Date of Publication
August 28, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

21 to 27 AUGUST 2023

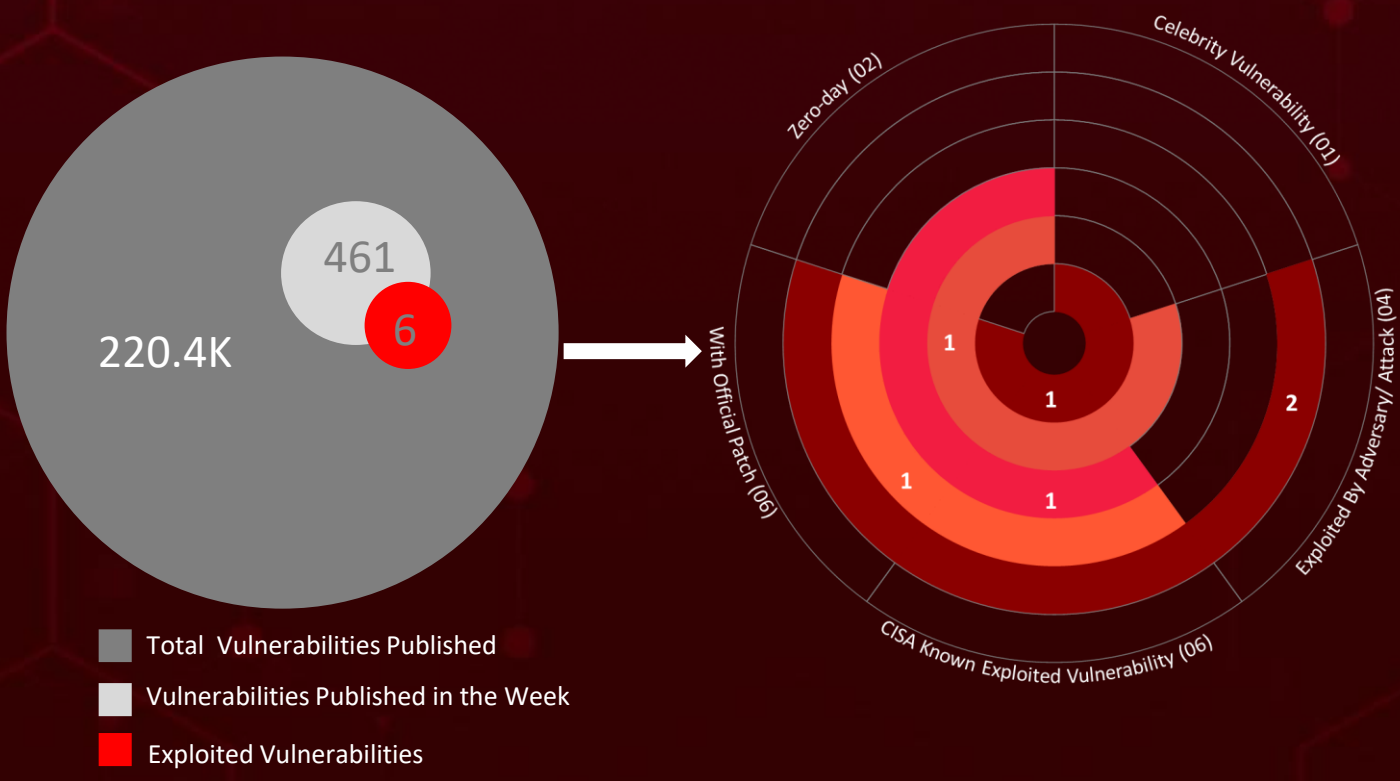
Table Of Contents

Summary

HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of **twelve** attacks executed, **six** vulnerabilities, and **three** different adversaries highlights the ever-present danger of cyber attacks.

Moreover, HiveForce Labs also discovered that the **Zerologon** Vulnerability was exploited in two separate campaigns by the **CosmicBeetle** threat actor to deploy the Scarab Ransomware and the **Cuba Ransomware**. Furthermore, identified that the Akira ransomware group targets Cisco VPN products to breach corporate networks and leverages tools like RustDesk for stealthy access.

Meanwhile, cybercriminals were found to be using **three** types of ransomware and **three** remote-access trojans in various orchestrated campaigns. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

12
Attacks Executed

6
Vulnerabilities Exploited

3
Adversaries in Action

- Cuba Ransomware
- BUGHATCH
- BURNTCIGAR
- Akira Ransomware
- PlugX
- DarkMe
- GuLoader
- Remcos RAT
- Scarab Ransomware
- Spacecolon
- QuiteRAT
- CollectionRAT

- CVE-2023-27532
- CVE-2020-1472
- CVE-2023-38035
- CVE-2023-38831
- CVE-2022-47966
- CVE-2023-32315

- Carderbee
- CosmicBeetle
- Lazarus Group

Insights

Akira Ransomware

Strikes Corporate Networks via Cisco VPN Exploits and Sneaky RustDesk Tactics

Wave of Cuba Ransomware

Targeting US Critical Infrastructure and Latin American IT Enterprises with a Fusion of Tools and Exploits

