Date of Publication
September 16, 2024

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

09 to 15 SEPTEMBER 2024

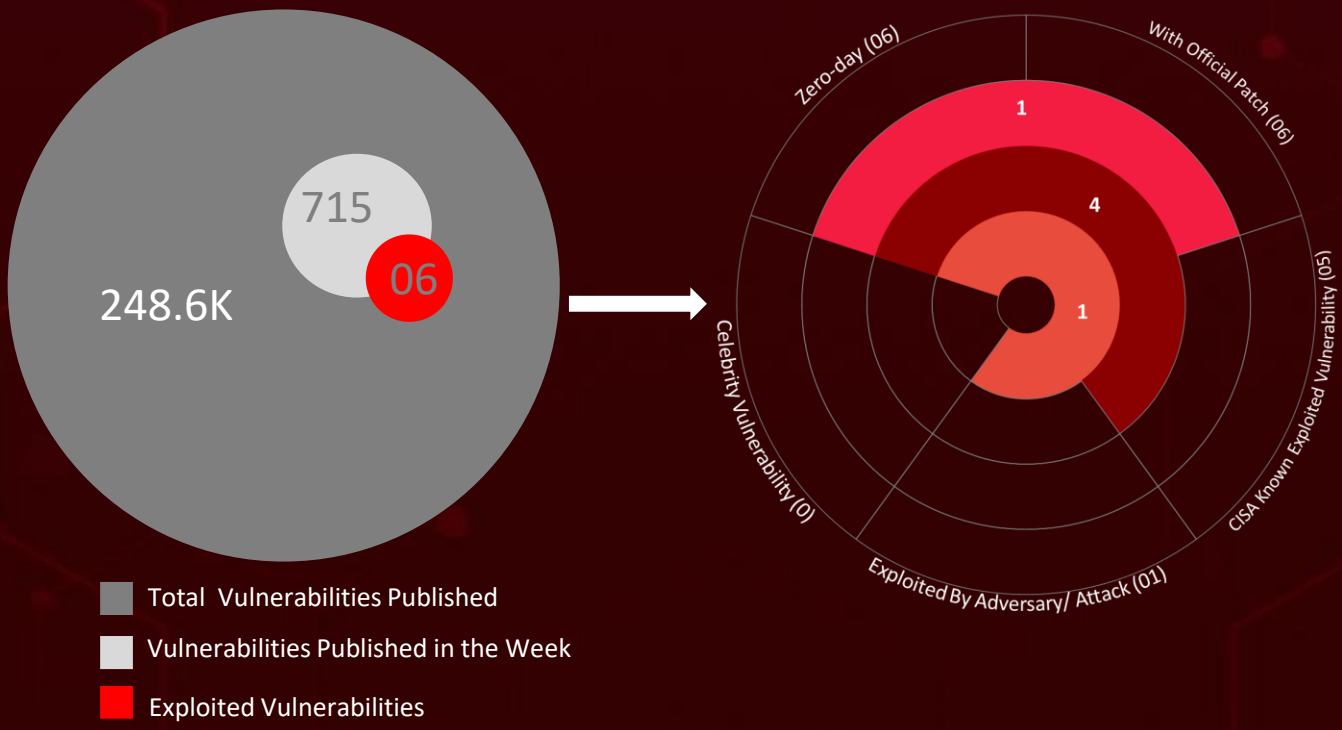
Table Of Contents

Summary

HiveForce Labs has recently made remarkable strides in exposing cybersecurity threats. In the past week alone, the lab detected **ten** executed attacks, **six** exploited vulnerabilities, and identified **five** active threat actors. These findings underscore the persistent and escalating risk of cyber intrusions.

Microsoft's September 2024 Patch Tuesday addresses **five** zero-day vulnerabilities currently exploited in the wild. **CVE-2024-41869**, a use-after-free flaw in Adobe Acrobat and Reader for Windows and macOS, poses a critical threat. This vulnerability demands immediate attention, with an active proof-of-concept exploit already circulating.

Additionally, **Fog Ransomware**, which previously targeted the education and recreational sectors, has now shifted its focus to the financial industry. The newly discovered **DragonRank** hacking group is concentrating its attacks on countries across Asia and Europe. Meanwhile, the **Blind Eagle** and **TIDRONE** threat actors remain active, engaging in espionage and intelligence-gathering operations, and posing serious threats to global security.



High Level Statistics

10
Attacks Executed

6
Vulnerabilities Exploited

5
Adversaries in Action

- BlotchyQuasar
- CXCLNT
- CLNTEND
- Fog ransomware
- DOWNBAIT
- PULLBAIT
- CBROVER
- PLUGX
- PUBLOAD
- BadIIS

- CVE-2024-38014
- CVE-2024-38217
- CVE-2024-38226
- CVE-2024-43491
- CVE-2024-43461
- CVE-2024-41869

- Blind Eagle
- TIDRONE
- Void Banshee
- Mustang Panda
- DragonRank

Insights

Cisco Closes the Gap: Two Critical Smart Licensing Vulnerabilities Fixed

Microsoft Patch Tuesday: Addresses **Five** Actively Exploited **Zero-Days** and **79** Other Flaws

