Date of Publication
July 29, 2024

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

22 to 28 JULY 2024

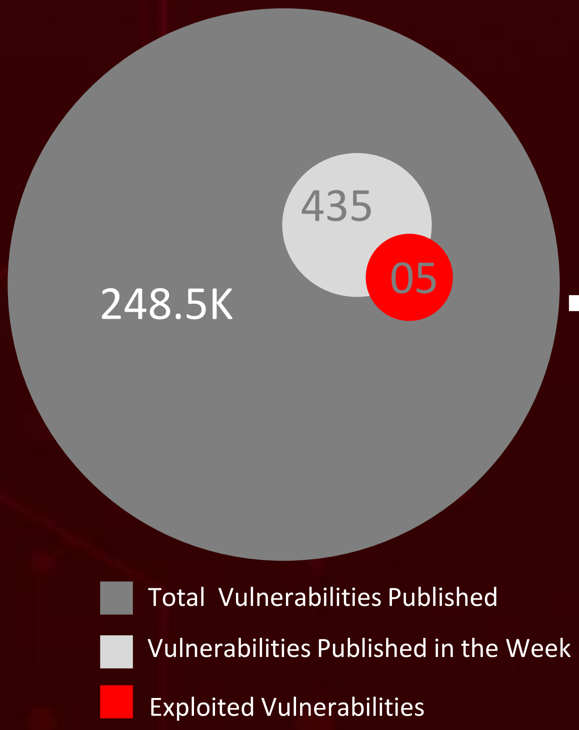
Table Of Contents

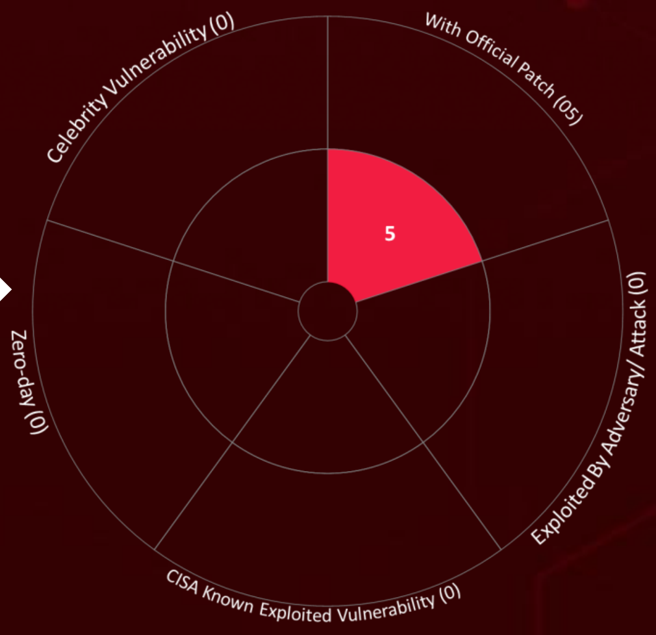
Summary

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

Furthermore, a new Linux variant of the **Play ransomware** is now targeting VMware ESXi environments, marking a departure from its previous focus on Windows systems. Additionally, a critical-severity vulnerability in Docker Engine, identified as **CVE-2024-41110**, was initially discovered and addressed in Docker Engine v18.09.1, released in January 2019. However, the fix was not incorporated into subsequent versions, leading to the reemergence of the vulnerability.

Moreover, the **EvilVideo** vulnerability specifically targeted the Telegram app for Android and was advertised for sale on a Russian-speaking XSS hacking forum by a seller named 'Ancryno.' **GhostEmperor**, a highly sophisticated Chinese-speaking cyber threat actor, has been executing advanced cyber espionage campaigns since 2020, primarily targeting entities in Southeast Asia. These escalating threats present a significant and immediate danger to users worldwide.