Unveiling Carderbee APT

Supply Chain Strike via Cobra DocGuard Paves Way for Sinister PlugX Backdoor

2 Rogue RATs Set Loose by the Lazarus Threat Group After Exploiting Zoho ManageEngine ServiceDesk Plus Vulnerability

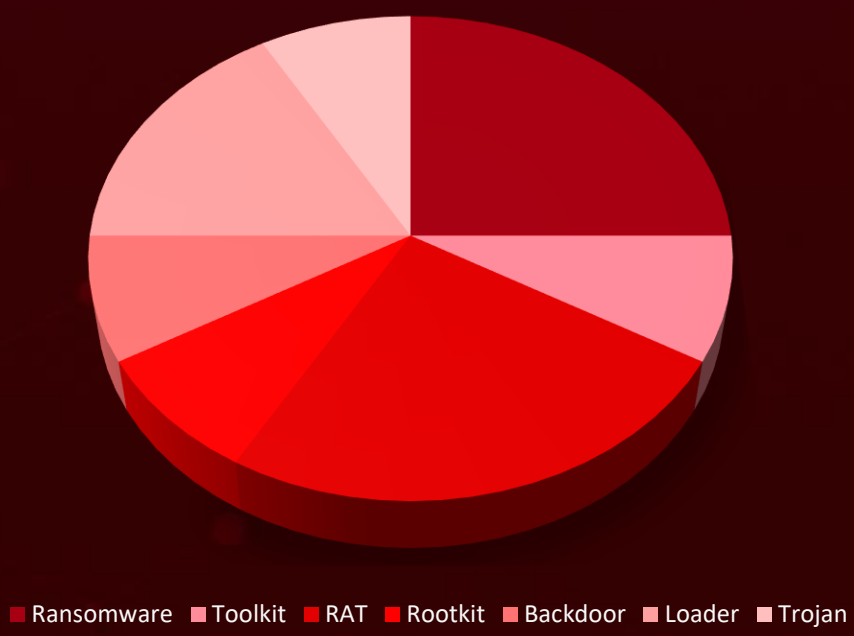
3-Fold Threat Unleashed

WinRAR's CVE-2023-38831 Zero-Day Exploited for Tricky Malware Infiltration

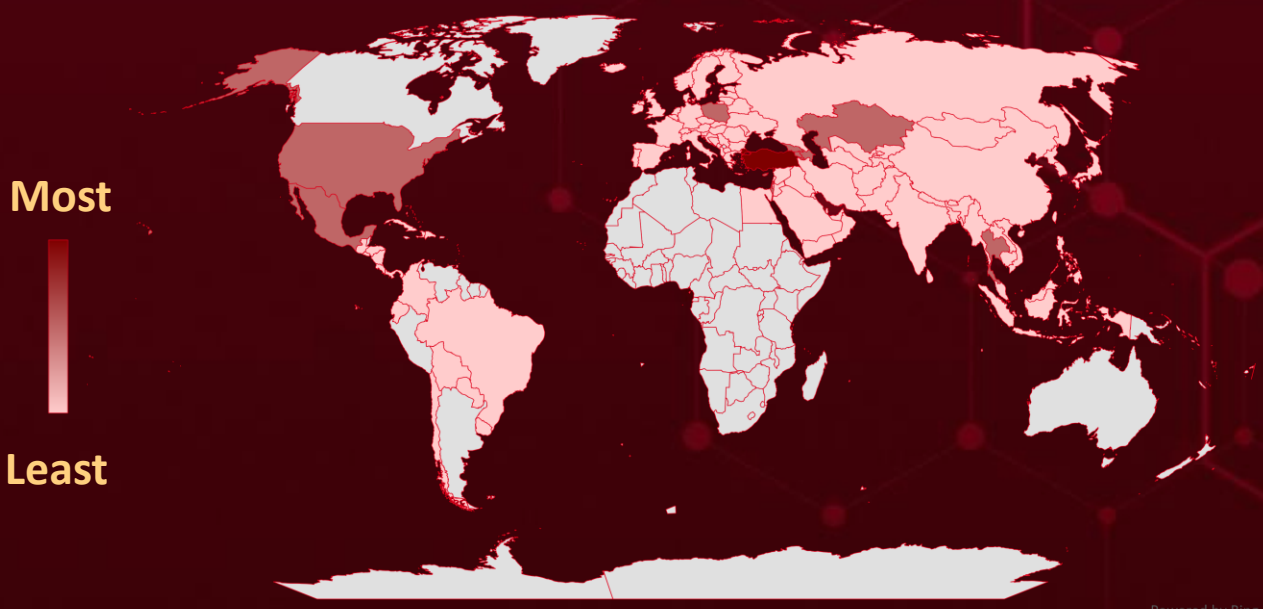
CosmicBeetle's Cyber Siege

The Relentless Spacecolon Toolset Fueling Scarab Ransomware Surge

Threat Distribution



Targeted Countries



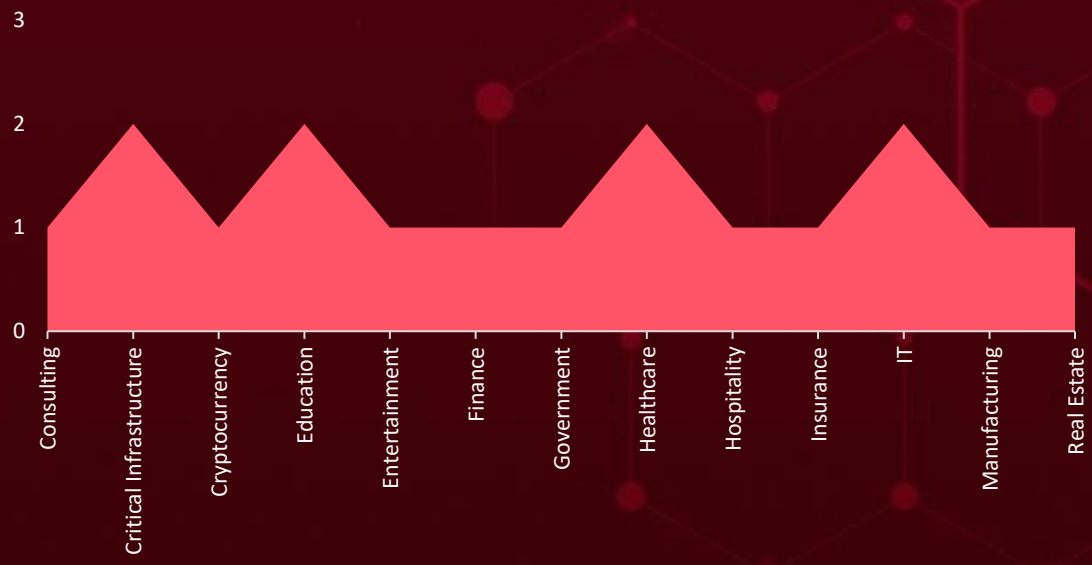
Countries
Turkey
Poland
USA
Israel
Azerbaijan
Mexico
Cyprus
Armenia
Thailand
Georgia
Kazakhstan
North Korea
Bolivia
San Marino
Bosnia and Herzegovina
Moldova
Brazil
Philippines
Brunei
Sri Lanka
Bulgaria
Malaysia
Cambodia
Myanmar

