

Date of Publication
November 04, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

28 OCTOBER to 03 NOVEMBER 2024

Table Of Contents

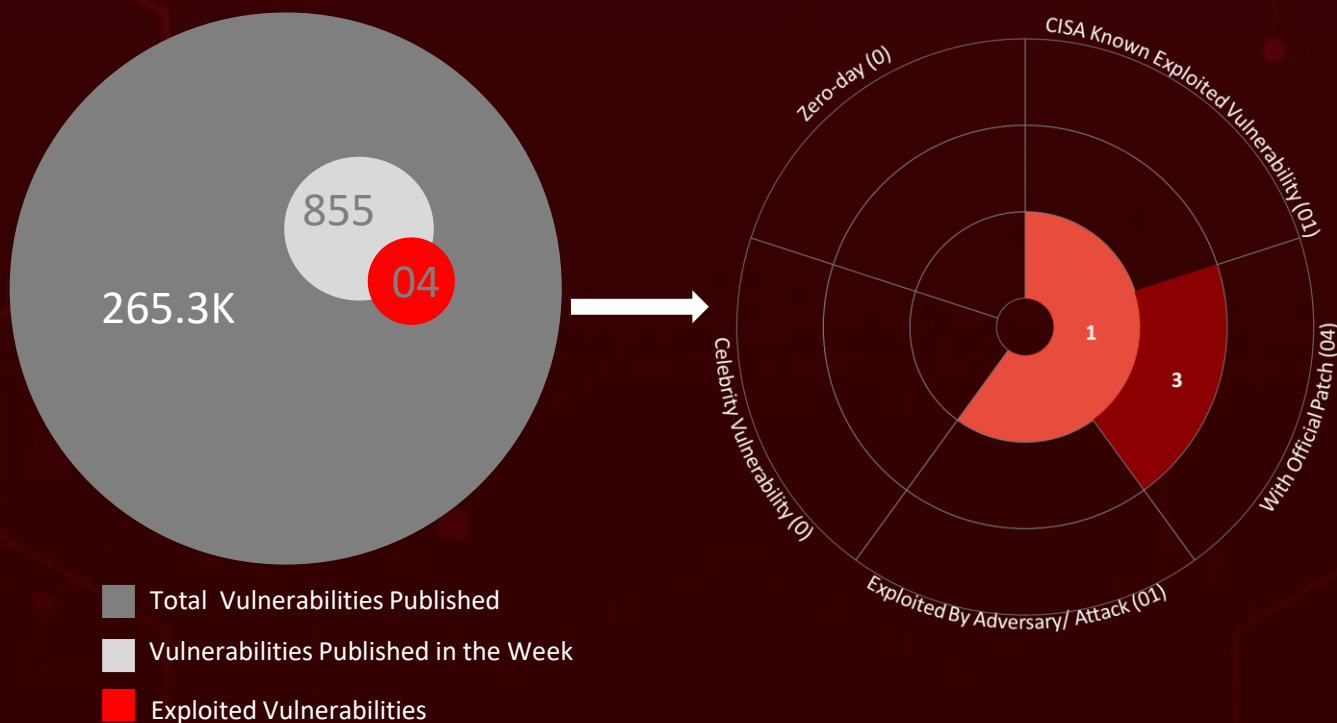
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	14
<u>Adversaries in Action</u>	16
<u>Recommendations</u>	19
<u>Threat Advisories</u>	20
<u>Appendix</u>	21
<u>What Next?</u>	24

Summary

HiveForce Labs recently reported a series of critical cybersecurity threats, underscoring the increasing frequency and sophistication of cyber incidents. Over the past week, **eleven** attacks were detected, **four** critical vulnerabilities were exploited, and **three** active threat groups were tracked, reflecting a relentless rise in cyber intrusions.

A particularly notable vulnerability involves SonicWall's SonicOS, identified as **CVE-2024-40766**. Since August 2024, attacks leveraging this access control flaw have risen, with more than **30 incidents** attributed to the **Akira and Fog ransomware** strains across various industries. Meanwhile, the **Embargo ransomware**, operating as a Ransomware-as-a-Service (RaaS) model since mid-2024, poses a **dual-platform threat** to both Windows and Linux systems.

