

Date of Publication
July 22, 2024



HiveForce Labs
WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors
15 to 21 JULY 2024

Table Of Contents

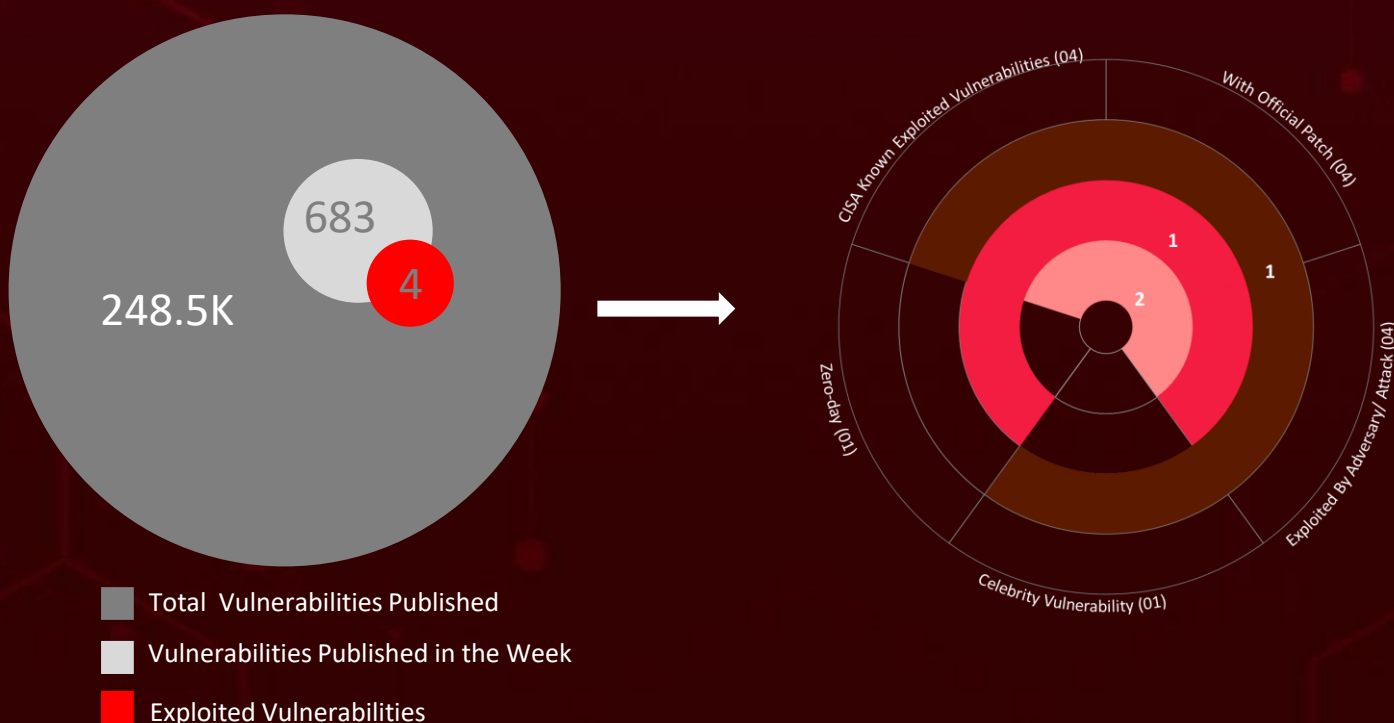
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	14
<u>Recommendations</u>	17
<u>Threat Advisories</u>	18
<u>Appendix</u>	19
<u>What Next?</u>	21

Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **five** attacks were executed, **four** vulnerabilities were uncovered, and **three** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs has identified a cyber threat actor known as **Void Banshee** exploiting the **CVE-2024-38112** vulnerability by manipulating the MHTML protocol handler to deceive Windows users into executing remote code. The APT group Void Banshee utilizes this flaw to deploy the Atlantida stealer, which is designed to exfiltrate sensitive information and achieve financial gain.

Furthermore, **EstateRansomware** a newly identified ransomware group exploiting the **CVE-2023-27532** vulnerability in Veeam Backup & Replication software to deploy file-encrypting malware and extort payments. The attack gains initial access to the target environment by brute-forcing a dormant account on a Fortinet FortiGate VPN appliance. These rising attacks present a significant and immediate threat to users globally.