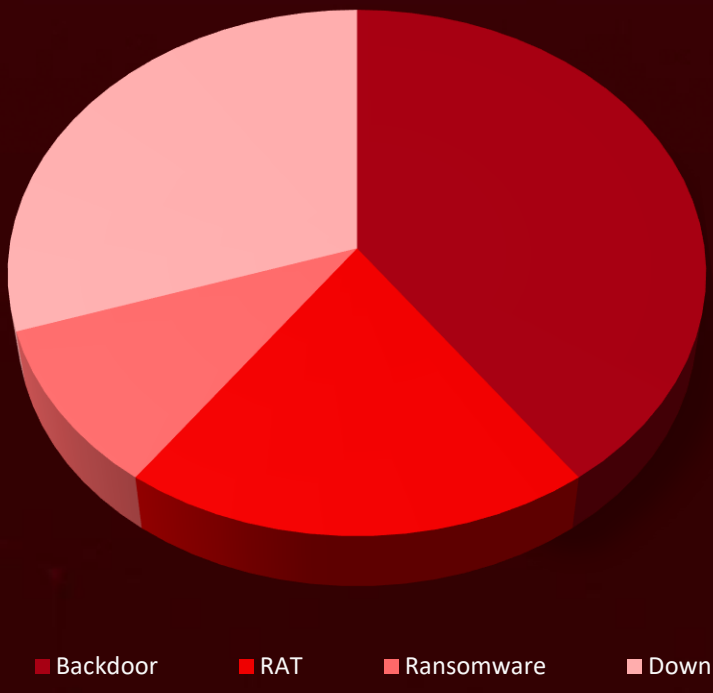
DragonRank on the Prowl: Asian and European Nations Under Fire

Adobe's Latest Fix: Zero-Day Use-After-Free Vulnerability CVE-2024-41869 Addressed

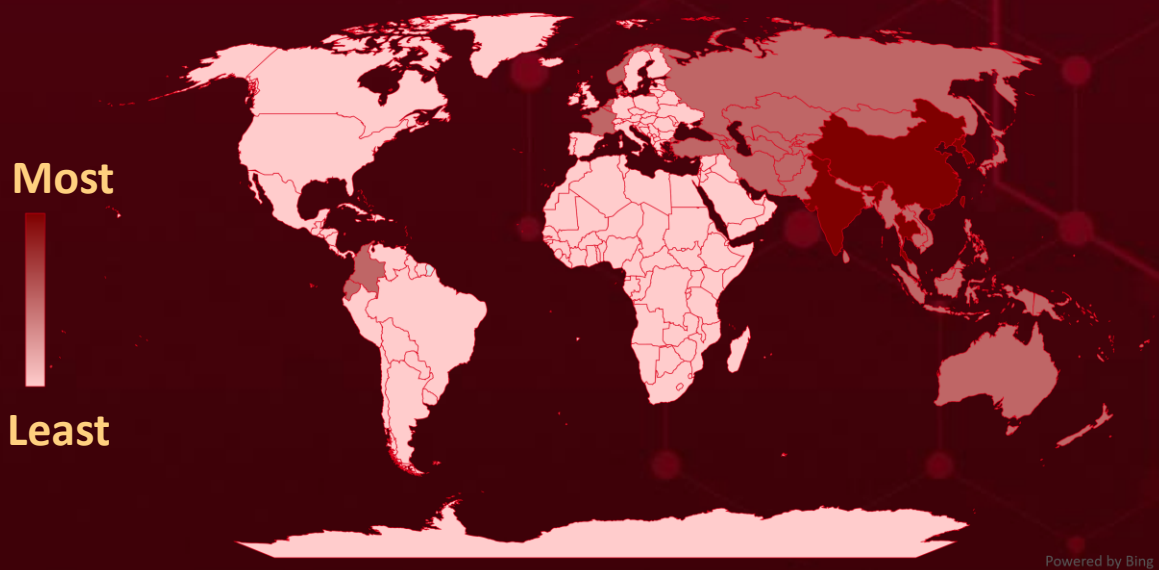
Mustang Panda's Refined Strategies: Targeting High-Value Victims with Malware Variants

