDealer, GoldenHowl, GoldenRobo, GoldenAce, GoldenUsbCopy, GoldenBlacklist, GoldenMailer, GoldenDrive, Akira ransomware,** and **Fog ransomware.**

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 **eleven exploited vulnerabilities.**

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT37, GoldenJackal, Awaken Likho** and malware **VeilShell, GorillaBot, Akira ransomware** and **Fog ransomware** in Breach and Attack Simulation(BAS).

Threat Advisories

SHROUDED#SLEEP: North Korea's Silent Cyber Assault on Southeast Asia

Critical Command Execution Flaw in Zimbra Under Active Exploitation

Critical Apache Avro Flaw Opens Door to Remote Code Execution

GorillaBot: A Rising Threat in Global DDoS Attacks

GoldenJackal’s Covert Ops: Stealing Secrets from Air-Gapped Systems

Microsoft’s October Patch Tuesday Addresses Active Zero-Day Exploits

Firefox Zero-Day Alert: Critical Animation Timeline Flaw Exploited in the Wild

Ivanti CSA Zero-Day Exploits Trigger Widespread Attacks

Awaken Likho Adopts New Tactics to Spy on Russian Government

GitLab Addresses Critical Flaws in Community and Enterprise Editions

Veeam Backup & Replication RCE Flaw Opens Door for Ransomware Attacks

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
VeilShell	SHA256	BEAF36022CE0BD16CAAEE0EBFA2823DE4C46E32D7F35E793AF4E1538E705379F, 9D0807210B0615870545A18AB8EAE8CECF324E89AB8D3B39A461D45CAB9EF957, 106C513F44D10E6540E61AB98891AEE7CE1A9861F401EEE2389894D5A9CA96EF, 6B95BC32843A55DA1F8186AEC06C0D872CAC13D9DF6D87114C5F8B7277C72A4F, AF74D416B65217D0B15163E7B3FD5D0702D65F88B260C269C128739E7E7A4C4D, 7E9F91F0CFE3769DF30608A88091EE19BC4CF52E8136157E4E0A5B6530D510EC
GorillaBot	MD5	276adc6a55f13a229a5ff482e49f3a0b, 63cbfc2c626da269c67506636bb1ea30, 7f134c477f307652bb884cafe98b0bf2, 3a3be84df2435623132efd1cd9467b17, 03a59780b4c5a3c990d0031c959bf7cc, 5b37be51ee3d41c07d02795a853b8577, 15f6a606ab74b66e1f7e4a01b4a6b2d7
	URL	hxxp[://]pen.gorillafirewall[.]su/
	SHA256	22a545fdb6ebbc5ba351c97d32cd008a1550a49891ae6112ddc8a6370376f053, 4cac6023b760e1fdae8c096a4db425eae3bbfe0d2554551efb76fc2f2d3a6b1b, e8320657b9ff24198170e6b30188304555b43281b654075052721717f66fb4df,

Attack Name	TYPE	VALUE
GorillaBot	SHA256	42845557a515bc05c290b3ab9d1ad291303691d472db9e09863bfc782b803ed2, d99d10559f1ad6bba1b59913604e261a613daa94af01ade8276effd692b5c03f, 826f9c8153c14a66ba730291e5f78d71d958c08cde45e2119afa227211ee5132, 6d10e4da8d8090e0e7e077ef4aead8b8720d1bd4f9b86d34ae66eac0e17e659c, b4a2a1900bab5b6e405cc78b72c5d1706c789b309bc1fa27ad746153ccb84004, 3905126f5f9f7430dee31c207706852e56292291449b563781bc6ee0b540343a, d4007f1ac2cb3a48db4bde7dbab7255421bf64f768a06492b81087f67a2e6c9c, e03580729f2f09dbd937d685fc9229959e84c9f329bee7eee16536bb8f9e60cf, 81c775f9540a66fded643fe4ec53dbbf35742bd3b069d95d689da313fc9b80a9
JackalWorm	SHA1	a87ceb21ef88350707f278063d7701bde0f8b6b7
GoldenDealer	SHA1	da9562f5268fa61d19648dff9c6a57fb8ab7b0d7
GoldenHowl	SHA1	5f12ffd272aabc0d5d611d18812a196a6ea2faa9
GoldenRobo	SHA1	6de7894f1971fdc1df8c4e4c2edcc4f4489353b6
GoldenAce	SHA1	24fbcec23e8b4b40fea188132b0e4a90c65e3ffb
GoldenUsbCopy	SHA1	7cb7c3e98cab2226f48ba956d3be79c52ab62140
GoldenBlacklist	SHA1	9cbe8f7079da75d738302d7db7e97a92c4de5b71
GoldenMailer	SHA1	c830efd843a233c170285b4844c5960ba8381979
GoldenDrive	SHA1	f7192914e00dd0ce31df0911c073f522967c6a97
Akira Ransomware	SHA256	8a2d54e3230a4e7656ca760b512a879e0cacbe912a519a1be6916449bd6b5628, 87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d, 58e685695afc3a85d2632777a2b54967dc53d6a6fa1b7e2c110b2023b561bfe9, 1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218, 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c, ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d, c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddccd5bb37857e7bde6d2eb7, a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc,