Adding to the concerns, the **Chinese APT group Evasive Panda** employs a toolset called **CloudScout** to infiltrate organizations in Taiwan. In other developments, QNAP recently addressed a critical vulnerability (**CVE-2024-50388**) after it was exploited to breach a TS-464 NAS device during the **Pwn2Own Ireland 2024**. These growing threats highlight an urgent need for strengthened cybersecurity defenses worldwide.



High Level Statistics

11

Attacks
Executed

4

Vulnerabilities
Exploited

3

Adversaries in
Action

- [Sliver](#)
 - [Tsunami](#)
 - [Embargo](#)
 - [CloudScout](#)
 - [MgBot](#)
 - [Nightdoor](#)
 - [Pronsis](#)
 - [SUNSPINNER](#)
 - [PURESTEALER](#)
 - [Akira](#)
 - [Fog](#)
- [CVE-2024-50388](#)
 - [CVE-2024-38030](#)
 - [CVE-2024-21320](#)
 - [CVE-2024-40766](#)
- [TeamTNT](#)
 - [Evasive Panda](#)
 - [UNC5812](#)

Insights

Exposed Docker Daemons Fuel **TeamTNT's** Large-Scale Cloud Campaign

Modular and Encrypted: Evasive Panda's Silent Access to Sensitive Data

Disaster Recovery at Risk:

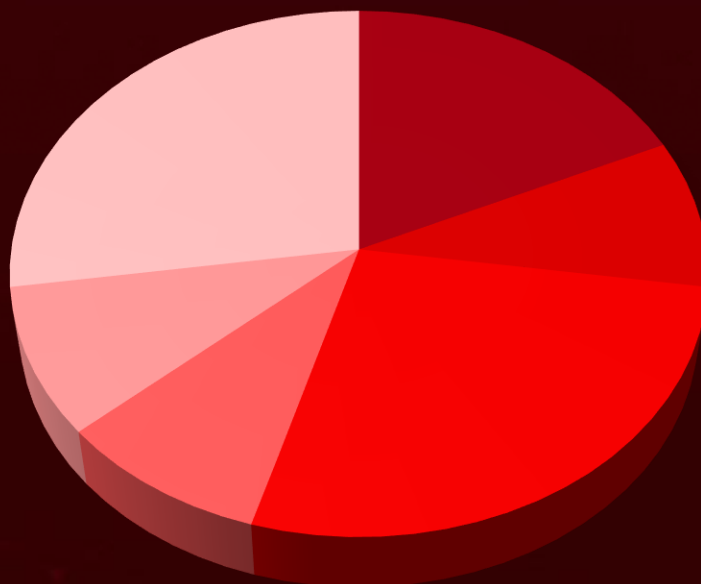
QNAP Patches Critical CVE-2024-50388 Vulnerability Exploited at Pwn2Own Ireland 2024

Credential Theft Made Easy: New Windows Themes Vulnerability Exposes NTLM Credentials to Attackers

Spike in Attacks: 30 Incidents Exploiting SonicWall CVE-2024-40766 Vulnerability Since August 2024

Civil Defense Russian-Led Telegram Profile: The Malware Threat Hiding in Plain Sight

