Date of Publication
November 18, 2024

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

11 to 17 NOVEMBER 2024

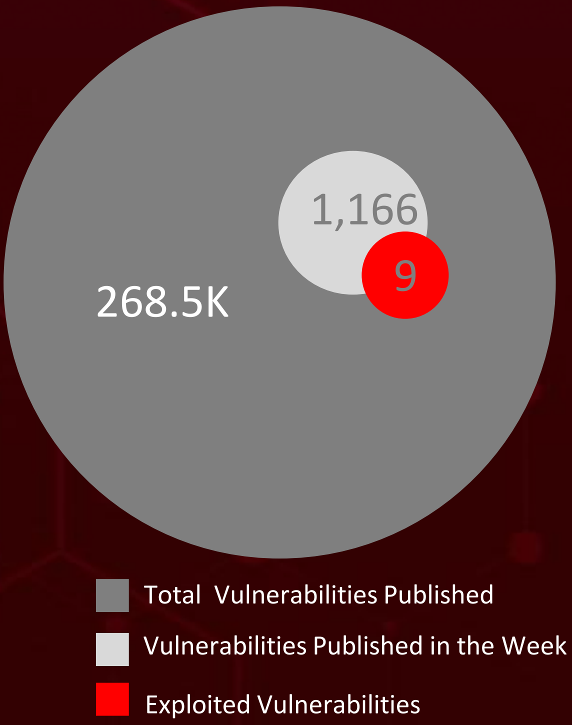
Table Of Contents

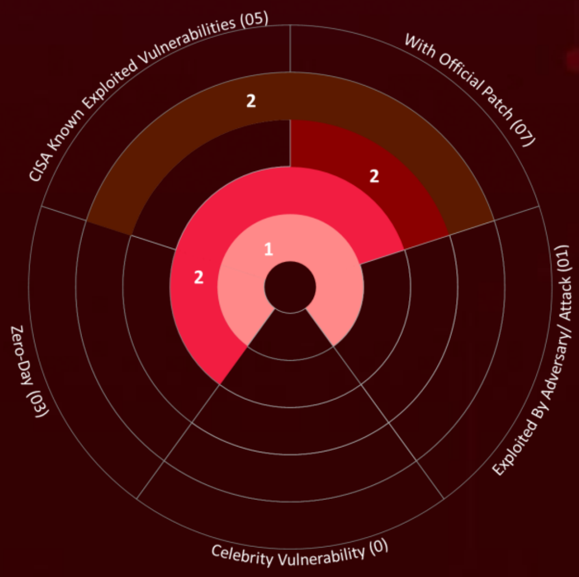
Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, **eight** attacks were executed, **nine** vulnerabilities were uncovered, and **two** active adversaries were identified, underscoring the persistent danger of cyberattacks.

HiveForce Labs has revealed that **WIRTE**, a Middle Eastern advanced persistent threat (APT) group, is actively targeting entities across the Palestinian Authority, Jordan, Egypt, Iraq, and Saudi Arabia. The group has employed a diverse set of malicious tools and techniques, including custom loaders such as "**IronWind**" and the wiper malware "**SameCoin**," to infiltrate and disrupt their targets.

Additionally, North Korean threat actors have introduced a new strategy to target macOS devices. They are leveraging trojanized Notepad apps and Minesweeper games, developed using **Flutter** and signed with a legitimate Apple developer ID, to compromise macOS systems. This marks a notable shift in their tactics. A newly identified phishing campaign is leveraging a variant of the **Remcos RAT** to target Microsoft Windows users. The attack begins with phishing emails that contain a malicious Excel document designed to exploit the **CVE-2017-0199** vulnerability. These escalating threats pose a significant and immediate risk to users worldwide.