Countries
Chile
Pakistan
China
Qatar
Colombia
Slovakia
Costa Rica
Taiwan
Croatia
Luxembourg
Cuba
Malta
Albania
Mongolia
Czechia
Netherlands
Denmark
Norway
Dominican Republic
Panama
East Timor
Portugal
Ecuador
Romania
Egypt

Countries
Serbia
El Salvador
South Korea
Estonia
Switzerland
Finland
Belgium
France
Lithuania
Austria
Macao
Germany
Maldives
Greece
Bangladesh
Guatemala
Monaco
Haiti
Montenegro
Honduras
Nepal
Hong Kong
Nicaragua
Hungary
North Macedonia

Countries
Iceland
Oman
India
Palestine
Indonesia
Paraguay
Iran
Belarus
Iraq
Puerto
Ireland
Rico
Andorra
Russia
Italy
Saudi Arabia
Japan
Singapore
Jordan
Slovenia
Turkmenistan
Spain
Ukraine
Sweden
United Kingdom

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1105** Ingress Tool Transfer	**T1543.003** Windows Service	**T1588.006** Vulnerabilities	**T1082** System Information Discovery
T1036 Masquerading	**T1190** Exploit Public-Facing Application	**T1056** Input Capture	**T1588** Obtain Capabilities	**T1018** Remote System Discovery
T1095 Non-Application Layer Protocol	**T1059.001** PowerShell	**T1133** External Remote Services	**T1059.003** Windows Command Shell	**T1518.001** Security Software Discovery
T1068 Exploitation for Privilege Escalation	**T1548.002** Bypass User Account Control	**T1070.004** File Deletion	**T1588.005** Exploits	**T1071** Application Layer Protocol

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cuba ransomware (aka Fidel, COLDDRAW)	The Cuba ransomware gains initial access through compromised administrative credentials via Remote Desktop Protocol (RDP), avoiding the need for brute force methods. The Bring Your Own Vulnerable Driver (BYOVD) technique is used to bypass endpoint protection tools.	Compromised administrative credentials via Remote Desktop Protocol	CVE-2023-27532 CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial Loss and Information theft	Veeam Backup & Replication & Veeam Cloud Connect and Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.veeam.com/kb4424 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

IOC TYPE	VALUE
SHA256	0a3517d8d382a0a45334009f71e48114d395a22483b01f171f2c3d4a9cfdbfbf, 0eff3e8fd31f553c45ab82cc5d88d0105626d0597afa5897e78ee5a7e34f71b3
SHA1	dce10f420e527bbb7eda14f15fa261b647fb0d56, 064e77464964a9a96ce79b56fe4d8b9e740d4e1f
MD5	286a7aa55ea888813b6df7c047aada5d, bcd57da0c23eae47fbe5b54db614cbc6

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
BUGHATCH	BUGHATCH is a custom loader exclusively linked to the Cuba ransomware group. This tool establishes a connection to a command-and-control (C2) server, fetching a payload, usually small PE files or PowerShell scripts.	PowerShell dropper	CVE-2023-27532 CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Information Theft	Veeam Backup & Replication & Veeam Cloud Connect and Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.veeam.com/kb4424 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472
IOC TYPE	**VALUE**		
SHA256	58ba30052d249805caae0107a0e2a5a3cb85f3000ba5479fafb7767e2a5a78f3		
SHA1	9a65eccba4d33801fdac0e89c90d7a03d430dd84		
MD5	1ef70081e367330f062fb5bae1234491		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BURNTCIGAR	BURNTCIGAR is an anti-malware utility that terminates kernel processes tied to endpoint security products. The threat actor has made some modifications, likely as a mechanism to impede both detections with the inclusion of the hashing functionality to BURNTCIGAR's codebase.	Unknown	CVE-2023-27532 CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Endpoint Security Products were decommissioned.	Veeam Backup & Replication & Veeam Cloud Connect and Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.veeam.com/kb4424 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472
IOC TYPE	**VALUE**		
SHA256	1c2d7f19f8c12e055e1ba8cdf5334e6cb5510847783fbe36121a35ad70f09eb3		

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 Ransomware	Akira, a relatively new ransomware operation, emerged in March 2023 and is written in C++. It has expanded its tactics by adding a Linux encryptor to target VMware virtual machines. Malware has been leveraging compromised Cisco VPN accounts to breach corporate networks without needing additional backdoors or persistence mechanisms.	Cisco VPN products	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware			
ASSOCIATED ACTOR		Extortion of data and Financial Loss	Windows, Linux, macOS and VMware
-			**PATCH LINK**
			-
IOC TYPE	**VALUE**		
SHA256	3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c, 5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5, 1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PlugX (aka Korplug)	The Carderbee advanced persistent threat (APT) group executed a supply chain attack by exploiting the legitimate Cobra DocGuard software. Their objective was to deploy the PlugX backdoor onto targeted organizations primarily situated in Hong Kong.	EsafeNet Cobra DocGuard Client	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor			
ASSOCIATED ACTOR		Data Theft, Malicious Downloads	-
Carderbee			**PATCH LINK**
			-
IOC TYPE	**VALUE**		
SHA256	1ff7b55dde007b7909f43dd47692f7c171caa2897d663eb9db01001062b1fe9d, 2400d8e66c652f4f8a13c99a5ffb67cb5c0510144b30e93122b1809b58614936		
URL	hxxp://111.231.100[.]228:8888/CDGServer3/UpgradeService2		