Threat Distribution



- Backdoor
- HackTool
- Information stealer
- Loader
- Modular
- Ransomware

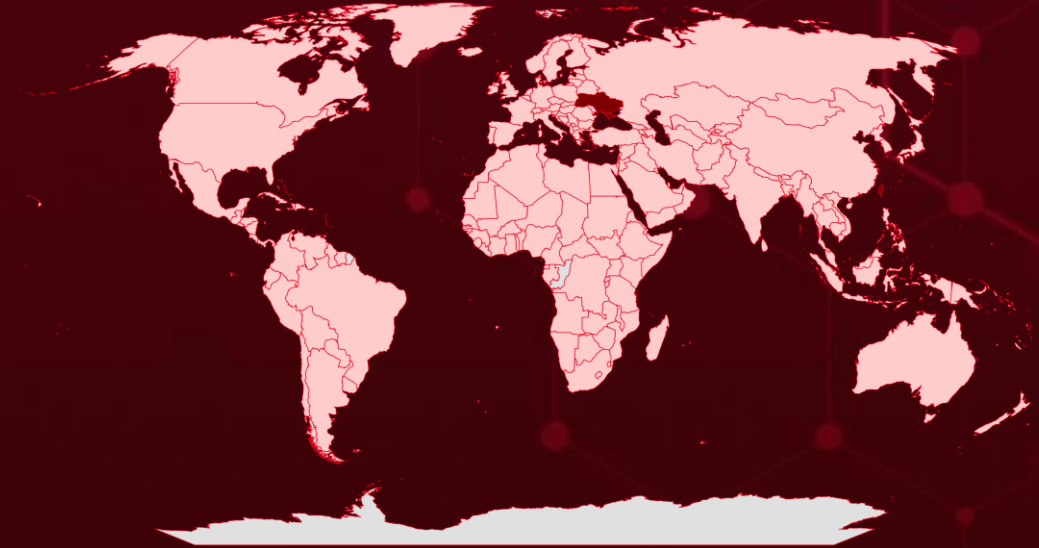


Targeted Countries

Most



Least



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

Countries	Countries	Countries	Countries
Ukraine	Barbados	Burundi	Spain
Taiwan	Morocco	Mexico	Croatia
North Macedonia	Belarus	Cabo Verde	Sudan
Zambia	Nicaragua	Mongolia	Cuba
South Korea	Belgium	Cambodia	Algeria
Andorra	Palau	Myanmar	Cyprus
Moldova	Belize	Cameroon	Togo
Angola	Qatar	Netherlands	Czech Republic
Saint Kitts & Nevis	Benin	Canada	Turkey
Antigua and Barbuda	Sao Tome & Principe	Nigeria	Denmark
Trinidad and Tobago	Bhutan	Central African Republic	Albania
Argentina	Slovenia	Oman	Djibouti
Maldives	Bolivia	Chad	Uruguay
Armenia	St. Vincent & Grenadines	Papua New Guinea	Dominica
Nauru	Bosnia and Herzegovina	Chile	Vietnam
Australia	Thailand	Poland	Dominican Republic
Peru	Botswana	China	Afghanistan
Austria	Tuvalu	Russia	DR Congo
Seychelles	Brazil	Colombia	Lithuania
Azerbaijan	Vanuatu	Samoa	Ecuador
Sweden	Brunei	Comoros	Madagascar
Bahamas	Liechtenstein	Senegal	Egypt
United Kingdom	Bulgaria	Congo	Malaysia
Bahrain	Malawi	Singapore	El Salvador
Luxembourg	Burkina Faso	Costa Rica	Mali
Bangladesh	Malta	Somalia	Equatorial Guinea
Mauritania		Côte d'Ivoire	Marshall Islands
			Eritrea