High Level Statistics

5
Attacks Executed

- Jellyfish Loader
- Play Ransomware
- Coroxy Backdoor
- Braodo Stealer
- Demodex Rootkit

5
Vulnerabilities Exploited

- CVE-2024-36991
- CVE-2024-41110
- CVE-2024-4879
- CVE-2024-5178
- CVE-2024-5217

1
Adversaries in Action

- GhostEmperor

Insights

Jellyfish Loader: The Asynchronous Task Master of Cybercrime

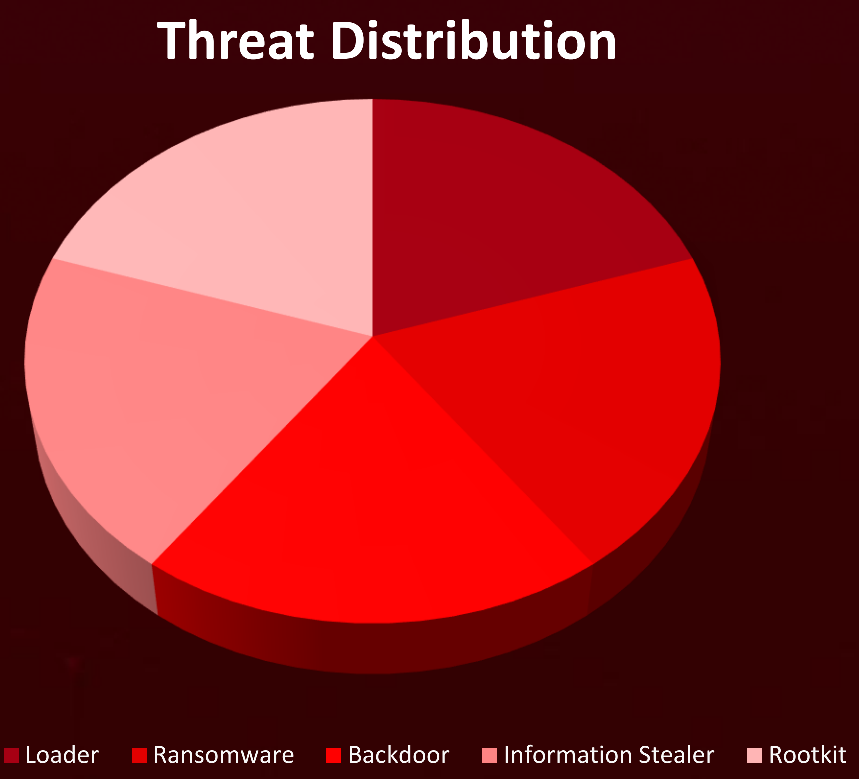
Critical ServiceNow Vulnerabilities: Remote Code Execution Risks Are on the Table

Telegram Users Beware: EvilVideo Vulnerability Uncovered in Telegram

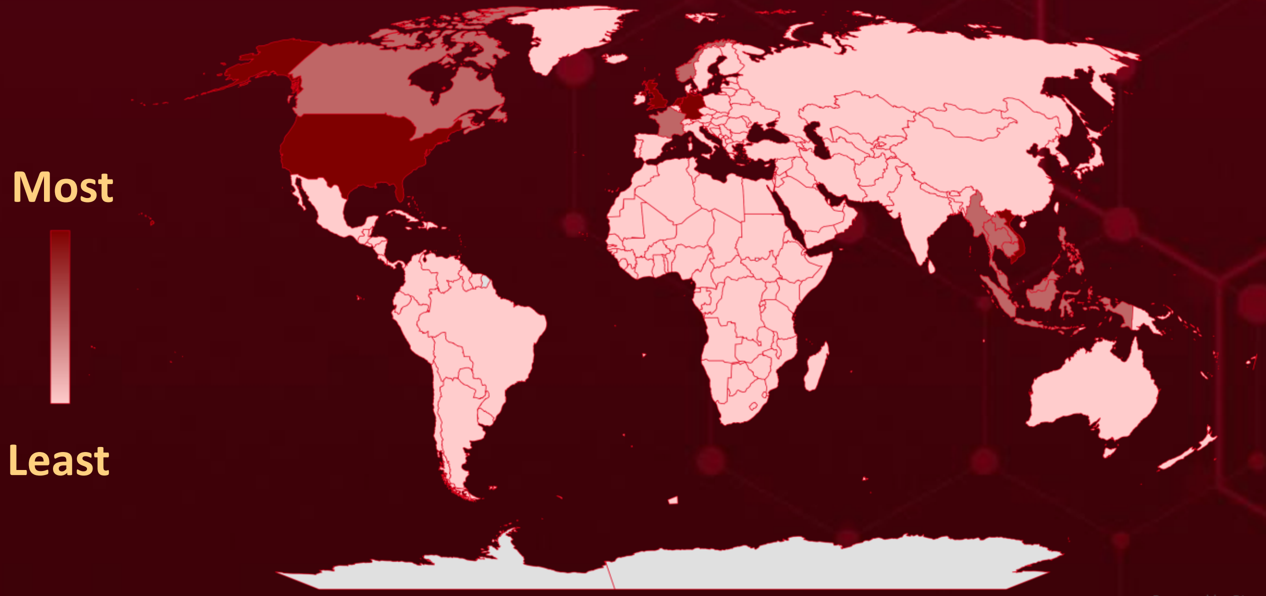
Reemerging Docker Flaw: CVE-2024-41110 A Persistent Threat