Fog Ransomware Shifts Focus: **Financial Industry** in the Crosshairs

Threat Distribution

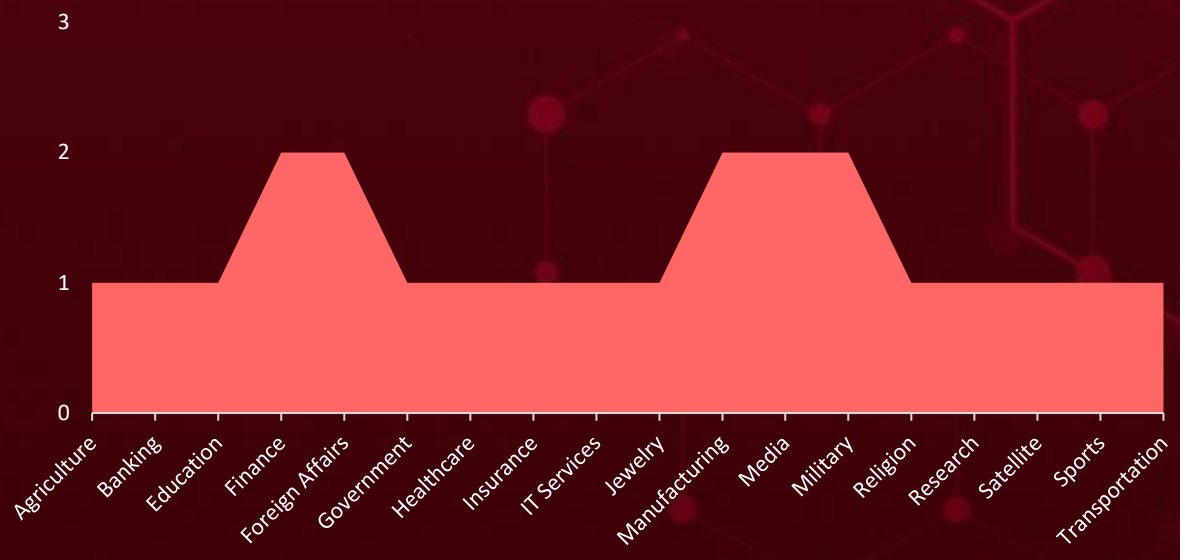


Targeted Countries



Countries	Countries	Countries	Countries
Taiwan	Vanuatu	Turkmenistan	Finland
North Korea	France	Laos	Panama
Thailand	Micronesia	Uzbekistan	Algeria
China	French Polynesia	Malaysia	Qatar
South Korea	Myanmar	Maldives	Bahamas
India	Georgia	Vietnam	Saint Pierre and Miquelon
Netherlands	Nepal	Somalia	
Tuvalu	Hong Kong	Oman	Gabon
American Samoa	New Caledonia	United Kingdom	Åland
Belgium	Palau	El Salvador	Gambia
Mongolia	Niue	Rwanda	South Ossetia
Bhutan	Papua New Guinea	Equatorial Guinea	Bahrain
Azerbaijan	Norway	Tanzania	Switzerland
Brunei	Russia	Eritrea	Germany
Australia	Bangladesh	Niger	Tokelau
Cambodia	Singapore	Estonia	Ghana
Marshall Islands	Philippines	Antigua and Barbuda	U.S. Virgin Islands
Afghanistan	Indonesia		Greece
Nauru	Samoa	Eswatini	Albania
Colombia	Iran	Senegal	Greenland
New Zealand	Solomon Islands	Ethiopia	Cameroon
Cook Islands	Japan	Sudan	Grenada
Pakistan	Sri Lanka	Falkland Islands	Canada
Denmark	Kazakhstan	Tunisia	Israel
Armenia	Tajikistan	Faroe Islands	Ukraine
Ecuador	Kiribati	Burundi	Italy
Turkey	Tonga	Austria	Uruguay
Fiji	Kyrgyzstan	North Macedonia	Egypt

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1547** Boot or Logon Autostart Execution	**T1068** Exploitation for Privilege Escalation
T1566 Phishing	**T1071.001** Web Protocols	**T1204** User Execution	**T1055** Process Injection	**T1547.001** Registry Run Keys / Startup Folder
T1574.002 DLL Side-Loading	**T1574** Hijack Execution Flow	**T1190** Exploit Public-Facing Application	**T1203** Exploitation for Client Execution	**T1588.005** Exploits
T1586 Compromise Accounts	**T1562.001** Disable or Modify Tools	**T1553.005** Mark-of-the-Web Bypass	**T1041** Exfiltration Over C2 Channel	**T1027** Obfuscated Files or Information

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlotchyQuasar	BlotchyQuasar malware is a variant of QuasarRAT. It enables keylogging, browser data theft, and surveillance of financial transactions.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Information Theft, Compromise Infrastructure, Financial Gains	-
ASSOCIATED ACTOR			**PATCH LINK**
Blind Eagle			-
IOC TYPE	**VALUE**		
MD5	b83f6c57aa04dab955fadcef6e1f4139		
SHA1	a68cac786b47575a0d747282ace9a4c75e73504d		
SHA256	ec2dd6753e42f0e0b173a98f074aa41d2640390c163ae77999eb6c10ff7e2ebd		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CXCLNT	CXCLNT acts as a backdoor, enabling communication between the compromised system and the command-and-control (C&C) server. It supports basic file upload and download capabilities, as well as features for erasing traces, gathering victim information, and downloading additional portable executable (PE) files for further execution.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft, Compromise Infrastructure	Windows
ASSOCIATED ACTOR			**PATCH LINK**
TIDRONE			-
IOC TYPE	**VALUE**		
SHA256	f13869390dda83d40960d4f8a6b438c5c4cd31b4d25def7726c2809ddc573dc7, 19bbc2daa05a0e932d72ecfa4e08282aa4a27becaabad03b8fc18bb85d37743a, 0d91dfd16175658da35e12cafc4f8aa22129b42b7170898148ad516836a3344f, 1f22be2bbe1bfcda58ed6b29b573d417fa94f4e10be0636ab4c364520cda748e		

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
CLNTEND	CLNTEND serves as a remote shell, providing attackers with full control over the infected system. It communicates with the C&C server using multiple protocols.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Compromise Infrastructure	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
TIDRONE			
IOC TYPE	VALUE		
SHA256	db600b0ae5f7bfc81518a6b83d0c5d73e1b230e7378aab70b4e98a32ab219a18, f3897381b9a4723b5f1f621632b1d83d889721535f544a6c0f5b83f6ea3e50b3		

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.	Compromised Virtual Private Network (VPN) credentials	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Sensitive Information Theft, Financial Loss, Compromised Infrastructure, Exfiltration of data	-
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
IPv4	85[.]209[.]11[.]227, 85[.]209[.]11[.]254, 85[.]209[.]11[.]27		

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
DOWNBAIT	DOWNBAIT is a multi-stage downloader that retrieves a decoy document from an attacker-controlled server, while the server simultaneously delivers other malware.	Spear Phishing Emails	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Compromise Infrastructure, Remote Control	-
Downloader			PATCH LINK
ASSOCIATED ACTOR			-
Mustang Panda			
IOC TYPE	VALUE		
SHA256	3b9ef9701ea2b2c1a89489ed0ed43ffabec9e22b587470899c0d5aca1a1e4302		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PULLBAIT	PULLBAIT is a lightweight shellcode that operates directly in memory. It performs further downloads and executions of additional malware.	DOWNBAIT deploys	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Compromise Infrastructure	-
Downloader			PATCH LINK
ASSOCIATED ACTOR			-
Mustang Panda			
IOC TYPE	VALUE		
SHA256	9dd62afdb4938962af9ff1623a0aa5aaa9239bcb1c7d6216f5363d14410a3369		