High Level Statistics

8

Attacks Executed

- GootLoader
- GootKit
- Ymir ransomware
- RustyStealer
- Remcos RAT
- IronWind Loader
- Havoc Demon
- SameCoin Wiper

9

Vulnerabilities Exploited

- CVE-2017-0199
- CVE-2024-49039
- CVE-2024-43451
- CVE-2024-49040
- CVE-2024-49019
- CVE-2024-49056
- CVE-2024-10914
- CVE-2024-9463
- CVE-2024-9465

2

Adversaries in Action

- TAG-112
- WIRTE

Insights

GootLoader

Bengal cat enthusiasts in Australia targeted with a new variant of the GootLoader

CVE-2024-10914

a critical flaw putting thousands of D-Link NAS devices at serious risk worldwide

TAG-112

a cyberespionage group, has compromised two Tibetan community websites, embedding malicious JavaScript

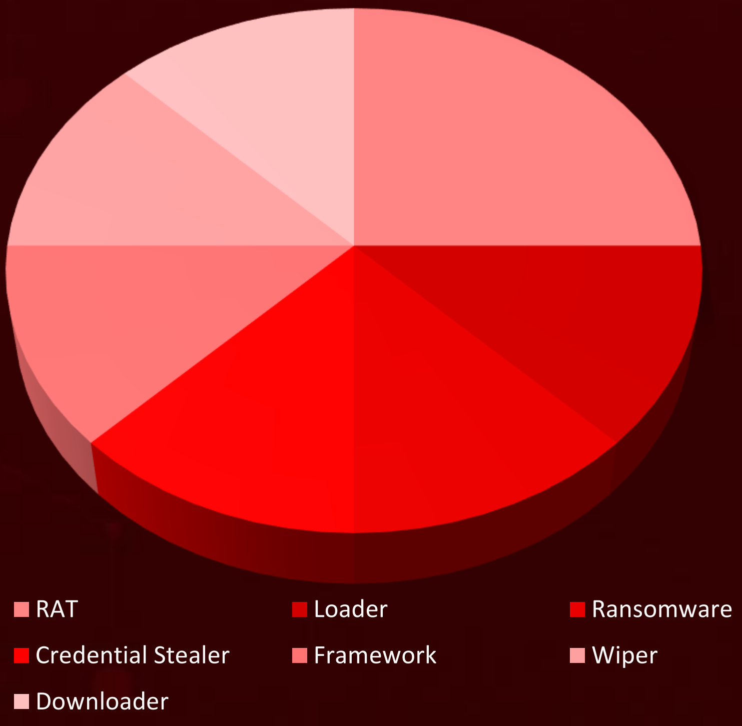
WIRTE, a Middle Eastern APT group, targets organizations in Palestine, Jordan, Egypt, Iraq, and Saudi Arabia with custom loaders like IronWind and wiper malware SameCoin

Ymir Ransomware employs in-memory execution and advanced evasion techniques to bypass defenses, linked to RustyStealer, recently targeting a Colombian organization, highlighting ties with access brokers