High Level Statistics

5

Attacks
Executed

- [EstateRansomware](#)
- [BugSleep Backdoor](#)
- [ShadowRoot Ransomware](#)
- [Atlantida Stealer](#)
- [9002 RAT](#)

4

Vulnerabilities
Exploited

- [CVE-2023-27532](#)
- [CVE-2024-38112](#)
- [CVE-2024-36401](#)
- [CVE-2024-34102](#)

3

Adversaries in
Action

- [MuddyWater](#)
- [Void Banshee](#)
- [APT17](#)



Insights

CosmicSting

unauthenticated XXE flaw in Adobe Commerce and Magento, exploited in wild

Void Banshee

APT group appears to target professionals and students who frequently use online libraries and cloud services, capitalizing on CVE-2024-38112, deploying the Atlantida stealer for information theft and financial gains

APT17

China-linked threat actor targeted Italian companies and government entities using a variant of the 9002 RAT malware

MuddyWater

has added a novel malware BugSleep Backdoor to its arsenal, which executes commands and facilitates the transfer of files between compromised machines and C&C servers

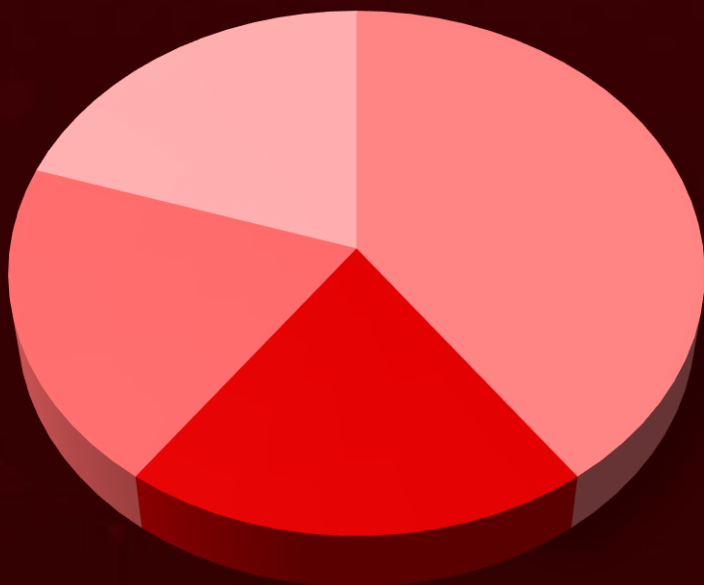
CVE-2024-36401

A critical remote code execution (RCE) vulnerability in OSGeo GeoServer GeoTools caused by the unsafe evaluation of property names as XPath expressions

EstateRansomware

exploiting a flaw in Veeam Backup & Replication software to deploy file-encrypting malware and extort payments