Play Ransomware Strikes Again: Now Targeting VMware ESXi Systems

CVE-2024-36991: The New Threat Lurking in Splunk's Messaging Module



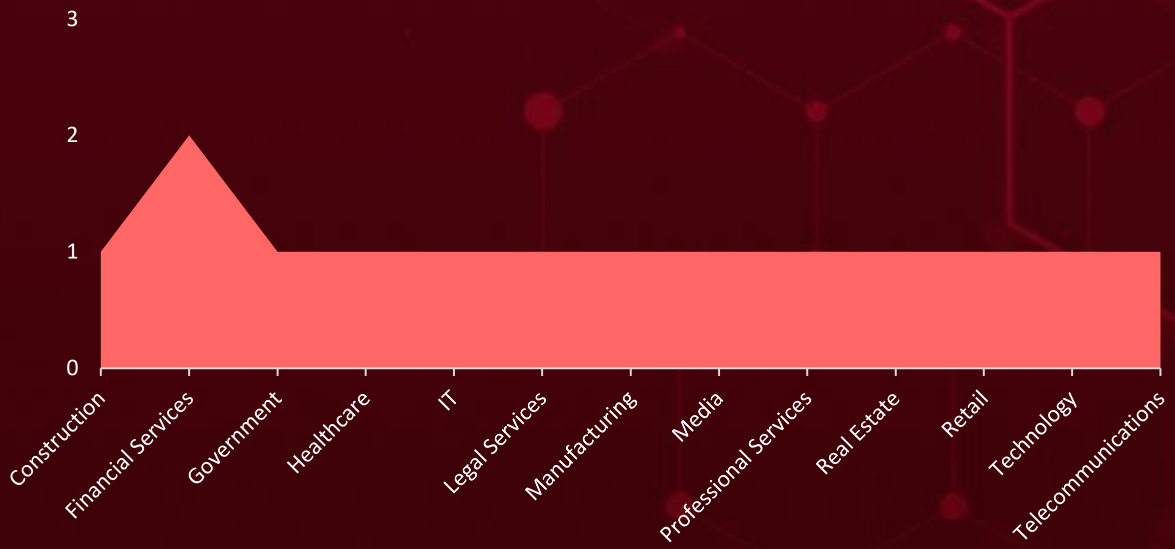
Targeted Countries



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

	Countries
🟥	Netherlands
🟥	United Kingdom
🟥	Singapore
🟥	Germany
🟥	United States
🟥	Vietnam
▨	Thailand
▨	Philippines
▨	Indonesia
▨	Cambodia
▨	France
▨	Myanmar
▨	Brunei
▨	Canada
▨	Norway
▨	Malaysia
▨	Laos
⬜	Malta
⬜	Armenia
⬜	Palau
⬜	Bahamas
⬜	Turkey
⬜	Bahrain
⬜	Nepal
⬜	Bangladesh
⬜	Saba
⬜	Barbados
⬜	Sudan
⬜	Belarus
⬜	Austria
⬜	Belgium
⬜	Mongolia
⬜	Belize
⬜	Norfolk Island
⬜	Benin
⬜	Poland
⬜	Bermuda
⬜	Samoa
⬜	Bhutan
⬜	South Africa
⬜	Bir Tawil
⬜	Tanzania
⬜	Bolivia
⬜	United Arab Emirates
⬜	Bonaire
⬜	Malawi
⬜	Bosnia and Herzegovina
⬜	Mexico
⬜	Botswana
⬜	Mozambique
⬜	Bouvet Island
⬜	Nicaragua
⬜	Brazil
⬜	Northern Mariana Islands
⬜	British Indian Ocean Territory
⬜	Paraguay
⬜	British Virgin Islands
⬜	Republic of the Congo
⬜	Afghanistan
⬜	Saint Lucia
⬜	Bulgaria
⬜	Senegal
⬜	Burkina Faso
⬜	Slovenia
⬜	Burundi
⬜	South Sudan
⬜	Akrotiri and Dhekelia
⬜	Switzerland
⬜	Cameroon
⬜	Tonga
⬜	Åland
⬜	U.S. Minor Outlying Islands
⬜	Cape Verde
⬜	Uzbekistan
⬜	Cayman Islands
⬜	Azerbaijan
⬜	Central African Republic
⬜	Maldives
⬜	Chad
⬜	Mauritania
⬜	Chile
⬜	Moldova
⬜	China
⬜	Montserrat
⬜	Christmas Island
⬜	Namibia
⬜	Clipperton Island
⬜	New Caledonia
⬜	Cocos
⬜	Nigeria
⬜	Colombia
⬜	North Macedonia
⬜	Comoros
⬜	Oman
⬜	Cook Islands
⬜	Panama
⬜	Coral Sea Islands
⬜	Argentina
⬜	Costa Rica
⬜	Puerto Rico
⬜	Croatia
⬜	Russia
⬜	Cuba
⬜	Curaçao
⬜	Cyprus
⬜	Czech Republic