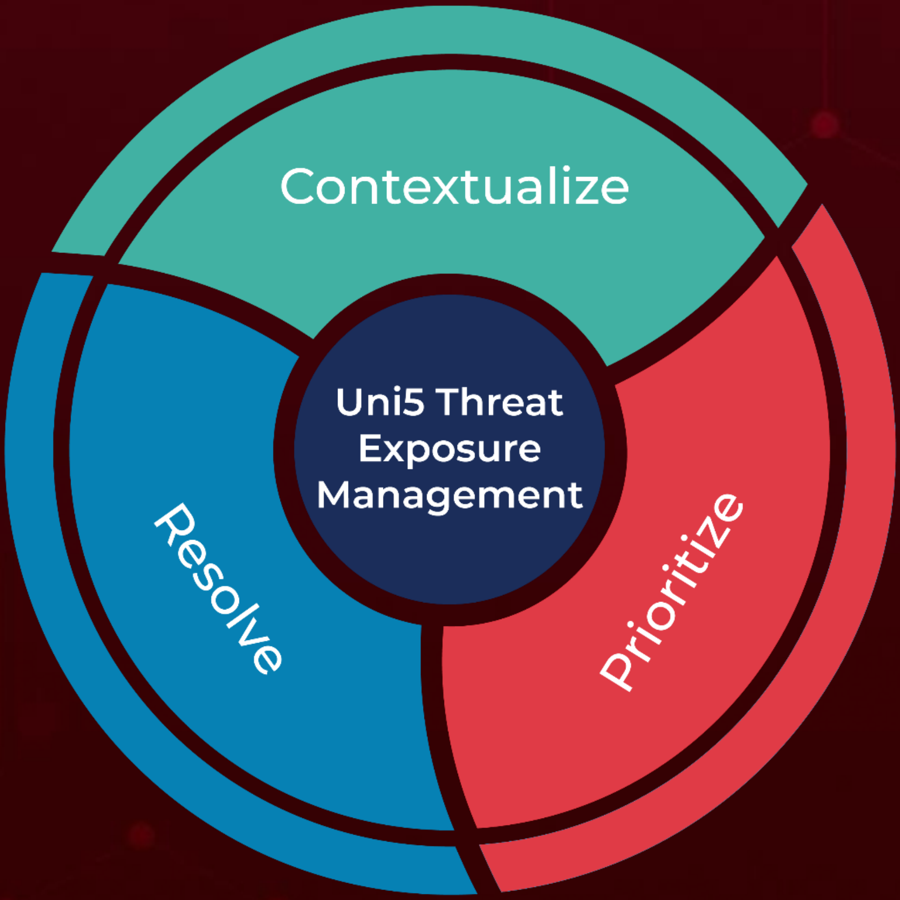
Attack Name	TYPE	VALUE
Akira Ransomware	SHA256	2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422, 74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1
Fog Ransomware	SHA256	e67260804526323484f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3

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

October 15, 2024 • 01:30 AM

More at www.hivepro.com