Threat Distribution



■ Ransomware

■ Backdoor

■ Stealer

■ RAT

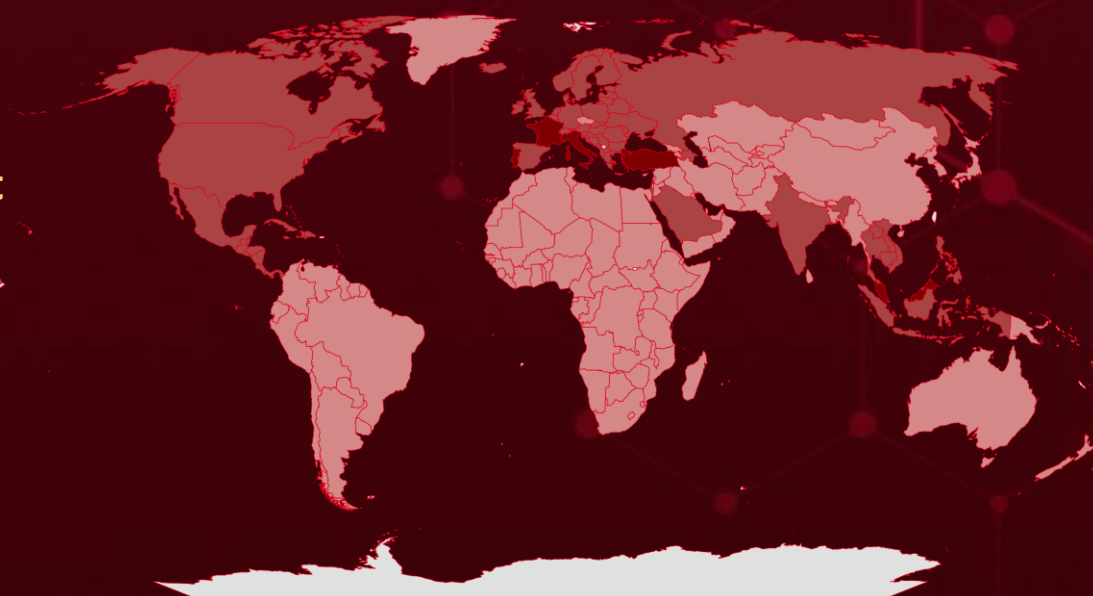


Targeted Countries

Most



Least



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

Countries
Italy
Turkey
Malaysia
Portugal
France
Timor-Leste
Netherlands
Lithuania
Bahamas
Serbia
Barbados
Antigua and Barbuda
Belarus
Mexico
Belgium
Russia
Belize
Spain
Bosnia and Herzegovina
United Kingdom
Brunei
Laos

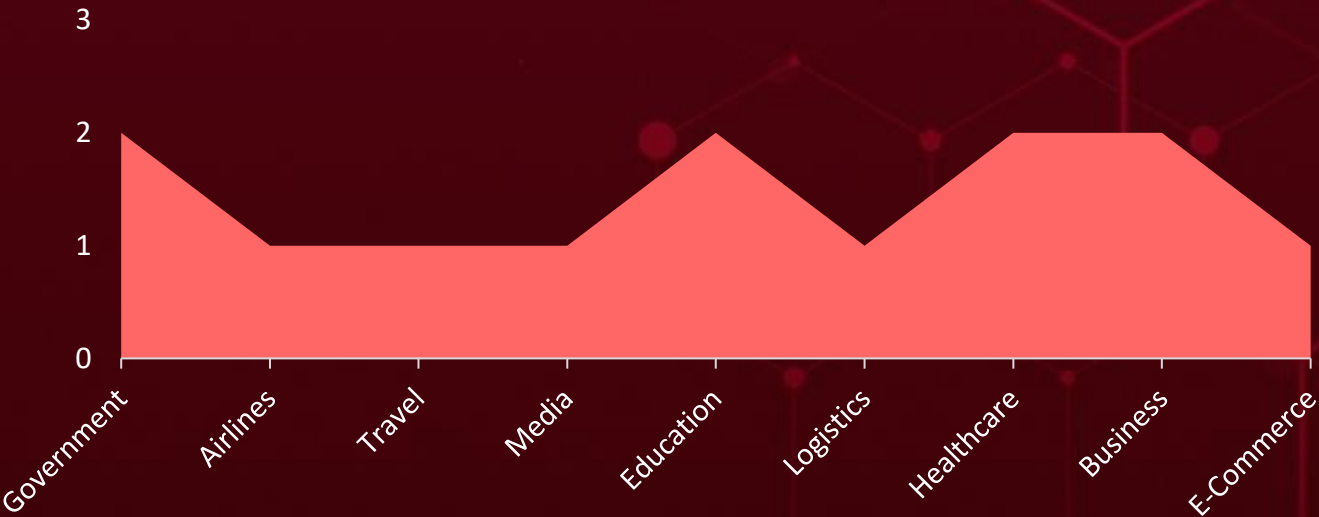
Countries
Bulgaria
Austria
Cambodia
Monaco
Canada
Azerbaijan
Costa Rica
San Marino
Croatia
Slovakia
Cuba
Switzerland
Czech Republic (Czechia)
Andorra
Denmark
Vietnam
Dominica
Jamaica
Dominican Republic
Latvia
El Salvador
Luxembourg
Estonia

Countries
Malta
Finland
Moldova
North Macedonia
Montenegro
Norway
Nicaragua
Philippines
Albania
Panama
Germany
Poland
Greece
Romania
Grenada
Saint Lucia
Guatemala
Saudi Arabia
Haiti
Singapore
Holy See
Slovenia
Honduras

Countries
Sweden
Hungary
Thailand
Iceland
Trinidad and Tobago
India
Ukraine
Indonesia
United States
Ireland
Israel
Liechtenstein
Bangladesh
Cameroon
Somalia
Iran
China
Iraq
Georgia
Comoros
Sudan
Congo
Uganda



Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1204

User Execution

T1041

Exfiltration Over C2 Channel

T1204.002

Malicious File

T1566

Phishing

T1005

Data from Local System

T1027

Obfuscated Files or Information

T1562

Impair Defenses

T1566.002

Spearphishing Link

T1082

System Information Discovery

T1036

Masquerading

T1059.005

Visual Basic

T1486

Data Encrypted for Impact

T1053

Scheduled Task/Job

T1070

Indicator Removal

T1083

File and Directory Discovery

T1059.001

PowerShell

T1113

Screen Capture

T1555

Credentials from Password Stores

T1588.006

Vulnerabilities

⚔ Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>EstateRansomw are</u>	EstateRansomware is a recently surfaced ransomware strain that gains access to victims' systems by brute-forcing dormant accounts on Fortinet FortiGate VPN. Moreover, the ransomware exploits vulnerabilities in Veeam Backup software to propagate within the compromised environments.	Abusing Fortinet VPN Service	CVE-2023-27532
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	Veeam Backup & Replication
ASSOCIATED ACTOR			PATCH LINK
-			https://www.veeam.com/kb4424
IOC TYPE	VALUE		
SHA1	cb704d2e8df80fd3500a5b817966dc262d80ddb8, 2c56e9beea9f0801e0110a7dc5549b4fa0661362		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BugSleep Backdoor	BugSleep is a backdoor designed to execute threat actors’ commands and transfer files between the compromised machine and the C&C server. BugSleep supports 11 different commands. Its core functionality includes sending file content to its C&C server, writing content into files, and running commands through a command pipe.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR			
MuddyWater			
		Steal data	-
			PATCH LINK
			-
IOC TYPE	VALUE		
SHA256	73c677dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52b9c6b30e, 960d4c9e79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809		

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
ShadowRoot Ransomware	The ShadowRoot ransomware campaign uses a downloaded payload, a Delphi binary designed to include additional components that conceal its operations and evade known cybersecurity solutions. These components culminate in executing the primary ransomware payload, “RootDesign.exe,” which methodically encrypts files on the victim’s PC and appends the “.shadowroot” extension to each compromised file.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA1	cd8fbf0dcdd429c06c80b124caf574334504e99a, 1c9629aeb0e6dbe48f9965d87c64a7b8750bbf93		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Atlantida Stealer	Atlantida stealer is an info-stealer malware targeting sensitive information from various applications, including Telegram, Steam, FileZilla, cryptocurrency wallets, and web browsers. This malware extracts stored sensitive and potentially valuable data, such as passwords and cookies, and collects files with specific extensions from the infected system's desktop. Additionally, Atlantida stealer captures the victim's screen and gathers comprehensive system information, enhancing its ability to exploit compromised systems.	Exploiting Vulnerabilities	CVE-2024-38112
TYPE		IMPACT	AFFECTED PRODUCTS
Stealer		Steal Data	Windows MSHTML
ASSOCIATED ACTOR			PATCH LINK
Void Banshee			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112
IOC TYPE	VALUE		
SHA256	6f1f3415c3e52dcdbb012f412aef7b9744786b2d4a1b850f1f4561048716c750		




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>9002 RAT (aka McRAT, Hydraq, HOMEUNIX)</u>	The 9002 RAT is a Remote Access Tool (RAT) commonly used by Advanced Persistent Threat (APT) groups to take control of a victim's machine. It is typically spread through zero-day exploits, such as those targeting Internet Explorer, and via email attachments. The infection process begins when a .LNK file is opened, triggering the execution of a PowerShell command.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT			
ASSOCIATED ACTOR			
APT17		System Compromise	PATCH LINK
IOC TYPE	VALUE		
SHA256	28808164363d221ceb9cc48f7d9dbff8ba3fc5c562f5bea9fa3176df5dd7a41e e024fe959022d2720c1c3303f811082651aef7ed85e49c3a3113fd74f229513c		




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-2023-27532</u>		Veeam Backup & Replication	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:veeam:veeam_backup_&_replication:*.~.*.*.*.*.*	EstateRansomware
Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability			
	CWE ID		ASSOCIATED TTPs
	CWE-306	T1212: Exploitation for Credential Access	https://www.veeam.com/kb4424


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-38112</u>		Windows MSHTML	Void Banshee
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:internet_explorer:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	Atlantida Stealer
Microsoft Windows MSHTML Platform Spoofing Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-668	T1204: User Execution T1218: System Binary Proxy Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-36401</u>		GeoServer	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:a:geoserver:geoserver:*.~*~*~*~*~*~*	-
OSGeo GeoServer GeoTools Eval Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-95	T1059: Command and Scripting Interpreter T1190: Exploit Public-Facing Application	https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv , https://github.com/geotools/geotools/security/advisories/GHSA-w3pj-wh35-fq8w