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
DarkMe	DarkMe is a VisualBasic spy Trojan first spotted in September 2021. The vulnerability allowed hackers to distribute malware by creating seemingly harmless archives that contained files like JPG images, text documents, or PDFs. When users opened these files, the flaw triggered a script that installed malware on their devices.	Exploiting zero-day vulnerability in WinRAR	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Financial Loss	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH DETAIL**
-			Update WinRAR version to 6.23 or later versions

IOC TYPE	VALUE
SHA256	a826570f878def28b027f6e6b2fcd8be1727e82666f8b65175d917144f5d0569, 7b478cd8b854c9046f45f32616e1b0cbdc9436fa078ceddb13ce9891b24b30a5, e72337c08d6b884b64fd9945c5a01557ccf40db93af866c00c48d36b6605f3a0

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GuLoader (aka CloudEye)	GuLoader is used to load other malicious files and employs various obfuscation and anti-reverse analysis techniques to evade detection by security products. Once the initial setup is done, different PowerShell scripts will run to launch the GuLoader payload.	Exploiting zero-day vulnerability in WinRAR	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Malicious Downloads and Financial Loss	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH DETAIL**
-			Update WinRAR version to 6.23 or later versions

IOC TYPE	VALUE
SHA256	7da5b2207cf789cf6807b6cc3373048cbc951d7fd09ca8fb858693cfa5f5edba
SHA1	10c6429825adaba12c34696a8ff00879b2abbb88
MD5	ab5050f0b4b71352722a6122c8107f83

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
Remcos RAT(aka: Remcos, Remvio, Socmer)	Remcos RAT (acronym of Remote Control & Surveillance Software) is a commercial Remote Access Tool to remotely control computers, granting attackers significant control over the compromised system.	Exploiting zero-day vulnerability in WinRAR	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft and Financial Loss	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH DETAIL**
-			Update WinRAR version to 6.23 or later versions

IOC TYPE	VALUE
SHA256	7a1bb4fe0f62425fdd2e163ea17d84465323c4f2df8aabb8a50b1433e7d42a9f, b89e2bec5923fcd2b7c4f50f80dd5cd992a45409424a8cd1711c453dc38a2dc8, d5082b124437716d3f436aef25c69662dbed756d681e9f2a5a82d6c35fa0a7bb
SHA1	822ce06e4eb9679158646050d3ec6f11754e273d
MD5	c96f60219124ec01111cf884ffd1d2d9

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Scarab Ransomware	The attacks aim to utilize ScService's access to introduce a variant of the Scarab ransomware. Scarab, coded in Delphi. It uses an embedded configuration similar to Zeppelin ransomware, determining encrypted file details, filenames, targeted extensions, and ransom messages.	Exploiting Zerologon Vulnerability	CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Ransomware		Data Theft and financial loss	Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH DETAILS**
CosmicBeetle			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

IOC TYPE	VALUE
SHA1	e2eaa1ee0b51caf803ceedd7d3452577b6fe7a8d, 8f1374d4d6cc2899da1251de0325a7095e719edc

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
Spacecolon	Spacecolon consists of three core Delphi components: ScHackTool, ScInstaller, and ScService. The primary orchestrator component is ScHackTool, which enables CosmicBeetle to deploy the other components.	Exploiting Zerologon Vulnerability	CVE-2020-1472
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Toolkit		Data Theft and financial loss	Microsoft Netlogon
ASSOCIATED ACTOR			**PATCH LINK**
CosmicBeetle			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472
IOC TYPE	**VALUE**		
IPv4	3.76.107[.]228, 87.251.64[.]19		
SHA1	40b8af12ea6f89db6ed635037f468aadee7f4ca6, 95931de0aa6d96568acebc11e551e8e1305bf003, 4b07391434332e4f8faadf61f288e48389bcea08		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
QuiteRAT	QuiteRAT consists of a compact set of statically linked Qt libraries along with some user-written code. The QuiteRAT can also receive a command code along with a numeric value from the C2 server.	Exploiting vulnerability in Zoho ManageEngine ServiceDesk Plus.	CVE-2022-47966
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Sensitive Data Theft	Zoho ManageEngine
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus Group			https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html
IOC TYPE	**VALUE**		
SHA256	ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6		

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">CollectionRAT</td><td rowspan="6">Exhibiting conventional RAT capabilities, CollectionRAT enables the execution of arbitrary commands on compromised systems. CollectionRAT appears to share connections with Jupiter/EarlyRAT, another strain of malware attributed to Andariel, a subgroup nestled within the Lazarus Group threat actor-network.</td><td>Exploiting vulnerability in Zoho ManageEngine ServiceDesk Plus.</td><td>CVE-2022-47966</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>RAT</td><td rowspan="3">Sensitive Data Theft</td><td>Zoho ManageEngine</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Lazarus Group</td><td>https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984, 773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df</td></tr>
</table>

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

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27532		Veeam Backup & Replication & Veeam Cloud Connect	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:veeam:backup_\&_replication:11.0.1.1261:*:*:*:*:*:*:*	Cuba ransomware BUGHATCH, and BURNTCIGAR
Veeam Missing Authentication for Critical Function			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-306	T1078: Valid Accounts, T1040: Network Sniffing	https://www.veeam.com/kb4424