Targeted Industries



TOP MITRE ATT&CK TTPs

T1588

Obtain Capabilities

T1588.006

Vulnerabilities

T1059

Command and Scripting Interpreter

T1587

Develop Capabilities

T1036

Masquerading

T1083

File and Directory Discovery

T1587.001

Malware

T1059.003

Windows Command Shell

T1562.001

Disable or Modify Tools

T1560.001

Archive via Utility

T1071

Application Layer Protocol

T1569.002

Service Execution

T1053

Scheduled Task/Job

T1560

Archive Collected Data

T1041

Exfiltration Over C2 Channel

T1562

Impair Defenses

T1027

Obfuscated Files or Information

T1569

System Services

T1204.002

Malicious File

T1586

Compromise Accounts



Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Sliver</u>	Sliver malware is an open-source, cross-platform framework designed for adversary emulation and red team operations. Its implants facilitate Command and Control (C2) communications through various protocols, such as mTLS, WireGuard, HTTP(S), and DNS, and are dynamically compiled with unique asymmetric encryption keys for each binary. This framework allows for the execution of commands and the delivery of payloads, including in-memory execution capabilities.	Exposed docker daemons	-
TYPE		IMPACT	AFFECTED PRODUCT
HackTool		Network Compromise, Operational Disruption, Increased Attack Surface	-
ASSOCIATED ACTOR			PATCH LINK
TeamTNT			-
IOC TYPE	VALUE		
SHA256	e576938b137260200dd6a7e650b32adbf9cbe4b69199e98b06b1a0f4f3b8fff3, b0555d287f41b160d3b8a275df2c00b112e98a5db7dd83907411415e5428f7a9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Tsunami</u>	Tsunami malware is a backdoor used by attackers to exploit vulnerable services and applications. It enables the execution of shell commands, and the downloading of malicious binaries, and turns compromised machines into launch points for additional attacks.	Exposed docker daemons	-
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		Remote Command Execution, Data Theft, Malware Propagation	-
ASSOCIATED ACTOR			PATCH LINK
TeamTNT			-
IOC TYPE	VALUE		
SHA256	0f37a4b3eb939b1a1750a7a132d4798aa609f0cd862e47f641dd83c0763d8c8f		

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 CVE
<u>Embargo</u>	Embargo ransomware is a sophisticated and emerging threat, first detected in June 2024. It is believed to function as a ransomware-as-a-service (RaaS) model, enabling affiliates to deploy the malware in return for a portion of the ransom payments. Developed in Rust, a favored language for ransomware, it targets both Windows and Linux systems.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware			Windows, Linux
ASSOCIATED ACTOR			PATCH LINK
-		Data Encryption, Financial Loss, Reputational Damage	-
IOC TYPE	VALUE		
SHA256	ebffc9ced2dba66db9aae02c7ccd2759a36c5167df5cd4adb151b20e7eab173c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>CloudScout</u>	CloudScout is a modular post-compromise toolkit developed in C#, allowing the team to customize its features specifically for the target environment. This toolset can extract data from multiple cloud services by utilizing stolen web session cookies. Additionally, CloudScout integrates smoothly with MgBot, via a plugin.	Leveraging stolen session cookies	-
TYPE		IMPACT	AFFECTED PRODUCTS
Information stealer			-
ASSOCIATED ACTOR			PATCH LINK
Evasive Panda		Data Theft, Potential for Further Intrusions, Loss of Privacy	-
IOC TYPE	VALUE		
SHA256	8ebce3ceaf166fe2edab157b88aa84349d2d848242ff305cdc7edb6a34e5b72f, d7468510a0123f4ece9cb7c1636a024d3ab96cc856439a924349b00618b87ae, 1f34527a01bd3c05affe6c90aeeaa926f57efa2fac06859f8427988865ccd310		

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 CVE
<u>MgBot</u>	MgBot is the hallmark malware framework of Evasive Panda, developed in C++ to access and exfiltrate data from various cloud services. It employs the pass-the-cookie technique to hijack authenticated sessions from web browsers.	-	-
TYPE		IMPACT	AFFECTED PRODUCT
Framework		Data Theft, Account Hijacking, Increased Attack Surface	-
ASSOCIATED ACTOR			PATCH LINK
Evasive Panda			-
IOC TYPE		VALUE	
SHA1	c70c3750ac6b9d7b033addef838ef1cc28c262f3, 812124b84c5ea455f7147d94ec38d24bdf159f84, ad6c84859d413d627ac589aedf9891707e179d6c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Nightdoor</u>	Nightdoor is a sophisticated backdoor that leverages public cloud services for command-and-control communications. First detected in 2020, it establishes a reverse shell and employs anonymous pipes for input and output management. Additionally, Nightdoor can access file attributes, relocate and delete files, and execute self-uninstallation.	-	-
TYPE		IMPACT	AFFECTED PRODUCT
Backdoor		Unauthorized Access, System Control, Persistent Presence, Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
Evasive Panda			-
IOC TYPE		VALUE	
SHA1	547bd65eee05d744e075c5e12fb973a74d42438f, 348730018e0a5554f0f05e47bba43dc0f55795ac		