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-34102</u>		Adobe Commerce and Magento Open Source	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:adobe:commerce:*:*:*:*:* cpe:2.3:a:adobe:magento:*:*:open_source:*:*:* cpe:2.3:a:adobe:commerce_webhooks:*:*:*:*:*:*:*	-
CosmicSting (Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability)		ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter T1606: Forge Web Credentials	https://experienceleague.adobe.com/en/docs/commerce-operations/release-notes/security-patches/2-4-7-patches , https://experienceleague.adobe.com/en/docs/commerce-operations/upgrade-guide/modules/upgrade



Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
<div></div> <p><u>MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix)</u></p>	Iran	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation, Airlines, Journalists, Logistics	Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Qatar, Pakistan, Russia, Saudi Arabia, Sudan, Tajikistan, Tanzania, Thailand, Tunisia, Turkey, UAE, Ukraine, USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSO MWARE	AFFECTED PRODUCTS
	-	BugSleep Backdoor	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1036: Masquerading; T1053: Scheduled Task/Job; T1204: User Execution; T1082: System Information Discovery; T1105: Ingress Tool Transfer; T1027: Obfuscated Files or Information; T1059: Command and Scripting Interpreter; T1133: External Remote Services; T1574: Hijack Execution Flow; T1497: Virtualization/Sandbox Evasion; T1070: Indicator Removal; T1033: System Owner/User Discovery; T1132: Data Encoding; T1132.002: Non-Standard Encoding; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
<div></div> <div><u>Void Banshee</u></div>	-	Education	North America, Europe, and Southeast Asia
	MOTIVE		
	Information Theft & Financial Gainer		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	CVE-2024-38112	Atlantida Stealer	Windows MSHTML
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.002: Malicious File; T1218: System Binary Proxy Execution; T1218.009: Regsvcs/Regasm; T1584: Compromise Infrastructure; T1584.004: Server; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1059.001: PowerShell; T1027: Obfuscated Files or Information; T1055: Process Injection; T1560: Archive Collected Data; T1560.001: Archive via Utility; T1005: Data from Local System; T1082: System Information Discovery; T1555: Credentials from Password Stores; T1555.003: Credentials from Web Browsers; T1113: Screen Capture; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>APT17 (aka Tailgater Team, Elderwood, Elderwood Gang, Sneaky Panda, SIG22, Beijing Group, Bronze Keystone, TG-8153, TEMP.Avengers, Dogfish, Deputy Dog, ATK 2)</u></p>	China	Defense, Education, Energy, Financial, Government, High-Tech, IT, Media, Mining, NGOs, lawyers, Business	Belgium, China, Germany, Indonesia, Italy, Japan, Netherlands, Switzerland, Russia, UK, USA
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	9002 RAT	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1113: Screen Capture; T1041: Exfiltration Over C2 Channel; T1083: File and Directory Discovery; T1007: System Service Discovery; T1005: Data from Local System; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1204: User Execution; T1204.001: Malicious Link; T1204.002: Malicious File; T1656: Impersonation; T1036: Masquerading; T1562: Impair Defenses; T1056: Input Capture			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actors **MuddyWater, Void Banshee, APT17** and malware **EstateRansomware, BugSleep Backdoor, ShadowRoot Ransomware, Atlantida Stealer, 9002 RAT**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **four exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **MuddyWater, Void Banshee, APT17** and malware **BugSleep Backdoor, ShadowRoot Ransomware** in Breach and Attack Simulation(BAS).

Threat Advisories

[EstateRansomware Leverages Veeam Backup Vulnerability](#)

[MuddyWater Expands Its Arsenal with BugSleep Malware](#)

[ShadowRoot Ransomware a Menace to Turkish Enterprises](#)

[Void Banshee's Zero-Day Assault on Windows Users via Internet Explorer](#)

[Critical GeoTools RCE Flaw Exploited in Geoserver Attacks](#)

[APT17's Espionage Surge: Italian Targets Hit by 9002 RAT](#)

[Wild Exploitation of Critical Flaw in Adobe Commerce and Magento](#)

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)