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
CBROVER	CBROVER is a first-stage backdoor that supports file download and remote shell execution. It is spawned using DLL side-loading techniques.	PULLBAIT deploys	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Remote Control, Infrastructure Compromise	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
Mustang Panda			
IOC TYPE	VALUE		
SHA256	d8747574251c8b4ab8da4050ba9e1f6e8dbbaa38f496317b23da366e25d3028a, 7c520353045a15571061c3f6ae334e5f854d441bab417ebf497f21f5a8bc6925		
IPv4	18[.]163[.]112[.]181		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PLUGX	PLUGX is a second-stage payload protected with RC4 and DPAPI. It injects its code into other processes that are launched with varying arguments.	Deployed by other malware, or via exploited vulnerabilities in web applications	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage, Remote Control, Infrastructure Compromise	-
RAT			PATCH LINK
ASSOCIATED ACTOR			-
Mustang Panda, DragonRank			
IOC TYPE	VALUE		
SHA256	b37b244595cac817a8f8dba24fbea208205e1d1321651237fe24fdcfac4f8ffc, de08f83a5d2421c86573dfb968293c776a830d900af2bc735d2ecd7e77961aaf,		

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">PUBLOAD (aka ClaimLoader)</td><td rowspan="6">The variant of HIUPAN spreads through removable drives to deliver PUBLOAD. PUBLOAD was used as the main control tool for most of the campaign and to perform various tasks, including executing tools such as RAR for collection and curl for data exfiltration. PUBLOAD was also used to introduce supplemental tools into the targets' environments.</td><td>HIUPAN spreads through removable drives</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="3">Information Theft, Espionage, Exfiltration</td><td>-</td></tr>
<tr><td>Downloader</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">-</td></tr>
<tr><td>Mustang Panda</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">a062fafaff556b17a5ccb035c8c7b9d2015722d86a186b6b186a9c63eeb4308a,
14a9a74298408c65cb387574ffa8827abd257aa2b76f87efbaa1ee46e8763c57,
2e44ebe8d864ae19446d0853c51e471489c0893fc5ae2e042c01c7f232d2a2c2</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">BadIIS</td><td rowspan="6">BadIIS is malware used to manipulate search engine crawlers and disrupt the SEO of affected sites. The proxy feature of BadIIS is configured to permit access to certain URL paths and to impose restrictions on specific file types based on their extensions.</td><td>Exploit vulnerabilities in web applications</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="3">Information Theft, Compromise Infarstructure</td><td>-</td></tr>
<tr><td>Backdoor</td><td>PATCH LINK</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td rowspan="2">-</td></tr>
<tr><td>DragonRank</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">157174f0b9be66e3c9090c95efdd1dd23b19e42aa671758ebac5540a173f760c,
716c14edbd08658fc72a7641913cbab451c3f947d2473fd36488b1a228d1e340,
e733b9444106ca37c3ef9e207ac6c813b787614496b275c1a455fccc3aca1c4a</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-2024-38014	✗	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:*:*:*:*:*:*:*:*	-
Windows Installer Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38217	✗	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:*:*:*:*:*:*:*:*	-
Windows Mark of the Web Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1553.005: Mark-of-the-Web Bypass, T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38226	✗	Microsoft Publisher 2016 Microsoft Office LTSC 2021 Microsoft Office 2019	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:publisher:*:*:*:*:*:*:*:*	-
Microsoft Publisher Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1553: Subvert Trust Controls, T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43491	✗	Windows 10	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
Microsoft Windows Update Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting, T1562.010: Downgrade Attack	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-41869		Acrobat DC Versions 24.003.20054 and earlier versions (Windows) 24.002.21005 and earlier versions (MacOS), Acrobat Reader DC Versions 24.003.20054 and earlier versions (Windows) 24.002.21005 and earlier versions (MacOS), Acrobat 2024 Versions 24.001.30159 and earlier versions, Acrobat 2020 Versions 20.005.30655 and earlier versions, Acrobat Reader 2020 Versions 20.005.30655 and earlier versions	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:adobe:acrobat:*:*:*:*:*:*:*:* cpe:2.3:a:adobe:reader:*:*:*:*:*:*:*:*	-
Adobe Acrobat and Reader Use After Free Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-416	T1203: Exploitation for Client Exécution, T1204: User Execution	https://helpx.adobe.com/security/products/acrobat/apsb24-70.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43461		Windows: 10 - 11 23H2, Windows Server: 2008 – 2022 23H2	Void Banshee
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Atlantida
Windows MSHTML Platform Spoofing Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-451	T1059: Command and Scripting, T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43461

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Blind Eagle (aka AguilaCiega, APT-C-36, APT-Q-98)	Colombia	Insurance, Banking Services, Financial	Colombia, Ecuador
	MOTIVE		
	Information theft, Espionage, Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	-	BlotchyQuasar RAT	-