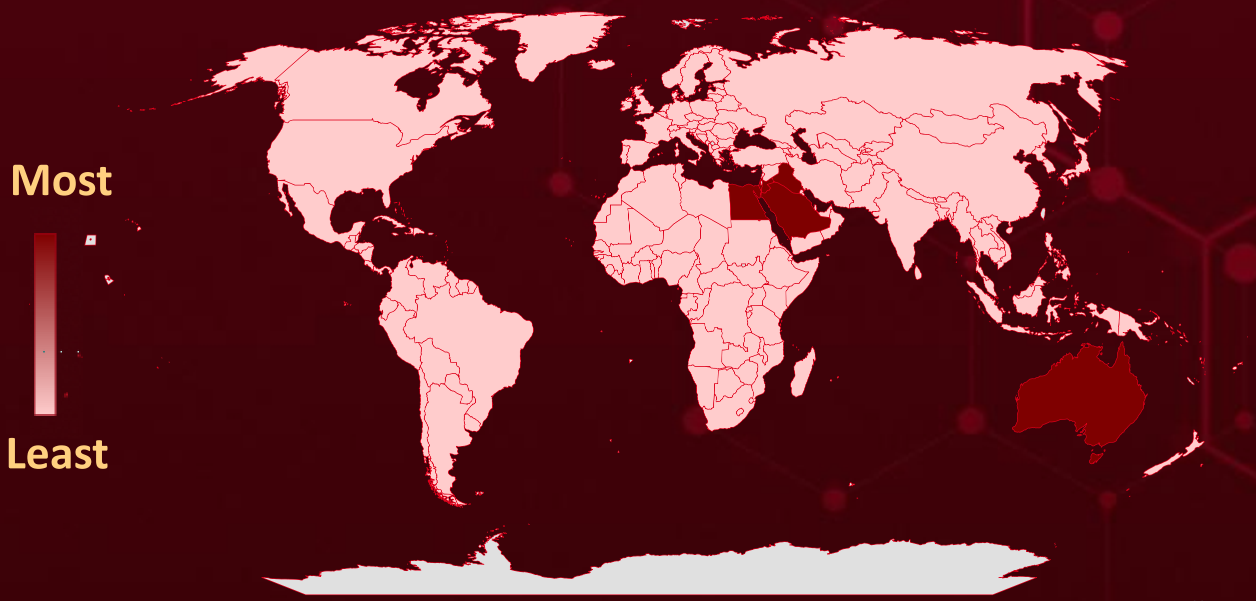
Remcos RAT

a potent malware capable of stealing data, controlling devices, and executing harmful actions

Threat Distribution



Targeted Countries



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

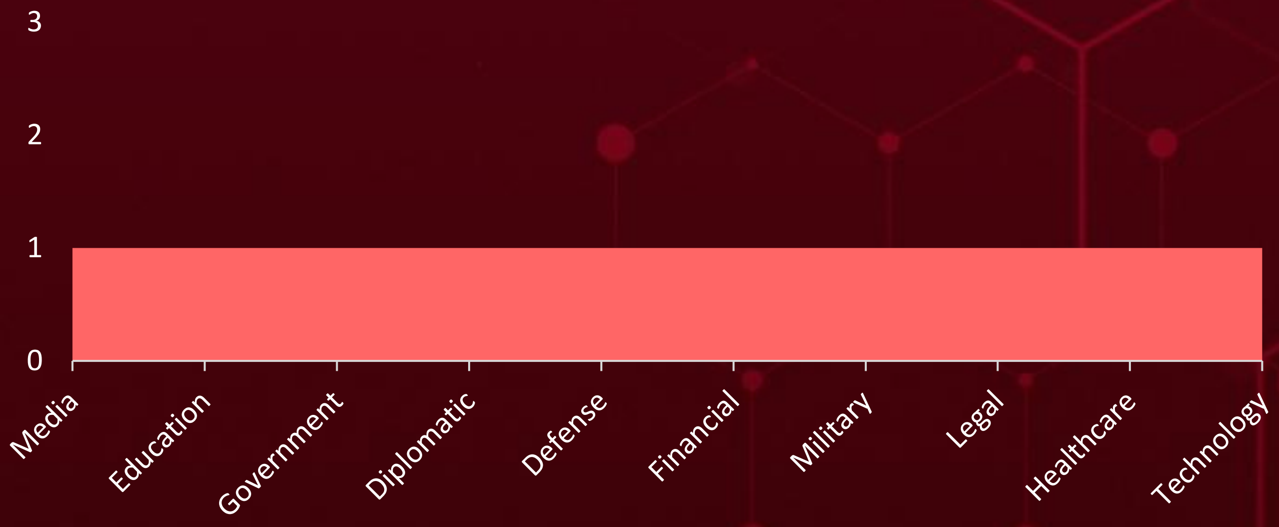
	Countries
■	Iraq
■	Saudi Arabia
■	Israel
■	Australia
■	Egypt
■	Jordan
■	Palestine
□	Oman
□	Liechtenstein
□	South Korea
□	Armenia
□	Mongolia
□	Albania
□	Saint Pierre and Miquelon
□	Austria
□	Uganda
□	Azerbaijan
□	Malta
□	Bahamas
□	Netherlands
□	Bahrain
□	Poland

	Countries
□	Bangladesh
□	Seychelles
□	Barbados
□	Sweden
□	Belarus
□	Venezuela
□	Belgium
□	Malawi
□	Belize
□	Mexico
□	Benin
□	Myanmar
□	Bhutan
□	Nigeria
□	Bolivia
□	Papua New Guinea
□	Bosnia and Herzegovina
□	Russia
□	Botswana
□	Sao Tome & Principe
□	Brazil

	Countries
□	United States
□	Burkina Faso
□	Zimbabwe
□	Burundi
□	Luxembourg
□	Cabo Verde
□	Maldives
□	Cambodia
□	Mauritania
□	Cameroon
□	Moldova
□	Canada
□	Morocco
□	Central African Republic
□	Nauru
□	Chad
□	Nicaragua
□	Chile
□	North Macedonia
□	China
□	Palau