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-1472	Zerologon	Microsoft Netlogon	CosmicBeetle
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	Scarab Ransomware, Spacecolon, Cuba ransomware, BUGHATCH, and BURNTCIGAR
Microsoft Netlogon Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-330	T1068: Exploitation for Privilege Escalation, T1204.001: Malicious Link,	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

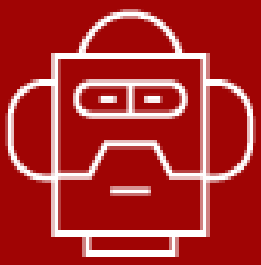
CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38035	✗	Ivanti Sentry versions 9.18. 9.17, 9.16 and older versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:mobileiron_sentry:*:*:*:*:*:*:*:*	-
Ivanti Sentry Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831	✗	WinRAR version 6.22 and older versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*:*:*	DarkMe, GuLoader, and Remcos RAT
WinRAR Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter	Update WinRAR version to 6.23 or later versions

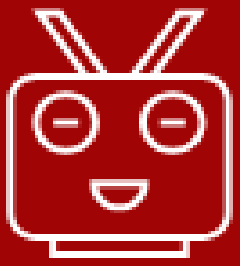
CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-47966	✗	Zoho ManageEngine	Lazarus Group
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_access_manager_plus:*:*:*:*:*:*:*:*	QuiteRAT, CollectionRAT
Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter	https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32315	✗	Openfire versions: 3.10.0 - 4.7.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:igniterealtime:openfire:*:*:*:*:*:*:*:*	-
Ignite Realtime Openfire Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1202: Indirect Command Execution, T1059: Command and Scripting Interpreter, T1505: Server Software Component	Upgrade Openfire versions to 4.6.8, 4.7.5, 4.8.0 or newer versions Link: https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Carderbee	Unknown	-	Asia
	MOTIVE		
	Financial Crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	-	PlugX (aka Korplug)	-
TTPs			
T1129: Shared Modules, T1543.003: Windows Service, T1547.008: LSASS Driver, T1027: Obfuscated Files or Information, T1036: Masquerading, T1070.004: File Deletion, T1112: Modify Registry, T1056: Input Capture, T1012: Query Registry, T1018: Remote System Discovery, T1082: System Information Discovery, T1518.001: Security Software Discovery, T1071: Application Layer Protocol, T1095: Non-Application Layer Protocol, T1105: Ingress Tool Transfer, T1573: Encrypted Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 CosmicBeetle	Unknown	Hospital, Hospitality, Insurance, Government, Entertainment, Education	Thailand, Israel, Poland, Brazil, Turkey, Mexico
	MOTIVE		
	Financial gains		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMW ARE**	**AFFECTED PRODUCTS**
	CVE-2020-1472	Scarab Ransomware, Spacecolon	Microsoft Netlogon
TTPs			
T1595.002: Vulnerability Scanning, T1583.001: Domains, T1587.001: Malware, T1587.003: Digital Certificates, T1190: Exploit Public-Facing Application, T1059.003: Windows Command Shell, T1059.001: PowerShell, T1059.005: Visual Basic, T1053.005: Scheduled Task, T1133: External Remote Services, T1547.001: Registry Run Keys / Startup Folder, T1136.001: Local Account, T1543.003: Windows Service, T1078.003: Local Accounts, T1140: Deobfuscate/Decode Files or Information, T1070.001: Clear Windows Event: Logs, T1003.001: LSASS Memory, T1082: System Information Discovery, T1115: Clipboard Data, T1071.001: Web Protocols, T1041: Exfiltration Over C2 Channel, T1095: Non-Application Layer Protocol, T1529: System: Shutdown/Reboot, T1486: Data Encrypted for Impact			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
Lazarus Group (aka Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, Diamond Sleet)</td><td>North Korea</td><td rowspan="2">Healthcare, IT, Critical Infrastructure</td><td rowspan="2">Europe and the U.S.</td></tr>
<tr><td>MOTIVE
Information theft and espionage, Sabotage and destruction, Financial crime</td></tr>
<tr><td>TARGETED CVEs
CVE-2022-47966</td><td>ASSOCIATED ATTACKS/RANSOMWARE
QuiteRAT, CollectionRAT</td><td>AFFECTED PRODUCT
Zoho ManageEngine</td></tr>
<tr><td colspan="4">TTPs
T1059: Command and Scripting Interpreter, T1574.002: DLL Side-Loading, T1497: Virtualization/Sandbox Evasion, T1056: Input Capture, T1018: Remote System: Discovery, T1082: System Information: Discovery, T1518.001: Security Software: Discovery, T1087.002: Domain Account, T1071: Application Layer Protocol, T1095: Non-Application Layer: Protocol, T1105: Ingress Tool Transfer, T1574: Hijack Execution Flow</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **six exploited vulnerabilities** and block the indicators related to the threat actors **Carderbee**, **CosmicBeetle**, **Lazarus Group** and **Cuba Ransomware**, **BUGHATCH**, **BURNTCIGAR**, **Akira Ransomware**, **PlugX**, **DarkMe**, **GuLoader**, **Remcos RAT**, **Scarab Ransomware**, **Spacecolon**, **QuiteRAT**, and **CollectionRAT**.