Targeted Industries



TOP MITRE ATT&CK TTPs

T1083 File and Directory Discovery	**T1059** Command and Scripting Interpreter	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities	**T1041** Exfiltration Over C2 Channel
T1190 Exploit Public-Facing Application	**T1566** Phishing	**T1036** Masquerading	**T1071.001** Web Protocols	**T1573** Encrypted Channel
T1059.001 PowerShell	**T1082** System Information Discovery	**T1068** Exploitation for Privilege Escalation	**T1027** Obfuscated Files or Information	**T1105** Ingress Tool Transfer
T1070 Indicator Removal	**T1071** Application Layer Protocol	**T1204** User Execution	**T1588.005** Exploits	**T1566.001** Spearphishing Attachment

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Jellyfish Loader	Jellyfish Loader is a .NET-based shellcode loader engineered for malicious purposes. It distinguishes itself by using asynchronous task method builders to execute code, securely gather and transmit system information, and prepare for the execution of additional malicious code delivered by the C&C server.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Information Theft, Resource Hijacking	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
MD5	e577fa8e0491fe027bc4da86a01f64ea		
SHA1	9ff473df01487ca59d6426c8fddf77a1c27b2437		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Play Ransomware	A new Linux variant of the Play ransomware that targets VMware ESXi environments, marking a shift from its previous focus on Windows systems. This ransomware employs advanced evasion techniques and is linked to the Prolific Puma group, enhancing its operational capabilities. It encrypts critical files and disrupts business operations by leaving ransom notes.	Valid credentials or Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Information Theft, Compromise Infrastructure, Financial Loss	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA1	2a5e003764180eb3531443946d2f3c80ffcb2c30		

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">Coroxy Backdoor</td><td rowspan="6">The Coroxy backdoor, also called SystemBC or DroxiDat, employed by Play ransomware, has been identified as making a connection to the designated IP address. This IP address further resolves to various domains that correspond to the registered domains of Prolific Puma. The backdoor executes instructions from a remote adversary, thereby compromising the integrity of the affected system.</td><td>Downloaded from the Internet, Dropped by other malware</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><th>TYPE</th><td rowspan="4">Information Theft, Compromise Infrastructure</td><td>-</td></tr>
<tr><td>Backdoor</td><th>PATCH LINK</th></tr>
<tr><th>ASSOCIATED ACTOR</th><td rowspan="2">-</td></tr>
<tr><td>-</td></tr>
<tr><th>IOC TYPE</th><th colspan="3">VALUE</th></tr>
<tr><td>SHA256</td><td colspan="3">872b07b4a322a8fd471d076c55c2231c26c011891f90821e839ae3604cc52de5</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">Braodo Stealer</td><td rowspan="6">Braodo Stealer is a Python-based malware that has been targeting users since early 2024. It spreads through phishing and spear-phishing emails, using GitHub and a Singapore-based VPS server to host and distribute its malicious code. The malware exfiltrates internet browser data through Telegram bots.</td><td>Spear Phishing</td><td>-</td></tr>
<tr><th>IMPACT</th><th>AFFECTED PRODUCTS</th></tr>
<tr><th>TYPE</th><td rowspan="4">Information Theft, Stealing Credentials, Espionage, Identity Theft, Financial Loss</td><td rowspan="2">-</td></tr>
<tr><td>Information Stealer</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">8dcced38514c8167c849c1bba9c3c6ef20f219a7439d2fc1f889410e34d8f6c9,
204a8346a401f3101361c4571fe1c4bbedc9e54e4f5c181bb7c81cf843286730</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
Demodex Rootkit	The Demodex rootkit, a critical component of GhostEmperor's toolkit, operates at the kernel level, making it extremely difficult to detect and remove. This sophisticated rootkit uses advanced techniques to avoid detection, including EDR evasion and a reflective loader to execute the Core-Implant.	Exploiting zero-day vulnerabilities in Internet-facing applications or Spear-phishing campaigns	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Information Theft, Financial Loss, and Compromise Infrastructure	-
ASSOCIATED ACTOR			**PATCH LINK**
GhostEmperor			-
IOC TYPE	**VALUE**		
SHA1	43f1c44fa14f9ce2c0ba9451de2f7d3dd1a208de, a59cca28205eeb94c331010060f86ad2f3d41882, bab2ae2788dee2c41065850b2877202e57369f37		