	Countries
□	India
□	Sierra Leone
□	Indonesia
□	Slovakia
□	Iran
□	Solomon Islands
□	Andorra
□	South Africa
□	Ireland
□	South Sudan
□	Angola
□	Sri Lanka
□	Italy
□	State of Palestine
□	Jamaica
□	Suriname
□	Japan
□	Switzerland
□	Togo
□	Tajikistan
□	Tonga

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1588.006** Vulnerabilities	**T1027** Obfuscated Files or Information	**T1204** User Execution	**T1204.001** Malicious Link
T1566 Phishing	**T1588** Obtain Capabilities	**T1588.005** Exploits	**T1036** Masquerading	**T1574** Hijack Execution Flow
T1055 Process Injection	**T1068** Exploitation for Privilege Escalation	**T1574.002** DLL Side-Loading	**T1059.007** JavaScript	**T1057** Process Discovery
T1082 System Information Discovery	**T1053** Scheduled Task/Job	**T1140** Deobfuscate/Decode Files or Information	**T1584** Compromise Infrastructure	**T1053.005** Scheduled Task

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GootLoader	GootLoader is a stealthy malware acting as a first-stage downloader targeting Windows systems. It plays a key role in Initial-Access-as-a-Service (IAaaS), a cornerstone of the Ransomware-as-a-Service (RaaS) criminal ecosystem. Its origins trace back to GootKit, a banking trojan and stealer active since 2014, which served as its earliest second-stage payload.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Loads other malware	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	882ff7d228e6c2494393bb964b039920139b8fab5bbcadfb5ce863b3950edf26, 4d2befd04bd2aff3c0ca7880f3e659a5e23cf6c399798e577fa0d5172b460c5d

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GootKit	GootKit is a banking trojan with an x86 loader and a Node.js-powered payload. The loader stores the payload in the registry, injects it into its process, and places encrypted DLLs into browser processes. These DLLs enable man-in-the-browser attacks, allowing GootKit to intercept and modify HTTP/HTTPS traffic using web injects from its command-and-control server for data theft and manipulation.	GootLoader	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Steal Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	1615ac8c21cce75cb9e66d60151215e368f6b2aef2547feee2bf68f998702eb9, 282d2563e428a52e763353b3f2155984f9e0f483d6386300822f8da86f023750

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
Ymir ransomware	The Ymir ransomware is a sophisticated new threat that uses in-memory execution and advanced evasion techniques to bypass traditional detection methods. Linked to credential-stealing malware like RustyStealer, Ymir operates by executing key functions directly within system memory through specialized memory management operations, making it a formidable addition to the ransomware landscape.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RustyStealer	RustyStealer, first identified in 2021, is a credential-stealing malware designed to harvest login data and enable unauthorized access. By targeting high-privilege accounts, it facilitates lateral movement within networks, creating a pathway for deploying Ymir ransomware.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Credential Stealer		Steal data	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	7c00152cc68f0104e7436f9ce8b4c99e685d05f4361f50af307d4bfdbc90bca0

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Remcos RAT	Remcos is a remote access trojan (RAT) that grants attackers backdoor access to infected systems, enabling the collection of sensitive data. It evades detection through techniques like process injection and process hollowing, running within legitimate processes. Its core functionality includes encrypted communication with command-and-control (C2) servers, often using Distributed DNS to generate multiple domains for C2 infrastructure.	Phishing	CVE-2017-0199
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Steal data	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199
IOC TYPE	**VALUE**		
SHA256	4A670E3D4B8481CED88C74458FEC448A0FE40064AB2B1B00A289AB504015E944, F99757C98007DA241258AE12EC0FD5083F0475A993CA6309811263AAD17D4661		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
IronWind Loader	IronWind is a newly identified initial access downloader designed to connect to attacker-controlled servers to retrieve additional payloads. Among these, it often delivers post-exploitation toolkits, enabling further malicious activities on compromised systems.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Loads Malware	-
ASSOCIATED ACTOR			**PATCH LINK**
WIRTE (aka White Dev 21)			-
IOC TYPE	**VALUE**		
SHA256	c068b9e7130f6fb5763beb9564e92a89644755f223b2f65dc762ed5c77c5b8e3		