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 **six exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Carderbee**, **CosmicBeetle**, **Lazarus Group** and **Cuba Ransomware**, **BUGHATCH**, **BURNTCIGAR**, **Akira Ransomware**, **PlugX**, **DarkMe**, **GuLoader**, **Remcos RAT**, **Scarab Ransomware**, **Spacecolon**, **QuiteRAT**, and **CollectionRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

Cuba Ransomware Targets U.S. with Veeam Exploit

Ivanti Addressed A New Zero-Day Flaw in Ivanti Sentry

Data Center Vulnerabilities a Ticking Time Bomb for Cloud Services

New Wave of Akira Ransomware Expands Arsenal with Cisco VPN Flaws

Carderbee APT Strikes Hong Kong with Supply Chain Attack

WinRAR Zero-Day Exploit Targeting Traders Since April

Lazarus Group Uses ManageEngine Exploit to Unlock Path for QuiteRAT

A Critical Vulnerability in Openfire Admin Console Actively Exploited in the Wild

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 been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Cuba Ransomware	SHA256	8a8cb6bd09ef535bfa09bee2678e0c75a0216b0cebd8fda5c9a6f9735822e329, c6753d4cfe9072acce9c0a6fc84a15bd582d66d5e0a3a65c36c6a3ba05b80a65, 7af49e468b3b2cc75b25ebcd711294373714585dca56196ed08430ba2fc849bd, 20c596d73812a9e9798e56cd6857451cad4686ed9212a40087d5a9fd9ab2532, a059ec5278a63614d358a743774bfb380dea1b370d98961049e6ba0ed754b234, 0910d1d5d0efa08c295f777551ec787511ab7625f0d08fed6d0a5c9d6d6b963e, 65a60352271ce7ee4934967173ab68896726fe8e922e39fd2a399d468657d2a5, 1cde997078f553ab9dbb0d94f948a26fbf4d3d3a20e801677d88daeb1dfb9e66, 81a22a4224f71bd66a89f2778b5842957b313ee5593c7c3e428d7a22507cda67
BUGHATCH	SHA256	58ba30052d249805caae0107a0e2a5a3cb85f3000ba5479fafb7767e2a5a78f3
BURNTCIGAR	SHA256	1c2d7f19f8c12e055e1ba8cdf5334e6cb5510847783fbe36121a35ad70f09eb3

Attack Name	TYPE	VALUE
Akira Ransomware	SHA1	24e7848dab0b82b200781630e617d6ed7e6016e7, 2cde82cf7a1bc88c8fc5865cb57f31f6437f74fc, 30d49ced95cb9a0fb6526b30131501b28cbbc388, 5e6d77960065df450e0533f9a8409c7463292243, 688d67eb4ff993963c86297ab8345962334ead27, 76beb70b06cfe714c4fa250b6b2d1e5025fe3c50, 843f3ad221a9da48d82df672bd8806cc090430b5, 9180ea8ba0cdfe0a769089977ed8396a68761b40, 923161f345ed3566707f9f878cc311bc6a0c5268, 9a14a69eb279513cde2de0be538cc8d275fd34e9, bdb3fa0c50db18f7ada02b2060b4c5110016e859, db9ba4f42942b27e1690c6d8a1bbd5b9d188fe49, f070a115100559dcaf31ce34d9e809a3134b2511, f2e6853050f76517a9a7d472f3a994d0ae8411cf
	MD5	302f76897e4e5c8c98a52a38c4c98443, 431d61e95586c03461552d134ca54d16, af95fbcf9da33352655f3c2bab3397e2, c7ae7f5becb7cf94aa107ddc1caf4b03, d25890a2e967a17ff3dad8a70bfdd832, e44eb48c7f72ffac5af3c7a37bf80587
	IPv4	172.82.86.148, 195.123.234.101
	Domain	akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion
	SHA256	89f5f29cf6b5bcfc85b506fb916da66cb7fd398cf6011d58e9409c7813e1a6f3, 27009c0abd2709cd5cac4c0135b8f3bed3229b0921601638ba9e90713ede91ea, 379ef7c4f6dfae8cc0c8556861ff41930b88c7d9b107a5de10ccd194e1bda0cb, 8738ba49fcd520789569aea7bf7af890741a745c79ae2bef49b93fb46c076c2b, d371ee0aa4fa710c00173d296c999a5497a18b38c80095db68a2dc5e46ed35f7, 2a9257c6c74e37d051f78ed5abaa620b71b27fa3604798af077256a128d911bb, 3f4ceeada7ff021c30df1646437d2ab0e55997bbb281444501f6d1f4ea8fa209, fb2433beb961839b36198e242d0dedb7fa85ab3e08a1141d02874aa4235ac776, c239dadd55b55b817fda5b0c2bb062adf399a5b78a8b3280a473d3ae66f81777, 4cb8365b18b1c319d374be0b9d219144c20fb8714e9cf346e655f854d2c60170, 772eb611c9ca20b461536fd0bd87d553dcecf3f4c82e26c2378cad40bbf4b0b0, 2e2ad6392e75d5a5155498c2a76cb373d17ca3ad4ba57c6d33c623fca5e29342,

Attack Name	TYPE	VALUE
Akira Ransomware	SHA256	367e13f234a46822aa9655690f18000319123ad07a62e56bcf8bebbfbb0de7b9, 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c, 4222681314f5ffd69fe17ab2ae4b9aaa60866571fe2b53afc10f87e3738cedda, 619614cda94a4b6b185c0c122d11ef2b8b0b3e7fc94a1a5c2ff1ac49233df54b, 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33, 67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4, 7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488, 8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50, 99331170be7aa48d572728f68e52ac8d3eb3c8307cb8050ce504ef9f4624a4ba, a6cd727a18e5e2a80fbd8a51c299a2030bd5e68e4bbf136e07eb9d0b3f3bb8ce, b44b4e162de1decc9a5d3c61a045eb4776c55fccd33c9eced5b9f622faee19fa, c417a89cdc86ea6d674d2dc629ae1872b4054ac43e948e8ed60d3f3f47178598, d793aaaba1b4b34a20432b86505b851d838def0cd722b8cbdd1d08e19a08b6ee
PlugX	SHA256	041d8c3460ce0b25dc6b597a69cbe0bc95f9f281bb66e4cbcd045ea69e308777, 10e60613394aa48b99b5bbaa13df6d5209912e64612e8dd2d09d24546e09d74f, 8649235c0c4deecabf319fb0b7e4842bdac75baa221973bf9f095114c3cbb252, 8978af4528721d4e1178ab36f7d90bc5d5206610178d5491fd58105c8eaf0448, 995664972e499c9ff036241dca05d03d902916d9c5c126f27d23403288cf8144, b2f005fc3eeff7ba5f8adac02705ad271381ac1a296e716da0a8eccf13161362, 03c559361d21802ea29a2803584af1bf41ced2989cdddec694995ae193622e10, 49f98c7452670fde067ca85d51b44d8cb7109ead55fa94e2118b26716f78911b, 11be38b5e7d83ce275a39dc61bf40592131bfe8b8e22d70bd4c67395ee3679c9, 207d563033cb6c28d64b3b3ff6de64a9af510981bf82e48820cf223211a6b36b