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 CVE
<u>Pronsis</u>	Pronsis Loader, developed in PHP, is converted into Java Virtual Machine (JVM) bytecode through the open-source JPHP project. Upon execution, Pronsis Loader triggers a complex malware delivery sequence that ultimately deploys SUNSPINNER and PURESTEALER.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCT
Loader			Windows
ASSOCIATED ACTOR			PATCH LINK
UNC5812			-
IOC TYPE		VALUE	
SHA256	f2058183f59cba1aed685d44e5c5b9d56995cfa54b38e18889c059b2bde36b3a		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>SUNSPINNER</u>	SUNSPINNER is a deceptive graphical user interface (GUI) application developed using the Flutter framework and compiled for both Windows and Android platforms. Upon execution, SUNSPINNER seeks to connect to a new "backend server" and subsequently requests map markers, which are displayed on the app's GUI.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCT
Information stealer			Windows, Android
ASSOCIATED ACTOR			PATCH LINK
UNC5812			-
IOC TYPE		VALUE	
SHA256	614e74654773e617475d519edd23380f531b60264fd7f8ed86aebf28efed4e39		

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 CVE
<u>PURESTEALER</u>	PURESTEALER is a heavily obfuscated commodity infostealer developed in .NET, specifically designed to extract browser data, including passwords and cookies, as well as information from cryptocurrency wallets and various applications like messaging and email clients. It is marketed by the "Pure Coder Team," with pricing options ranging from \$150 for a monthly subscription to \$699 for a lifetime license.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
TYPE	Information stealer	Operational Disruption, Data Theft	Windows
ASSOCIATED ACTOR			PATCH LINK
UNC5812			-
IOC TYPE	VALUE		
SHA256	d66075b2c70c3de22c9e774ad9e5f88d3d85708d1a5b17ccd4e76049c86b49b5		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
<u>Akira</u>	Akira ransomware, initially detected in March 2023, targets both Windows and Linux systems and employs a hybrid encryption approach that combines ChaCha20 and RSA algorithms. This ransomware utilizes a double extortion strategy, encrypting files while simultaneously exfiltrating sensitive data before demanding substantial ransoms, often reaching into the millions.	Exploiting CVE-2024-40766 vulnerability	CVE-2024-40766
		IMPACT	AFFECTED PRODUCT
TYPE	Ransomware	Data Encryption, Data Exfiltration, Financial Loss	SonicWall SonicOS
ASSOCIATED ACTOR			PATCH LINK
-			https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015
IOC TYPE	VALUE		
SHA256	d323d32cbd906c495a6e9fe7da01bf3e0eca407609a2693c7246346687d59f50, ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5, 88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2		




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 CVE
<u>Fog</u>	<p>Fog ransomware employs techniques like "pass-the-hash" attacks to elevate privileges, allowing access to administrator accounts. Encrypted files are generally appended with the extensions .FOG or .FLOCKED.</p>	Exploiting CVE-2024-40766 vulnerability	CVE-2024-40766
TYPE		<p>IMPACT</p> <p>Data Theft, Unauthorized Surveillance, Operational Disruption</p>	AFFECTED PRODUCT
Ransomware			SonicWall SonicOS
ASSOCIATED ACTOR			PATCH LINK
-			https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015
IOC TYPE	VALUE		
SHA256	e67260804526323484f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3		




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

Vulnerabilities Exploited


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTOR
CVE-2024-50388		QNAP HBS 3 Hybrid Backup Sync 25.1.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:a:qnap:hbs3_hybrid_backup_sync:*.:*:*:*:*:*	-
QNAP HBS 3 Hybrid Backup Sync OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1588.005: Exploits	https://www.qnap.com/en-us/security-advisory/qsa-24-41


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38030		Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*.:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*.:*:*:*:*:*	-
Microsoft Windows Themes Spoofing Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1003: OS Credential Dumping, T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38030

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21320		Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Microsoft Windows Themes Spoofing Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1003: OS Credential Dumping, T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-40766		SonicWall SonicOS SOHO (Gen 5) version 5.9.2.14-12o and older, Gen6, Firewalls Version 6.5.4.14-109n and older, Gen7 Firewalls SonicOS build version 7.0.1-5035 and older	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:sonicwall:sonicos:*:*:*:*:*	Akira and Fog Ransomware
SonicWall SonicOS Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1190: Exploit Public-Facing: Application, T1068: Exploitation for Privilege: Escalation, T1078: Valid Accounts, T1210: Exploitation of Remote Services	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015


Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRY	TARGETED REGION
 <u>TeamTNT (aka Adept Libra)</u>	-	All	Worldwide
	MOTIVE Information Theft , Espionage, Sabotage, Destruction		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCT
	-	Sliver, Tsunami	-
TTPs			
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1578: Modify Cloud Compute Infrastructure; T1578.002: Create Cloud Instance; T1211: Exploitation for Defense Evasion; T1036: Masquerading; T1552: Unsecured: Credentials; T1552.001: Credentials In Files; T1552.007: Container API; T1586: Compromise Accounts; T1586.003: Cloud Accounts; T1014: Rootkit; T1018: Remote System Discovery; T1102: Web Service; T1102.001: Dead Drop Resolver; T1071: Application Layer Protocol; T1071.004: DNS; T1090: Proxy; T1496: Resource Hijacking; T1588: Obtain Capabilities; T1588.006: Vulnerabilities			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGION
 <p><u>Evasive Panda</u> (aka <u>Bronze Highland</u>, <u>Daggerfly</u>, <u>Storm Cloud</u>, <u>StormBamboo</u>)</p>	China	Government and Religious organizations	Taiwan
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCT
-	CloudScout, MgBot, Nightdoor	Google Drive, Gmail, and Microsoft Outlook	

TTPs

TA0010: Exfiltration; TA0042: Resource Development; TA0004: Privilege Escalation; TA0002: Execution; TA0007: Discovery; TA0006: Credential Access; TA0009: Collection; TA0011: Command and Control; TA0003: Persistence; TA0005: Defense Evasion; T1543.003: Windows Service; T1082: System Information Discovery; T1114.002: Remote Email Collection; T1114: Email Collection; T1095: Non-Application Layer Protocol; T1041: Exfiltration Over C2 Channel; T1548: Abuse Elevation Control Mechanism; T1027: Obfuscated Files or Information; T1550.004: Web Session Cookie; T1550: Use Alternate Authentication Material; T1548.002: Bypass User Account Control; T1140: Deobfuscate/Decode Files or Information; T1036.005: Match Legitimate Name or Location; T1036: Masquerading; T1560.001: Archive via Utility; T1569.002: Service Execution; T1543: Create or Modify System Process; T1185: Browser Session Hijacking; T1539: Steal Web Session Cookie; T1560: Archive Collected Data; T1530: Data from Cloud Storage; T1583.004: Server; T1583: Acquire Infrastructure; T1587.001: Malware; T1587: Develop Capabilities; T1569: System Services; T1106: Native API

NAME	ORIGIN	TARGETED INDUSTRY	TARGETED COUNTRY
 <u>UNC5812</u>	Russia	Military	Ukraine
	MOTIVE		
	Information Theft, Espionage		
	TARGETED CVE	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	Pronsis Loader, SUNSPINNER, PURESTEALER	Windows and Android

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0042: Resource Development; T1071.001: Web Protocols; T1053: Scheduled Task/Job; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1083: File and Directory Discovery; T1119: Automated Collection; T1203: Exploitation for Client Execution; T1041: Exfiltration Over C2 Channel; T1036: Masquerading; T1105: Ingress Tool Transfer; T1083: File and Directory Discovery; T1204.002: Malicious File; T1587.001: Malware; T1071: Application Layer Protocol; T1588.001: Malware; T1587: Develop Capabilities; T1588: Obtain Capabilities

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 **TeamTNT, Evasive Panda, UNC5812**, and malware **Sliver, Tsunami, Embargo, CloudScout, MgBot, Nightdoor, Pronsis, SUNSPINNER, PURESTEALER, Akira, Fog**.

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

- Run 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 actors **TeamTNT, Evasive Panda, UNC5812**, and malware **Prochider Rootkit, Embargo Ransomware, CloudScout, PURESTEALER, Pronsis Loader, SUNSPINNER** in Breach and Attack Simulation(BAS).