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
Havoc Demon	Havoc is an open-source command-and-control (C2) framework emerging as an alternative to tools like Cobalt Strike and Brute Ratel. Threat actors deliver its Havoc Demon Agent via a ZIP archive named "ZeroTwo.zip", which contains a downloader file and a decoy document to initiate the infection chain.	Social Engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Framework		Remote Access, System Compromise	-
ASSOCIATED ACTOR			PATCH LINK
WIRTE (aka White Dev 21)			-

IOC TYPE	VALUE
SHA256	c22f0544e29c803d2cacbca3a57617496e3691389e9b65da84c374c90e699433

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SameCoin Wiper	SameCoin is a multi-platform wiper targeting Android and Windows systems, disguised as an INCD security update. On infection, it modifies the system's background while executing its destructive payload.	Disguised as an INCD security update	-
TYPE		IMPACT	AFFECTED PRODUCTS
Wiper		Wipe Data, Modify Data	-
ASSOCIATED ACTOR			PATCH LINK
WIRTE (aka White Dev 21)			-

IOC TYPE	VALUE
SHA256	2abff990d33d99a0732ddbb3a39831c2c292f36955381d45cd8d40a816d9b47a, 7c0a8d3dec1675fd8ba0a73fb5b8eee3bef0214aa78a7aab73b8ba9814651f9f, B447ba4370d9becef9ad084e7cdf8e1395bafde1d15e82e23ca1b9808fef13a7

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-2017-0199	✗	Microsoft Office and WordPad	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	Remcos RAT
Microsoft Office and WordPad Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0199

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-49039	✗	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Task Scheduler Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49039

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43451	✗	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
NTLM Hash Disclosure Spoofing Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-49040	✗	Microsoft Exchange Server 2016 & 2019	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2016:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:*:*:*:*:*:*	-
Microsoft Exchange Server Spoofing Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-451	T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49040

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2024-49019]()	❌	Windows Server: 2008 - 2025	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Active Directory Certificate Services Elevation of Privilege Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1390	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49019

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2024-49056]()	❌	airlift.microsoft.com	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:airlift.microsoft.com:*:*:*:*:*:*:*:*	-
Airlift.microsoft.com Elevation of Privilege Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-302	T1068: Exploitation for Privilege Escalation	No patch

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-10914	❌	DNS-320 Version 1.00, DNS-320LW Version 1.01.0914.2012, DNS-325 Version 1.01, Version 1.02, DNS-340L Version 1.08	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:dns-320_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:dlink:dns-320lw_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:dlink:dns-325_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:dlink:dns-340l_firmware:*:*:*:*:*:*:*:*	-
D-Link NAS Command Injection Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	No patches are available as these devices are no longer supported, by the vendor.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9463	✗	Palo Alto Networks’ Expedition versions prior to 1.2.92	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:paloaltonetworks: expedition:*:*:*:*:*:*:*:*	-
Palo Alto Networks Expedition OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9465	✗	Palo Alto Networks’ Expedition versions prior to 1.2.92	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:paloaltonetworks: expedition:*:*:*:*:*:*:*:*	-
Palo Alto Networks Expedition SQL Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter	https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
TAG-112	China	Media, Education	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; T1583: Acquire Infrastructure; T1583.004: Server; T1583.006: Web Services; T1584: Compromise Infrastructure; T1584.004: Server; T1189: Drive-by Compromise; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1071: Application Layer Protocol; T1204: User Execution; T1204.001: Malicious Link; T1539: Steal Web Session Cookie; T1573: Encrypted Channel; T1057: Process Discovery; T1105: Ingress Tool Transfer