Attack Name	TYPE	VALUE
GuLoader	SHA256	81d7b35cc9d332c69e374bb7727e3c63bc44caf1dc21a80cba841f532fdd359d, 7699f9c7977b3dff0510173ef2e9854dff1e2ede9a0b3be176a6c06cad46f6a9, 1c3898115a8187b236f40dbeb117557ab42489a2a1d1255fa0dbf12300096b73, 1c3898115a8187b236f40dbeb117557ab42489a2a1d1255fa0dbf12300096b73, 7c73489a0aa6bcabf4307d22af917a663dc8f6615312abd81806769e36232a04, 46df94d126ed67857062d22471e48b50c4bf388da1da9f544532671dcb1f4f96, 42715639c8e8557bba09d97271da711e53773311b354b802bd3136870ca2098c, e20123e0f8e42012759e848cb456c6bb60f09fcf0fc76b2494f8ce1dbb023e0b, b4d2e40296ddd8f6127f9d2ba3703b134fee350602ee9c90f6d73737a2186a86, b4d2e40296ddd8f6127f9d2ba3703b134fee350602ee9c90f6d73737a2186a86, 769e6002b8038a0a87c66347326d314fa597a228c04c9ec58e3c2a6e686da7db, 769e6002b8038a0a87c66347326d314fa597a228c04c9ec58e3c2a6e686da7db, dc3e8bcb96174f4eebeace1b2f8d1dd0e21f1113005c093d6605953e7f5d41e0, 88298b8df4baa6e0947191c55624418c9968940d5b4bee55c44d320b4bbcfb36, 7fbdcfc41f0c35738dc338732df68db6c9890f48b1281bf2f013cc892b5da202, b72134165e07293b02438e4ebf025481e11be7d5590d2714c383c216a53357c6, 97548d4f2ed2306e827adbe6d3ce84f1aca47e9a0be0c22dd0a7a053ebcd64b2, 6b91613f78377d180e0385169b9582636dabd880e7e956b2d42495d1b627e7ea, 91a0627626abd3ba900aa0c377d77da88ec4f7d24aedd09d0d9da344e46b992e, bc16b3c2eea43cd58cd903b2c9a80daecf5d0bde654f4b7cb3800d0ef152d32a, 6174c652fbbcd3fa7fb6b3c49f11304a75c089f12b20f21c5e2c05ef30d55c0e, 46df94d126ed67857062d22471e48b50c4bf388da1da9f544532671dcb1f4f96, 33f0aeb010952556d8dd51e16a4c4440278a3d7c036cd4e666b1ac8233607e1b,

Attack Name	TYPE	VALUE
GuLoader	SHA256	42715639c8e8557bba09d97271da711e53773311b354b802bd3136870ca2098c, 42715639c8e8557bba09d97271da711e53773311b354b802bd3136870ca2098c, b3441cd04205175c973de6e529b4ce95c76b42b43c9ff6cf28d22cbf4c5abf95, 1d956e3ac17a4da68760e042410f5c27818f0257e7bb20a5460c76ca37370de5, b3441cd04205175c973de6e529b4ce95c76b42b43c9ff6cf28d22cbf4c5abf95, 61ba44ffbcc11625b7685394d28fd6022bc78c9aaf4342d55db66a6163fe7a06, 040e86b9d787d3d5af074511c8aeb6a0ca11225c1ce2dccdfc6980bdaa163647, 46df94d126ed67857062d22471e48b50c4bf388da1da9f544532671dcb1f4f96, 50a055c22972c8fc0ab0a5f26afb453e630be88e9eb9c3592a137a2a7dd6a10c, 5cd77da31b20eb6c30380095e2fcc9711a305c8b1ddd9718d15149b04cae6495, 50a055c22972c8fc0ab0a5f26afb453e630be88e9eb9c3592a137a2a7dd6a10c, a37065097b533862a2432be87cb63a9dd755397439aae30a700b09e7abad0691, 3ab67edd421427d8e26c522fde52b72e0822fab92f3a4dae0b5305e2b908f15a, 3ab67edd421427d8e26c522fde52b72e0822fab92f3a4dae0b5305e2b908f15a, b4fe86bc79f2b87ee1467ba230c4f69839b7ef72df78b0ca70ed729b2a7f6936, 715f585fbea156c841e4f47a830c56842b01239ad3bc56a0f2fabe269a227aad, 0c068a91d2f44fd614d7429e9d13020d1f59031c26d5d8bf35e76cd3335f1d55, 67434f853750f35f663aea7c2a731961d02557766d0fb6492b86c5e4a155f560, a318c671ef27d19bdea95d9d20b6894a39bd156cf3ab7ff94e295117a3cdf910, df41db44dea7e6a49689e58efa4ee7f3a18ab82f77aff5cfc3fafa4ab3039956, e19c39ac680dec3b1003b2840f24976c1b86e6e09a4e27e8166df910f55ba917, ee6bfabb37ffee5c31e1de467a9b816d5d079d3867c107c7f16753c61dfc86ef, 236c73a241d229cc820b4fa2aa914403151deb84b90939ac4760460fc107dda4,