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1056.002: GUI Input Capture; T1095: Non-Application Layer Protocol; T1583: Acquire Infrastructure; T1583.001: Domains; T1586: Compromise: Accounts; T1586.002: Email Accounts; T1587: Develop Capabilities; T1587.001: Malware; T1608: Stage Capabilities; T1608.001: Upload Malware; T1566: Phishing; T1566.002: Spearphishing Link; T1204: User Execution; T1204.002: Malicious File; T1204.001: Malicious Link; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053.005: Scheduled Task; T1562.001: Disable or Modify Tools; T1564.001: Hidden Files and Directories; T1027: Obfuscated Files or Information; T1027.003: Steganography; T1027.009: Embedded Payloads; T1027.013: Encrypted/Encoded File; T1553.005: Mark-of-the-Web Bypass; T1027.002: Software Packing; T1140: Deobfuscate/Decode Files or Information; T1056.001: Keylogging; T1056: Input Capture; T1539: Steal Web Session Cookie; T1041: Exfiltration Over C2 Channel; T1490: Inhibit System Recovery; T1036: Masquerading

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRY</th></tr>
<tr><td rowspan="4"> 
TIDRONE</td><td>Chinese-speaking threat actor</td><td rowspan="3">Military, Satellite, Drone Manufacturing Sector</td><td rowspan="3">Taiwan</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft, Espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>CXCLNT, CLNTEND</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1203: Exploitation for Client Execution; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1036: Masquerading; T1036.005: Match Legitimate Name or Location; T1040: Network Sniffing; T1212: Exploitation for Credential Access; T1083: File and Directory Discovery; T1012: Query Registry; T1057: Process Discovery; T1119: Automated Collection; T1021.001: Remote Desktop Protocol; T1071.001: Web Protocols; T1041: Exfiltration Over C2 Channel; T1082: System Information Discovery; T1070: Indicator Removal; T1543: Create or Modify System Process; T1055: Process Injection; T1560: Archive Collected Data; T1071.002: File Transfer Protocols; T1071: Application Layer Protocol; T1021: Remote Services; T1105: Ingress Tool Transfer</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Void Banshee</td><td>-</td><td rowspan="2">All</td><td rowspan="2">All</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial Gain, Information Theft,</td><td rowspan="2">ASSOCIATED ATTACKS/RANSOMWARE</td><td rowspan="2">AFFECTED PRODUCTS</td></tr>
<tr><td>TARGETED CVEs</td></tr>
<tr><td colspan="3">CVE-2024-43461</td><td>Atlantida</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0004: Privilege Escalation; TA0042: Resource Development; TA0005: Defense Evasion; TA0002: Execution; T1068: Exploitation for Privilege Escalation; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1588.005: Exploits; T1204: User Execution; T1204.002 : Malicious File; T1036: Masquerading; T1059: Command and Scripting Interpreter; T1587.001: Malware; T1587: Develop Capabilities</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 Mustang Panda (aka Earth Preta, Stately Taurus, Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Camaro Dragon, PKPLUG)	China	Government, Military, Foreign Affair, Education	Asia-Pacific (APAC)
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	DOWNBAIT, PULLBAIT, CBROVER, PLUGX, PUBLOAD (aka ClaimLoader)	-

TTPs
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1091: Replication Through Removable Media; T1566: Phishing; T1566.001: Spearphishing Attachment; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1053.005: Scheduled Task; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1480.001: Environmental Keying; T1553.002: Code Signing; T1055: Process Injection; T1518: Software Discovery; T1518.001: Security Software Discovery; T1049: System Network Connections Discovery; T1016: System Network Configuration Discovery; T1005: Data from Local System; T1560.001: Archive via Utility; T1567.002: Exfiltration to Cloud Storage; T1048: Exfiltration Over Alternative Protocol; T1071.001: Web Protocols

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 DragonRank	China	Jewelry, media, research services, healthcare, video and television production, manufacturing, transportation, religious and spiritual organizations, IT services, international affairs, agriculture, sports, and even niche markets	Thailand, India, Korea, Belgium, Netherlands and China
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PlugX and BadIIS	Windows

TTPs
TA0007: Discovery; TA0008: Lateral Movement; TA0042: Resource Development; TA0003: Persistence; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0040: Impact; TA0011: Command and Control; TA0009: Collection; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1016: System Network Configuration Discovery; T1057: Process Discovery; T1033: System Owner/User Discovery; T1069.001: Local Groups; T1082: System Information Discovery; T1555 : Credentials from Password Stores; T1505.003: Web Shell; T1505: Server Software Component; T1021.001: Remote Desktop Protocol; T1021: Remote Services; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1055: Process Injection; T1608.006: SEO Poisoning; T1608: Stage Capabilities; T1547: Boot or Logon Autostart Execution; T1090: Proxy; T1584.004: Server; T1584: Compromise Infrastructure; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1059: Command and Scripting Interpreter; T1218.011: Rundll32; T1218.007: Msiexec T1218: System Binary Proxy Execution; T1547.001: Registry Run Keys / Startup Folder; T1113: Screen Capture

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 **Blind Eagle, TIDRONE, Void Banshee, Mustang Panda, DragonRank** and malware **BlotchyQuasar, CXCLNT, CLNTEND, Fog ransomware, DOWNBAIT, PULLBAIT, CBROVER, PLUGX, PUBLOAD, BadIIS.**

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 **Blind Eagle, TIDRONE, Void Banshee, Mustang Panda, DragonRank,** and malware **BlotchyQuasar, CLNTEND, CXCLNT, PlugX, PUBLOAD, BadIIS, CBROVER,** in Breach and Attack Simulation(BAS).