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
WIRTE (aka White Dev 21)	Middle East	Government, diplomatic, defense, financial, military, legal, healthcare, and technology	Jordan, Egypt, Saudi Arabia, Iraq, Israel, Palestine
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	IronWind Loader, Havoc Demon, SameCoin Wiper	-
TTPs			
TA0003: Persistence; TA0005: Defense Evasion ; TA0001: Initial Access; TA0002: Execution; TA0010: Exfiltration; TA0040: Impact; TA0011: Command and Control; T1053.005: Scheduled Task; T1059: Command and Scripting Interpreter; T1566: Phishing; T1027: Obfuscated Files or Information; T1055: Process Injection; T1574.002: DLL Side-Loading; T1574: Hijack Execution Flow; T1041: Exfiltration Over C2 Channel; T1584: Compromise Infrastructure; T1140: Deobfuscate/Decode Files or Information; T1204.002: Malicious File; T1053: Scheduled Task/Job; T1204.001: Malicious Link; T1204: User Exécution; T1505.005: Terminal Services DLL; T1505: Server Software Component			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actors **TAG-112, WIRTE** and malware **GootLoader, GootKit, Ymir ransomware, RustyStealer, Remcos RAT, IronWind Loader, Havoc Demon, SameCoin Wiper.**

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 **nine exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **TAG-112, WIRTE** and malware **GootLoader, GootKit, Ymir ransomware, RustyStealer, Remcos RAT, IronWind Loader, Havoc Demon, SameCoin Wiper** in Breach and Attack Simulation(BAS).

Threat Advisories

GootLoader's Evolution: From SEO Poisoning to Persistent Network Intrusions

Ymir Ransomware a New Era of In-Memory Execution Tactics

New Remcos RAT Variant Targets Windows Users

North Korean Hackers Unleash Flutter-Based Malware in New macOS Attack

Microsoft’s November Patch Tuesday Addresses Active Zero-Day Exploits

Critical Flaw in D-Link NAS Devices Exposes Thousands to Remote Command Attacks

China-affiliated group Infiltrated Tibetan Websites

Hamas-Linked WIRTE Expands Cyber Activities Against Israel

Hackers Exploiting Critical Palo Alto Networks Vulnerabilities

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
GootLoader	SHA256	882ff7d228e6c2494393bb964b039920139b8fab5bbcadfb5ce863b3950edf26, 4d2befd04bd2aff3c0ca7880f3e659a5e23cf6c399798e577fa0d5172b460c5d, 94895c34d4467687f818ed661384b8736b6662c12514b26c94ec1b3f66bf4bdc, c4b3e2224c23826d1b72923ee5089f26f9b79ada450b10545c8ffa6725c010b2, 05d7c90f77b08d730e1b5fa600fad48cbb942a53686665de87695d0202377506, c236db30c0d4a72c859c1e9bed572f4a481da8738fb32431648c631b922cdc7c, d0c9246d858e08fabfa000ba6c12ad55dc227023fc6a411c1fdf3668dfedac80, 5b119d32c6bf846edf88a6d1cfc65fe0ed84062f147f58c00c38005b4c0bfe57, 5bd1ea3189abff1bcd3abb80ebbec1112f3decd1b973983817fabff41b2c70e2, f6d028706168ea5155e325384278b6a5c17c63c47c72f0400f193d0e9bbb799b, b760bd6055aec8392be58b731c84a5496ef8c1777b9ce24efb015d7174c26b9b, f28d53019112dcbf1019c27d8b2f59c5c82c9af7a446d99cce6c836cb264be57, ae7d1d1aecaa1054570b26cbfe4bb1e1b6e0bdb3d5b0090ee0973419d75a0af3, 6fb715415bec220d6bff3507ca3f78412154870c9bc20675e1598e3b8306212a, 425f4fcfecfeec8d5eb3d3f1051b67a1999bef16f983a1281d7c13be3ebe0e7b, c70be3e7fcdaef811f5c3471bf08502dda83d65e32268ddabd7a0e3f304fb347, 517fd5c641f732f308e0b0346ff2ae9abd08bb36ad5a8565ac4f9122ab70b965, eb104343436305c6b469386868084f65c5755917f3a366fd840889e561645415, 447f36c5fb3310a72df2ddcfa1717a8ded05d0d2330e8d256b2ce913c6baa89e, 2af54118c2934178ec28866dde98f05bbcffc56d472afbce01fd68f40404d716, 933915ca590e6cae2d359b56a9e6fca3afea4d23f35ac996c07c643c05e6d8be c54dc4217b3629c3d84733208d65e5fec94a13d144b26fe3b041aa550ab5d7be, fa6891cf009fbc98e3b860fb96ca03c84083fcb919ee75a296561137bbf9c49d, 6b869c6592e2f52bd2501c36959cf2936c50b0c28c32a3bf51574c04e9c3bd66, 273178f2dab81c0907dcdda645285a0d297d9c38f45ff2559dff32fe9c47eaef, 568eeaab68afe15f420fcdc4ac5174dfae9cb1b56b365ddf0951dee35f916dff, b939ec9447140804710f0ce2a7d33ec89f758ff8e7caab6ee38fe2446e3ac988