Threat Advisories

[TeamTNT Taps Docker to Unleash Sliver Malware in Major Cloud Assault](#)

[New Embargo Rust-Based Ransomware Threat for Cross-Platform Systems](#)

[Evasive Panda's CloudScout: A Stealthy Threat to Cloud Security](#)

[QNAP Patches Critical Flaw in HBS 3 to Prevent Remote Attacks](#)

[True Face of Civil Defense: Russian Espionage Group Targets Ukraine](#)

[New Windows Themes Vulnerability Exposes NTLM Credentials](#)

[SonicWall SonicOS Flaw Allows Unauthorized Access & Firewall Crashes](#)

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>Sliver</u>	MD5	8b553728900ba2e45b784252a1ff6d17, 9dc2819c176c60e879f28529b1b08da1
	SHA1	953bd0859c86e0a3a3da52fe392a7d579a9f937b, 538cb25bfae6501d8c3c7053a293e8ca85a8dba4
	SHA256	e576938b137260200dd6a7e650b32adb9cbe4b69199e98b06b1a0 f4f3b8fff3, b0555d287f41b160d3b8a275df2c00b112e98a5db7dd8390741141 5e5428f7a9
<u>Tsunami</u>	IPv4	95[.]182[.]101[.]23
	SHA256	0f37a4b3eb939b1a1750a7a132d4798aa609f0cd862e47f641dd83c 0763d8c8f
	SHA1	37cb34a044c70d1acea5a3a91580b7bfc2a8e687
	MD5	87c8423e0815d6467656093bff9aa193
<u>Embargo</u>	SHA1	8a85c1399a0e404c8285a723c4214942a45bbff9, 612ec1d41b2aa2518363b18381fd89c12315100f
	MD5	5d55fb708834d5ccde15d36554ea63e8
	SHA256	ebffc9ced2dba66db9aae02c7ccd2759a36c5167df5cd4adb151b20e 7eab173c
<u>CloudScout</u>	SHA1	9b6a473820a72111c1a38735992b55c413d941ee, 621e2b50a979d77ba3f271fab94326ccc009b4, c058f9fe91293040c8b0908d3dafc80f89d2e38b, 4a5bcdaac0bc315edd00bb1fccd1322737bcbbeb, 67028aeb095189fdf18b2d7b775b62366ef224a9,