Threat Advisories

Blind Eagle's BlotchyQuasar Malware Rattles Colombian Insurance Sector

Critical RCE Vulnerability Hits Progress LoadMaster

TIDRONE's Full-Scale Attack on Taiwan's Defense Industry

Critical Vulnerability in LiteSpeed Cache Plugin Allows Website Takeover

Fog Ransomware: A Growing Threat to the Financial Industry

Cisco Smart Licensing Utility Flaws Enable Remote Privilege Escalation

Mustang Panda Reloaded with an Expanding Malware Arsenal

Microsoft's September Patch Tuesday Addresses Active Zero-Day Exploits

Adobe Addresses Critical Vulnerabilities Leading to Remote Code Execution

GitLab Fixes Multiple Flaws, Urges Immediate User Patching

DragonRank: The SEO Hackers Manipulating Search Results

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
BlotchyQuasar	MD5	b83f6c57aa04dab955fadcef6e1f4139
	SHA1	a68cac786b47575a0d747282ace9a4c75e73504d
	SHA256	ec2dd6753e42f0e0b173a98f074aa41d2640390c163ae77999eb6c10ff7e2ebd
	URL	hxxps[:]//pastebin[.]com/raw/XAfmb6xp
	Domain	edificiobaldeares[.]linkpc[.]net, equipo[.]linkpc[.]net, perfect5[.]publicvm[.]com, perfect8[.]publicvm[.]com
CXCLNT	SHA256	f13869390dda83d40960d4f8a6b438c5c4cd31b4d25def7726c2809ddc573dc7, 19bbc2daa05a0e932d72ecfa4e08282aa4a27becaabad03b8fc18bb85d37743a, 0d91dfd16175658da35e12cafc4f8aa22129b42b7170898148ad516836a3344f, 1f22be2bbe1bfcda58ed6b29b573d417fa94f4e10be0636ab4c364520cda748e,
CLNTEND	SHA256	db600b0ae5f7bfc81518a6b83d0c5d73e1b230e7378aab70b4e98a32ab219a18, f3897381b9a4723b5f1f621632b1d83d889721535f544a6c0f5b83f6ea3e50b3
Fog ransomware	File Name	advanced_port_scanner_2.5.3869(1).exe, advanced_port_scanner_2.5.3869(1).tmp, advanced_port_scanner.exe, locker.exe, rclone.exe,

Attack Name	TYPE	VALUE
Fog ransomware	File Name	SharpShares.exe, vssadmin.exe
	TOR Address	Xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gtqh26newid[.]onion
	File Path	C:\programdata\advanced_port_scanner_2.5.3869 (1).exe, C:\programdata\locker.exe, C:\ProgramData\SharpShares.exe, C:\users\xxxxx\appdata\local\temp\advanced_port_scanner_2.5.3869 (1).tmp, C:\users\xxxxx\appdata\local\temp\advanced_port_scanner.exe, C:\Windows\System32\vssadmin.exe delete shadows /all /quiet
	IPV4	85[.]209[.]11[.]227, 85[.]209[.]11[.]254, 85[.]209[.]11[.]27
DOWNBAIT	SHA256	3b9ef9701ea2b2c1a89489ed0ed43ffabec9e22b587470899c0d5aca1a1e4302
PULLBAIT	SHA256	9dd62afdb4938962af9ff1623a0aa5aaa9239bcb1c7d6216f5363d14410a3369
CBROVER	SHA256	d8747574251c8b4ab8da4050ba9e1f6e8dbbaa38f496317b23da366e25d3028a, 7c520353045a15571061c3f6ae334e5f854d441bab417ebf497f21f5a8bc6925
	IPv4	18[.]163[.]112[.]181
PLUGX	SHA256	b37b244595cac817a8f8dba24fbea208205e1d1321651237fe24fdcfac4f8ffc, de08f83a5d2421c86573dfb968293c776a830d900af2bc735d2ecd7e77961aaf, d32d7e86ed97509289fff89a78895904cf07a82824c053bfaf1bc5de3f3ba791, 046a03725df3104d02fa33c22e919cc73bed6fd6a905098e98c07f0f1b67fadb, 785d92dc175cb6b7889f07aa2a65d6c99e59dc1bbc9edb8f5827668fd249fa2e, f748b210677a44597a724126a3d97173d97840b59d6deaf010c370657afc01f8, ffa94d76d4423e43a42c7944c512e1a71827a89ad513d565f82eb8fe374ef74d
	Domain	www[.]ynsins[.]com, www[.]aihkstore[.]com, www[.]bcller[.]com
PUBLOAD	MD5	7103a25d591a051aa37424bc3a9d0733
	SHA1	3e716409192e5023328920e67512185fea89b3b1
	SHA256	a062fafaff556b17a5ccb035c8c7b9d2015722d86a186b6b186a9c63eeb4308a,