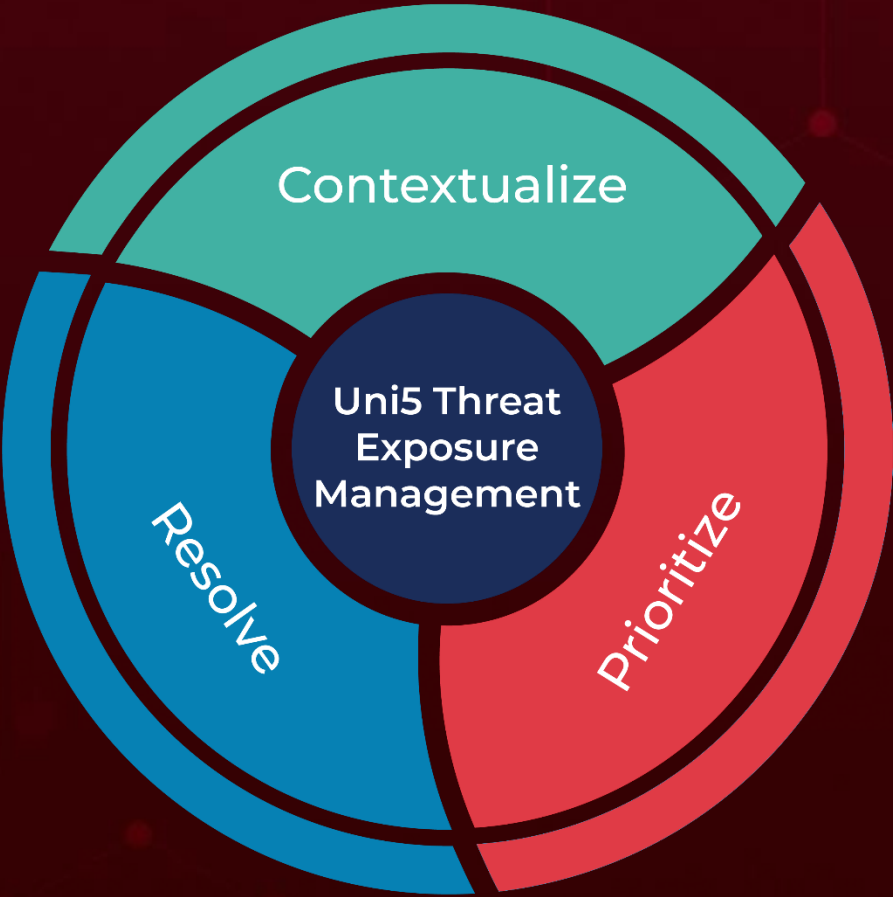
Attack Name	TYPE	VALUE
<u>EstateRansomware</u>	SHA1	cb704d2e8df80fd3500a5b817966dc262d80ddb8, 2c56e9beea9f0801e0110a7dc5549b4fa0661362, 5e460a517f0579b831b09ec99ef158ac0dd3d4fa, 107ec3a7ed7ad908774ad18e3e03d4b999d4690c
<u>BugSleep Backdoor</u>	SHA256	73c677dd3b264e7eb80e26e78ac9df1dba30915b5ce3b1bc1c83db52b9c6b30e, 960d4c9e79e751be6cad470e4f8e1d3a2b11f76f47597df8619ae41c96ba5809, b8703744744555ad841f922995cef5dbca11da22565195d05529f5f9095fbfca, 94278fa01900fdbfb58d2e373895c045c69c01915edc5349cd6f3e5b7130c472, 5df724c220aed7b4878a2a557502a5cefee736406e25ca48ca11a70608f3a1c0
<u>ShadowRoot Ransomware</u>	SHA1	cd8fbf0dcdd429c06c80b124caf574334504e99a, 1c9629aeb0e6dbe48f9965d87c64a7b8750bbf93
<u>Atlantida Stealer</u>	SHA256	6f1f3415c3e52dcdbb012f412aef7b9744786b2d4a1b850f1f4561048716c750
<u>9002 RAT</u>	SHA256	28808164363d221ceb9cc48f7d9dbff8ba3fc5c562f5bea9fa3176df5dd7a41e e024fe959022d2720c1c3303f811082651aef7ed85e49c3a3113fd74f229513c, d6b348976b3c3ed880dc41bb693dc586f8d141fbc9400f5325481d0027172436,

Attack Name	TYPE	VALUE
<u>9002 RAT</u>	SHA256	c0f93f95f004d0afd4609d9521ea79a7380b8a37a8844990e85ad4eb3d72b50c, caeca1933efcd9ff28ac81663a304ee17bbcb8091d3f9450a62c291fec973af5, de19e0163af15585c305f845b90262aee3c2bdf037f9fc733d3f1b379d00edd0

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
July 22, 2024 • 6:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com