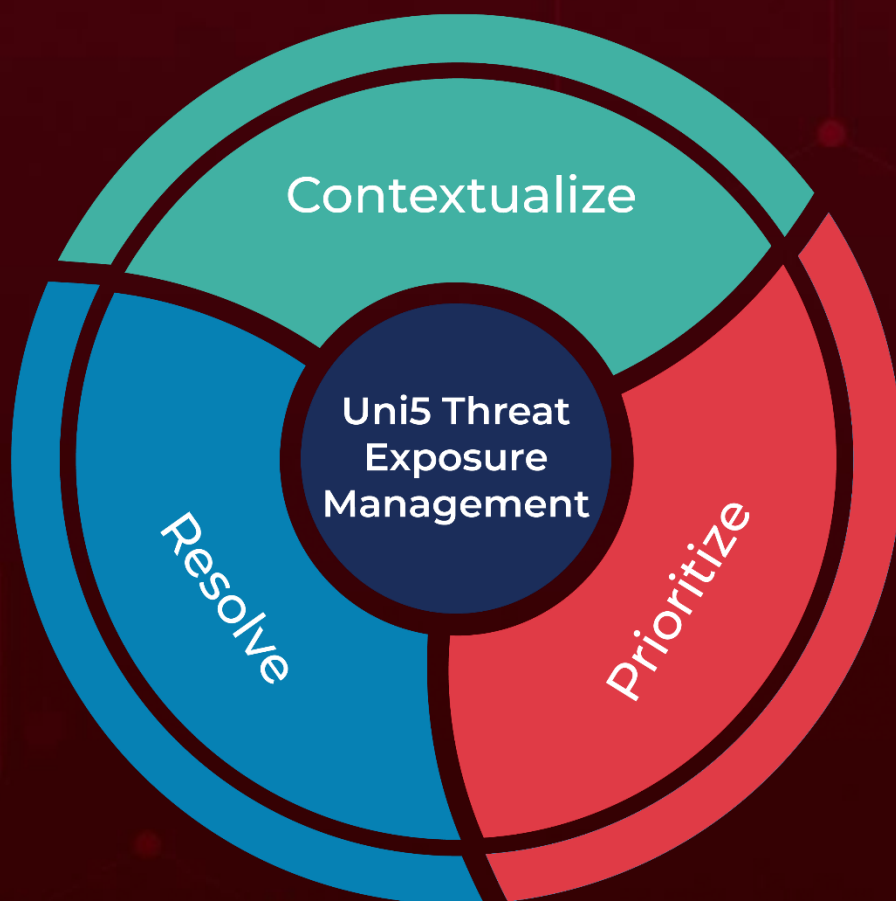
Attack Name	TYPE	VALUE
<u>CloudScout</u>	SHA1	b3556d1052bf5432d39a6068ccf00d8c318af146, 84f6b9f13cdcd8d9d15d5820536bc878cd89b3c8, 93c1c8ad2af64d0e4c132f067d369ecbebae00b7, 8eaa213ae4d482938c5a7ec523c83d2c2e1e8c0e, a1ca41fdb61f03659168050de3e208f0940f37d8
	File Name	CommonUtilities.dll, CGM.dll, CGD.dll, COL.dll
	SHA256	8ebce3ceaf166fe2edab157b88aa84349d2d848242ff305cdc7edb6a 34e5b72f, d7468510a0123f4ecea9cb7c1636a024d3ab96cc856439a924349b0 0618b87ae, 1f34527a01bd3c05affe6c90aeaea926f57efa2fac06859f842798886 5ccd310
<u>MgBot</u>	SHA1	c70c3750ac6b9d7b033addef838ef1cc28c262f3, 812124b84c5ea455f7147d94ec38d24bdf159f84, ad6c84859d413d627ac589aedf9891707e179d6c, 3dd958ca6eb7e8f0a0612d295453a3a10c08f5fe
<u>Nightdoor</u>	SHA1	547bd65eee05d744e075c5e12fb973a74d42438f, 348730018e0a5554f0f05e47bba43cd0f55795ac
<u>Pronsis</u>	MD5	d36d303d2954cb4309d34c613747ce58
	SHA1	e2de9ca2575dfe6114e688c44647a58a1ec325c2
	SHA256	f2058183f59cba1aed685d44e5c5b9d56995cfa54b38e18889c059b 2bde36b3a
<u>SUNSPINNER</u>	SHA256	614e74654773e617475d519edd23380f531b60264fd7f8ed86aebf2 8efed4e39
	MD5	4ca65a7efe2e4502e2031548ae588cb8
	SHA1	eef25d4316a0c67ed00e3d40441fcb30ccd0a9d
<u>PURESTEALER</u>	MD5	b3cf993d918c2c61c7138b4b8a98b6bf
	SHA256	d66075b2c70c3de22c9e774ad9e5f88d3d85708d1a5b17ccd4e760 49c86b49b5
	SHA1	a8cf0215610317b68a71d7a6fed7d9e07241d373
<u>Akira</u>	SHA256	3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d1 0fcb3312c, ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bb c59df4d1d, c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddcc5bb37857e7 bde6d2eb7, a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455 e4da67bc, 2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba 0f1624422,

Attack Name	TYPE	VALUE
<u>Akira</u>	SHA256	74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1, d323d32cbd906c495a6e9fe7da01bf3e0eca407609a2693c7246346687d59f50, ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5, 88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2, 8816caf03438cd45d7559961bf36a26f26464bab7a6339ce655b7fba d68bb439, 87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d, 78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0, 68d5944d0419bd123add4e628c985f9cbe5362ee19597773baea565bff1a6f1a, 58e685695afc3a85d2632777a2b54967dc53d6a6fa1b7e2c110b2023b561bfe9, 566ef5484da0a93c87dd0cb0a950a7cff4ab013175289cd5fccf9dd7ea430739, 51e250342faa954d28f46517a83a6ff81cce89c30dc86a9fb3c5fd50d095d850, 462505ad0fd657e7b031b0a3706fdcd04a20402c185b82caec91e29c2ff1e2d9, 43b0ac119ff957bb209d86ec206ea1ec3c51dd87bebf7b4a649c7e6c7f3756e7, 1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218
<u>Fog</u>	SHA256	e67260804526323484f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3

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

November 04, 2024 • 11:30 PM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com