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-2024-36991	⊗	Splunk Enterprise Versions 9.2.0 to 9.2.1, 9.1.0 to 9.1.4, 9.0.0 to 9.0.9	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:splunk:splunk:*:*:*:*:enterprise:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	-
Splunk Enterprise Path Traversal Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-35	T1083: File and Directory Discovery	https://docs.splunk.com/Documentation/Splunk/9.2.2/ReleaseNotes/MeetSplunk

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-5217	⊗	ServiceNow Now Platform	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*:*:*	-
ServiceNow GlideExpression Script Input Validation Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-184	T1059: Command and Scripting Interpreter, T1588: Obtain Capabilities	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-41110	⊗	Docker Engine: Versions Prior to and v19.03.15, Versions Prior to and v20.10.27, Versions Prior to and v23.0.14, Versions Prior to and v24.0.9, Versions Prior to and v25.0.5, Versions Prior to and v26.0.2, Versions Prior to and v26.1.4, Versions Prior to and v27.0.3, Versions Prior to and v27.1.0	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:docker:docker_engine:*:*:*:*:*:*:*:*	-
Docker Engine AuthZ Plugin Bypass Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-187 CWE-444 CWE-863	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1588: Obtain Capabilities	https://github.com/docker/compose/releases/tag/v2.29.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4879	⊗	ServiceNow Now Platform	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*:*:*	-
ServiceNow UI Macros Jelly Template Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1287	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1645154

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-5178	❌	ServiceNow Now Platform	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*:*:*	-
ServiceNow SecurelyAccess API Input Validation Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-184	T1588: Obtain Capabilities, T1083: File and Directory Discovery	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648312

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5">GhostEmperor</td><td>China</td><td rowspan="3">Telecommunications and Government</td><td rowspan="3">Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Information Theft, Espionage</td></tr>
<tr><th>TARGETED CVEs</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th><th>AFFECTED PRODUCTS</th></tr>
<tr><td>-</td><td>Demodex Rootkit</td><td>-</td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1190: Exploit Public-Facing Application; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1204: User Execution; T1047: Windows Management Instrumentation; T1543: Create or Modify System Process; T1055: Process Injection; T1055.012: Process Hollowing; T1027: Obfuscated Files or Information; T1070: Indicator Removal; T1014: Rootkit; T1082: System Information Discovery; T1041: Exfiltration Over C2 Channel; T1573: Encrypted Channel</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actors **GhostEmperor,** and malware **Jellyfish Loader, Play Ransomware, Coroxy Backdoor, Braodo Stealer, Demodex Rootkit.**

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 **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **GhostEmperor,** and malware **Jellyfish Loader, Play Ransomware, Braodo Stealer** in Breach and Attack Simulation(BAS).