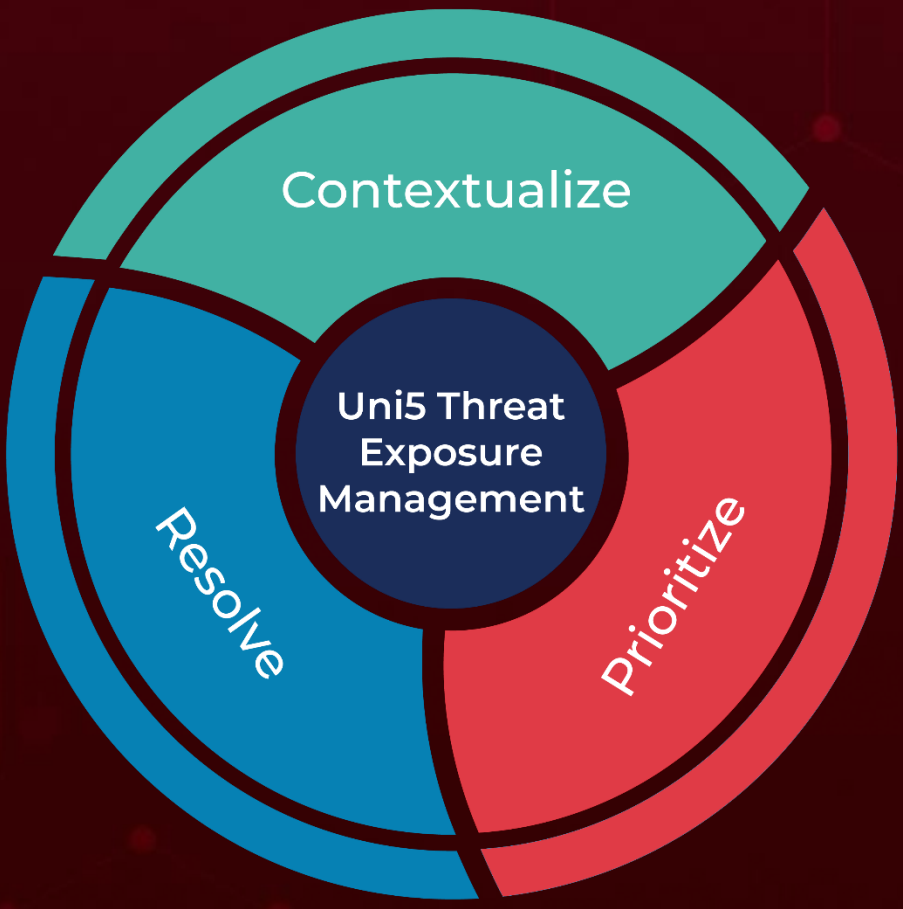
Attack Name	TYPE	VALUE
GuLoader	SHA256	236c73a241d229cc820b4fa2aa914403151deb84b90939ac4760460fc107dda4, ee6bfabb37ffee5c31e1de467a9b816d5d079d3867c107c7f16753c61dfc86ef, b48a5ebf4d21ce938606b70952e053ff15581a50d96e1e2cec000a8173edade3, b48a5ebf4d21ce938606b70952e053ff15581a50d96e1e2cec000a8173edade3
DarkMe	SHA256	a826570f878def28b027f6e6b2fcd8be1727e82666f8b65175d917144f5d0569, 7b478cd8b854c9046f45f32616e1b0cbdc9436fa078ceddb13ce9891b24b30a5, e72337c08d6b884b64fd9945c5a01557ccf40db93af866c00c48d36b6605f3a0
Remcos RAT	SHA256	08628529673070b41cd0774e0b5e1d22747cd0fc09c82b479143b538b67d976b, ca9c5b008a075bbdb57a89b0aef111458f5f9c8ee21f279a06abc481d35ba324, ec901217558e77f2f449031a6a1190b1e99b30fa1bb8d8dabc3a99bc69833784, b89e2bec5923fcd2b7c4f50f80dd5cd992a45409424a8cd1711c453dc38a2dc8, d5082b124437716d3f436aef25c69662dbed756d681e9f2a5a82d6c35fa0a7bb
Scarab Ransomware	SHA1	E2EAA1EE0B51CAF803CEEDD7D3452577B6FE7A8D, 8F1374D4D6CC2899DA1251DE0325A7095E719EDC
Spacecolon	IPV4	3.76.107[.]228, 87.251.64[.]19, 87.251.64[.]57, 87.251.67[.]163, 162.255.119[.]146, 185.170.144[.]190, 185.202.0[.]149, 193.37.69[.]152, 193.37.69[.]153, 193.149.185[.]23, 206.188.196[.]104, 213.232.255[.]131
	SHA1	40B8AF12EA6F89DB6ED635037F468AADEE7F4CA6, 1CB9320C010065E18881F0AAA0B72FC7C5F85956, EF911DB066866FE2734038A35A3B298359EDABCE

Attack Name	TYPE	VALUE
Spacecolon	SHA1	0A2FA26D6EAB6E9B74AD54D37C82DEE83E80BDD7, B916535362E2B691C6AEF76021944B4A23DDE190, 95931DE0AA6D96568ACEBC11E551E8E1305BF003, 6700AFB03934B01B0B2A9885799322307E3299D5, 4B07391434332E4F8FAADF61F288E48389BCEA08, B9CF8B18A84655D0E8EF1BB14C60763CEFFF9686
QuiteRAT	SHA256	ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6
CollectionRAT	SHA256	db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984, 773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df

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

August 28, 2023 . 8:00 AM

More at www.hivepro.com