Attack Name	TYPE	VALUE
PUBLOAD	SHA256	14a9a74298408c65cb387574ffa8827abd257aa2b76f87efbaa1ee46e8763c57, 2e44ebe8d864ae19446d0853c51e471489c0893fc5ae2e042c01c7f232d2a2c2
	IPv4	103[.]15[.]29[.]17, 47[.]253[.]106[.]177
BadIIS	SHA256	3f17c66aab154212fb02fc7e329296c233aebe4abd9248204fa99c490c113a6e, 875239000f22cff75f62f9a1aa9924a8c3fea72124b0c4b31c7b3814f9dc0601, 157174f0b9be66e3c9090c95efdd1dd23b19e42aa671758ebac5540a173f760c, 716c14edbd08658fc72a7641913cbab451c3f947d2473fd36488b1a228d1e340, e733b9444106ca37c3ef9e207ac6c813b787614496b275c1a455fccc3aca1c4a, 6da823fa4950b95f9ada74e6899fb0a17c90e8f64c75be43f037461f3eee3d02, 138a48279b17d4f04368096a6f2de5d16cf3d4c4472342d3263468a69399b9b8, 0644b3ffc856eb54b53338ab8ecd22dd005ee5aacfe321f4e61b763a93f82aea, 9f7de916e513f89e8b7192bfc1daadf927110f3eafa836d036fad2b3db1a93d7, 40384f574e4ea0a1dd0876cf4af60f79a4a0b37d2a8287a795b8ab5e3427521e, 12f6b72cdf8660d94eb5d915d4eddc0ee3ae4adaa719cacad60c6f7d44e90486, 01830ea1e8bcfa8307d1d271982ef40c3451a21f7b109835b524f7a2f5f50dcc, 497e6965120a7ca6644da9b8291c65901e78d302139d221fcf0a3ec6c5cf9de3, f8eeb8a8e336eaa8723d483fd3dec802c504a7121976477a3a1d6baf44f19a12, 41cd5131c323ed643bebb245da7ec39f49efe1014bce2f3b4031ba5903fb97db, 507b77ab91f1b9c792210d7e38f4d43f16ab652f2b3008f1361cacc81817f992, feeea74325d2f389e9325a8113f185bc823dc0681b86a82982c3a3f2951750c8, fde34c06dff9a5304c394097047233930da199cce90d5a2ded3a1634dea42470, 7353030af3274ea1ab9756aaad8130fb01bcacd82fb6c6d2358ddcd060257275, 82b107aa1791a58c65e3a266981e886e24e7d6abcf076750f3e72bf4e3697aa4, a19144fad371a7fb476e5c109e1ca943245c41ea833c5e10ad4ff0db0e045869,

Attack Name	TYPE	VALUE
BadIIS	SH256	64a2785b41c0864cb630f54d749371e4ae6d916d421b96f0e394d203c066c883, 9793ea98b7fbd43f0a7273594d7b4e53338048c651c33fbfdbeb1cc275957996, 241cce3bde9379fcb18c81a856e8b67582b44e48f2134b3e750a9370bd87d707, 819500f6d820bffd4290b172eb84721eee9f4d3a5814d58a65d5a321ce3e51ab, bbdada0149cd4833a32e9f0d981e36ed13685b1f00233e7196b8432ec1589b3d, c79086813d0c846deecb7eeca238f78a662f0aec1ded892c3561522cbb39a24a, 46644577e1d6f748a7c10667eed8255de711b95018a4a75234f07040 9ba8bd8d, 05d2fde8b6141318a97cb0044c2494f009761351af9b6633ecc7e7f089879998, 4fbda60f74a4003bc93e75acffbd55520c99236052b527f920c67c18673e6bbb, 56715f3e15e8d39125e0b8cb46aaac1788fa46df4eed6881ddc5beb805679506, e3ace9e5b9a71a6a2e98daa33fd19e536d2a520a0160495b4b77ec98ad0f71d9, 611a41a2856b907abd2ebc627369aebfe0156864f2927bb1a124a3dc1e8463a0, 68a57727aa0097cfe65782961fd10c8f6fc8766c7a816f85098c3ddcf7a681be, b8e15597e1b137274f36c5e5f6f0811f041dbd5c2cd0784a2a928f6eeb68cba2, a62734619ec889e7c80bb2edc3497cd4139ebd5646db30c20e0928b264b53435, cb816863576b982fb7f14a41c63282d8f6f7a635e555353f5a75110794196f87, aa34ecb2922ce8a8066358a1d0ce0ff632297037f8b528e3a37cd53477877e47, 0b7fed82d2594b8a30772eec6eb6bf2db6a23404504535bb78c828ec1fc870f5, d52ebfa1ea0366ffbce967a652190e3eb0206e47319a19df630d37443e7d0d69, 44d95ff98bc70dca8c9bae7b7cdb2e6f94685f5fc65f2ec5cd27d069c4e4797d, d15d07add8f4f27ac87127c7d98d287f7cd0a4e5d480119dab62aa6488a70d59, 3ae3ae44712a4cc7645bbce3b54f6a431ea08d33105f78cd8f330027aa15b8cc, 4d4bcf6be29b3074d01f839d81a78880be7afc5df366d65006a5d07fc9d11fea, 00142e46c997fe7051af5667953908cc876268be30d61cd985f6265514639251,

Attack Name	TYPE	VALUE
BadIIS	SH256	6a9e2cb9592bee7dda6165fc5f8c26e6be5eb49d9de58b3251327c1d02d858b3, f0e95504b127dc1477cc1d89aac29edb8b7578ce21224ddb4d67c3b81ab19e52, c6847600910ab196652a38e94ecf592e645d43025d1d61b3710b2f715238307b, 4f8775e26d6e291905f49a2766b804c6fe8398d8acc26c11ec6a2fa96a02b3de, f5615c120aaab860b279e095a68ea0ae2ca556929395f118ad7b63af53d61f21, 2f708f00f6c2743f61b662dcc82ac908f5d86c6a87d72cc7061311d267d36e56, cefd1c9abbfe0dd44d923a24a568b3531d067ef821f40ca64c471a8aa1ff33d3, cfaec2a27dc9667443bc5be81b66e01c42ad5d83a90393e4dffc396e46f99ee7, 7553767046f15e37550f3d26a779a7e8ec3704842b97b928092602d725528a4d, 28b4c4f001517ac4a682b728fd4b9d1364da6698a84d2f1f6016937e8240219e, ad1c768f5f6bba0110be23c36ad6aaffca7f122cf3a5624934af6cf871f58bee, 80e327564d00167a6eb4ecf5a6fa0526d5261b390c46ef442673c2e69173e470, 08ee575b9cda0ea5f12c8d5132469c99cd1deebfc9514f7b8cb520348d3a9abc, 91bb5a365478de474d938690f4ee9bcd6413ef59d331829da93c9c1c88fcb771, 4995992852f5c5066581e4d63bcb9b2655d7458534c2710276587159c234e135, 2a2c1447a24fca304815b8de8b546276e37a866f0bb9390a69f92ec150855a1f, 9abc210de663efa287e09adfb6fe4196d46d4f3f4541fd4d64439adc220709ae, bcde2ee839d6bc2e18bd150f4fc21beb369f7877425efeb6e721bf954f54679d, a11626d55ee9c958d86e8c77dfe19f66cdf545fbd8743126081f46dc24446767, 95795de242b0b42d4ad0bb66ef8d9baa0c2e9e35f419fb515f023e9a33ed271e, 307f905981965afc33bc17e5053d877deb2eb4fe7b88b892d59dbae96992c161, fb07c5b6e8f0ae482d9c571611f5868179227938e1e23de3d09dcbcb14fb7972, 7c61c37356a2486cb39eef47ffb91b0e64efd2d1caa9e686ae2422dfba621e6d, 0cbc4d4941c509608c0892bf337abe6b004a2fa7c1e83e7ff23d54e323064faf, 6549dd663b597a951781f1ab6b820079f4ffeec85f396f349d5ce2f97b3f9bf6,