Threat Advisories

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
Jellyfish Loader	MD5	e577fa8e0491fe027bc4da86a01f64ea
	SHA1	9ff473df01487ca59d6426c8fddf77a1c27b2437
	SHA256	e654e97efb6214bea46874a49e173a3f8b40ef30fd0179b1797d14bcc2c2aa6c
Play Ransomware	SHA1	2a5e003764180eb3531443946d2f3c80ffcb2c30
	IPv4	108[.]61[.]142[.]190 , 45[.]76[.]165[.]129, 149[.]248[.]2[.]42
	URL	hxxp[:]//108[.]61[.]142[.]190/FX300[.]rar, hxxp[:]//108[.]61[.]142[.]190/1[.]dll[.]sa, hxxp[:]//108[.]61[.]142[.]190/64[.]zip, hxxp[:]//108[.]61[.]142[.]190/winrar-x64-611[.]exe, hxxp[:]//108[.]61[.]142[.]190/PsExec[.]exe, hxxp[:]//108[.]61[.]142[.]190/host1[.]sa
Coroxy Backdoor	SHA256	872b07b4a322a8fd471d076c55c2231c26c011891f90821e839ae3604cc52de5
	URL	hxxp[:]//108[.]61[.]142[.]190/host1[.]sa, hxxp[:]//108[.]61[.]142[.]190/1[.]dll[.]sa
	IPv4	45[.]76[.]165[.]129, 108[.]61[.]142[.]190
Braodo Stealer	SHA256	8dcced38514c8167c849c1bba9c3c6ef20f219a7439d2fc1f889410e34d8f6c9, 204a8346a401f3101361c4571fe1c4bbedc9e54e4f5c181bb7c81cf843286730

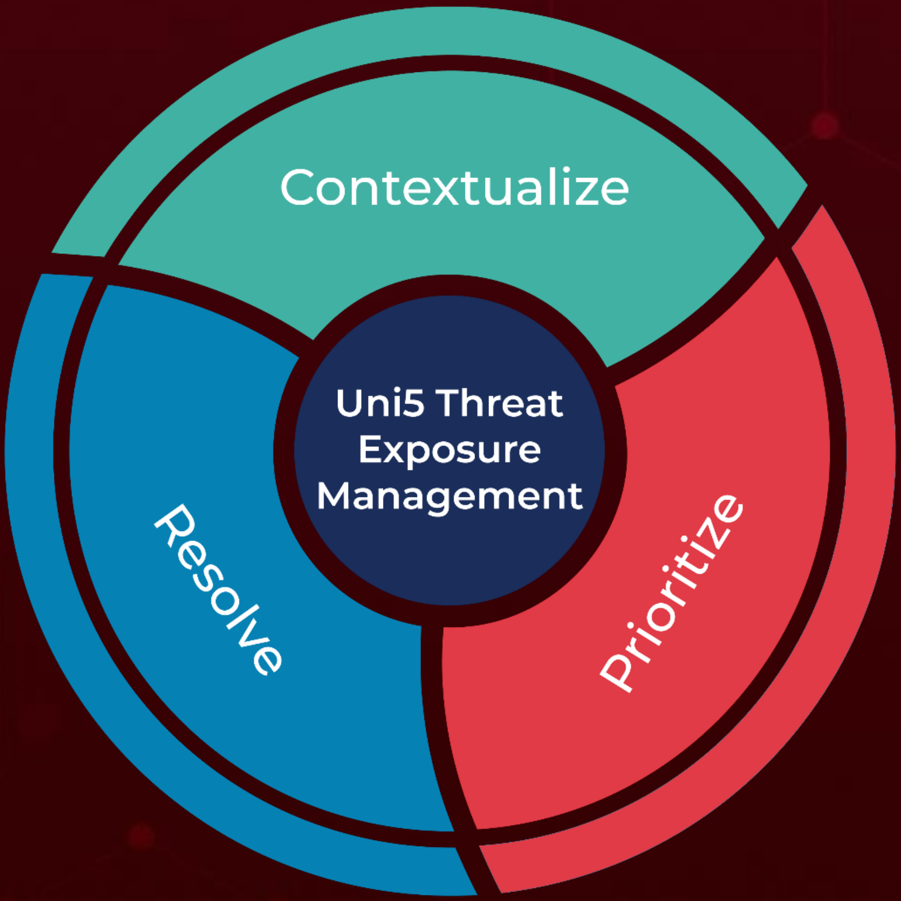
Attack Name	TYPE	VALUE
Demodex Rootkit	MD5	4bb191c6d3a234743ace703d7d518f8f, 95e3312de43c1da4cc3be8fa47ab9fa4, d8ebfd26bed0155e7c4ec2ca429c871d
	SHA1	43f1c44fa14f9ce2c0ba9451de2f7d3dd1a208de, a59cca28205eeb94c331010060f86ad2f3d41882, bab2ae2788dee2c41065850b2877202e57369f37

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

July 29, 2024 • 5:30 AM

More at www.hivepro.com