Attack Name	TYPE	VALUE
GootKit	SHA256	1615ac8c21cce75cb9e66d60151215e368f6b2aef2547feee2bf68f998702eb9, 282d2563e428a52e763353b3f2155984f9e0f483d6386300822f8da86f023750, 14d150a2ea315ad6ebe5b0f6cf2093d474636c3ed7af97f5f322f56194077bf9, b1f70bd7d0c27a06e65aae69ae221a7f77d378177bf7c1faeccaf04e3bdc861f, 38933984f5ff8b71c054d1c1155e308ac02377b89315ef17cea859178a30dbab, 6b6f47abe5a8103adf1b12e5f3651ed24b632a64c5c94ce297a6f9ca0710f772, 9e7580489a6e346a26ac16c42a33e1857d67801bcc4191c1303d158e52c931ae, 92e2bf4ecdfbc1d16650902698b047e659e7e25ed22665aabfc0b2e22817b679, 7166921e37458ba67f1e96a7ed289edf0e6157664f8e8e84767a215c9ecc9cd3, b683ccee257c2edb5dada7ca00e936cfbb7a81e006719afc5c91778188d349e5, 35fd40cd3529e9b39b363bba62990949468f3a97ebb7e30e0f7629a64ae3c1d3, f7ecd1b95bc537cc04d2b4503c66000c465f4398b71da2a00e2a0d804477c992
Ymir	MD5	dd7799d822f052cfa8ad1e16b33bb2cb
	SHA1	fe6de75d6042de714c28c0a3c0816b37e0fa4bb3
	SHA256	04dce8eb632250f64f1741f47707e6cb991926d35f4157d540c2fc3230b6a92f
RustyStealer	MD5	5ee1befc69d120976a60a97d3254e9eb
	SHA1	e6c4d3e360a705e272ae0b505e58e3d928fb1387
	SHA256	7c00152cc68f0104e7436f9ce8b4c99e685d05f4361f50af307d4bfdbc90bca0
Remcos RAT	IPv4:PORT	107[.]173[.]4[.]16[:]2404
	URLs	hxxps://og1[.]in/2Rxzb3, hxxp://192[.]3[.]220[.]22/xampp/en/cookienetbookinetcahce.hta, hxxp://192[.]3[.]220[.]22/hFXELFSwRHRwqbE214.bin, hxxp://192[.]3[.]220[.]22/430/dllhost.exe
	SHA256	4A670E3D4B8481CED88C74458FEC448A0FE40064AB2B1B00A289AB504015E944, F99757C98007DA241258AE12EC0FD5083F0475A993CA6309811263AAD17D4661, 9124D7696D2B94E7959933C3F7A8F68E61A5CE29CD5934A4D0379C2193B126BE, D4D98FDBE306D61986BED62340744554E0A288C5A804ED5C924F66885CBF3514, F9B744D0223EFE3C01C94D526881A95523C2F5E457F03774DD1D661944E60852, 24A4EBF1DE71F332F38DE69BAF2DA3019A87D45129411AD4F7D3EA48F506119D
IronWind Loader	SHA256	c068b9e7130f6fb5763beb9564e92a89644755f223b2f65dc762ed5c77c5b8e3

Attack Name	TYPE	VALUE
Havoc Demon	SHA256	c22f0544e29c803d2cacbca3a57617496e3691389e9b65da84c374c90e699433
SameCoin Wiper	SHA256	2abff990d33d99a0732ddbb3a39831c2c292f36955381d45cd8d40a816d9b47a, 7c0a8d3dec1675fd8ba0a73fb5b8eee3bef0214aa78a7aab73b8ba9814651f9f, b447ba4370d9becef9ad084e7cdf8e1395bafde1d15e82e23ca1b9808fef13a7

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.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

November 18, 2024 • 7:10 AM

More at www.hivepro.com