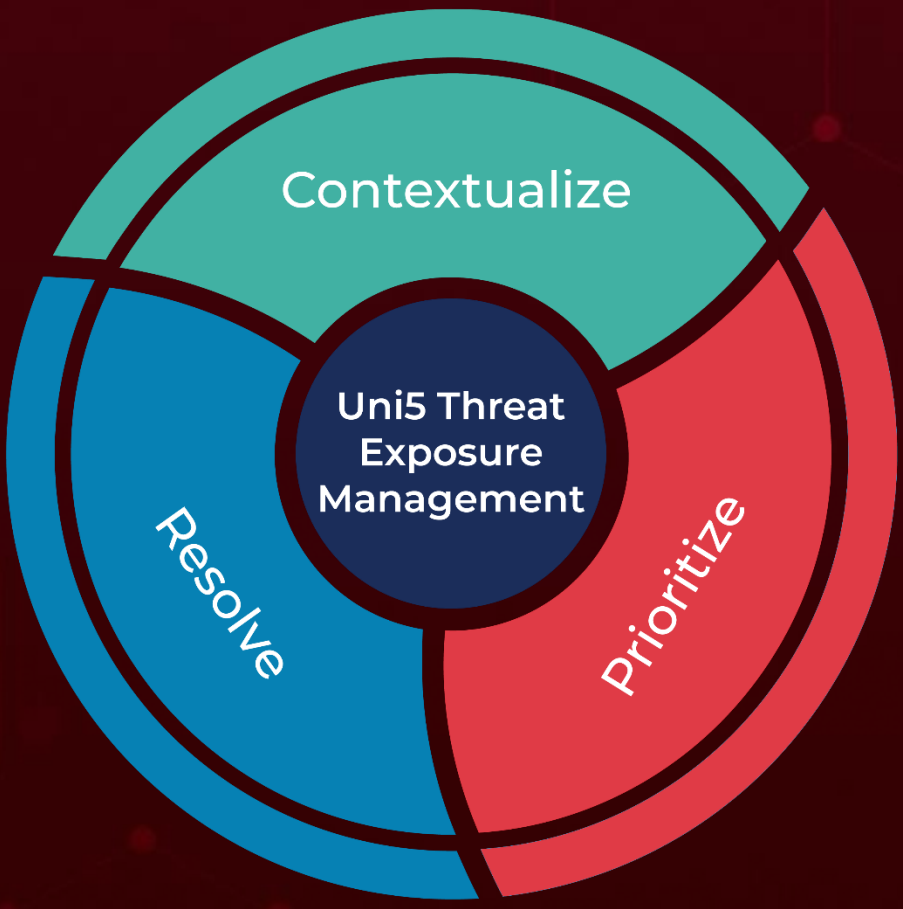
Attack Name	TYPE	VALUE
BadIIS	SHA256	165b55f40e9b488a20a7346d7b110729f0b7025ca767b0e174c6b45c9e09b42b, 364bf510c9c1d54eedbcfab6260e1ea72d9bce0c9c8dd4ea8e84e254f5c1c91c, 320da8cc3e46df550363d8a2452c2c459bf30142da065ccb29a7f2b9629ee112, c29e53de6684d771cff912a4ad57d203d1a63ff8334aa30727e76c874492ab54, 15ada077c7bd86103f729810ea33a4856bb2b39ba1c017293c492a347036c331, c9a69b28d4505b608da384e104a9046d1200aa84157adc2dd1628c823f2c6323, 3150c48438d4781d4c3ada83b7be45d76d8ac7a78f5d8d602152ac1abc3528bf, 2ea3202ca7ebd5c407409d35e71520f4782a136454487ca857afb5032660f93f, cdb7c3638fffffd42111e0a72dc959f1b49e15be7e8bb9a7bad2c5d89cc00f8b, 17de3f731a78bc740c5b57fb6d667cb68d93b5fe94076c852ddb30d7089988cc, a9c92b29ee05c1522715c7a2f9c543740b60e36373cb47b5620b1f3d8ad96bfa, 3d482e87a0e97e70c8b2e7541ba0bdee388029a5a7f26bbd62d981565cc3a91b, 59249bede0deaea326c5bb6584daf5e25c9f65ede0af7e7cd5f63761dd91b3af, 9869782b98afef7b1619cebbbe3a45ec4bc50c7138a4e8291a31f2e039d08b46

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

September 16, 2024 . 10:00 PM

More at www.hivepro.com