Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

Hamas-Linked WIRTE Expands Cyber Activities Against Israel

Date of Publication	Admiralty code	TA Number
November 15, 2024	A1	TA2024432

Summary

First Seen: 2018
Malware: IronWind Loader, Havoc Demon, SameCoin Wiper
Threat Actor: WIRTE (aka White Dev 21)
Targeted Region: Jordan, Egypt, Saudi Arabia, Iraq, Israel, Palestine
Affected Platforms: Windows and Android
Targeted Industries: Government, diplomatic, defense, financial, military, legal, healthcare, and technology

Actor Map

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

Actor Details

#1

WIRTE, a Middle Eastern advanced persistent threat (APT) group active since at least 2018, is connected to the Hamas-affiliated Gaza Cybergang. Despite the current regional conflict, WIRTE has sustained its operations, targeting entities within the Palestinian Authority, Jordan, Egypt, Iraq, and Saudi Arabia. Initially known for espionage, WIRTE has evolved to include disruptive attacks. Notably, these activities align with recent geopolitical events, as WIRTE has exploited these developments for cyber-espionage, particularly targeting organizations in these countries with sophisticated malware.

#2

WIRTE's recent campaigns reveal a variety of malicious tools and techniques, including custom loaders like "IronWind" and the wiper malware "SameCoin." Two major disruptive attacks against Israeli entities in February and October 2024 involved SameCoin, underscoring WIRTE's new strategy of cyber-disruption. Unlike their past operations, these attacks were intended not only for intelligence gathering but to destabilize Israel. They targeted Israeli organizations like hospitals and municipalities, using tools capable of persistent system access, data exfiltration, and control.

#3

WIRTE's techniques highlight a well-coordinated, evolving toolkit. The group leverages HTML tags for malware communication, implements user-agent-specific responses to filter targets, and redirects traffic to legitimate websites if the user-agent conditions are unmet. WIRTE's infrastructure uses consistent domain-naming themes related to Middle Eastern countries, health, and finance, allowing them to mask malicious activities and evade detection. These sophisticated tactics suggest a mature operational model focused on both evasion and effective targeting.

#4

The campaign also points to clear ideological connections between WIRTE and Hamas. For instance, the SameCoin wiper used against Israeli targets included propaganda elements promoting Hamas's Al-Qassam Brigades. This, coupled with WIRTE's persistent focus on the Palestinian Authority (a Hamas rival) and consistent selection of targets aligned with Hamas's interests, indicates WIRTE's broader ideological alignment with Hamas. Although WIRTE's disruptive operations center on Israel, their espionage activities encompass broader Middle Eastern political entities.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
WIRTE (aka White Dev 21)	Middle East	Jordan, Egypt, Saudi Arabia, Iraq, Israel, Palestine	Government, diplomatic, defense, financial, military, legal, healthcare, and technology
	MOTIVE		
	Information theft and espionage		

Recommendations

Enhance Email Security: Implement advanced email filtering solutions to detect and block phishing attempts. Use technologies like DMARC, DKIM, and SPF to authenticate incoming emails and reduce the risk of spoofing.

Implement Robust Access Controls: Enforce the principle of least privilege, restricting access to critical systems and data, and closely monitor user permissions to prevent lateral movement by attackers.

Enhance Incident Response Capabilities: Develop and regularly test a proactive incident response plan that includes scenarios involving sophisticated malware, persistence mechanisms, and data exfiltration techniques.

Network Segmentation: Segment networks to limit the lateral movement of attackers within the organization. This can help contain potential breaches and minimize damage in case of an attack.

Advanced Threat Detection and Response: Deploying advanced threat detection and response solutions is essential for identifying and mitigating sophisticated attacks. This includes using Endpoint Detection and Response (EDR) tools, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). These tools can detect unusual activity and provide alerts on potential intrusions, allowing for quicker response times.

Potential MITRE ATT&CK 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 Execution	T1505.005 Terminal Services DLL	T1505 Server Software Component	

Indicator of Compromise (IOCs)

TYPE	VALUE
SAH256	2700142c0b78fdbf3df30125a72443e2317d5079a01ff26022a66d0b7bd4c5b1, 3fc92e8a440ca16172f7d93bd9de3c6f9391e26d3a1cb964e966ee1ee31770df, 5d773e734290b93649a41ccda63772560b4fa25ba715b17df7b9f18883679160, 5fa809c0e5dff03bd202b86cd334e80c7ed5dbad9aed7b12a3799ea0800e5f31, 0a4397f7d5da024b10c778910d6db84a6ba0fc3375fe6fe9b470f7e269ddc716, 26cb6055be1ee503f87d040c84c0a7cacb245b4182445e3eee47ed6e073eca47,

TYPE	VALUE
SHA256	7c0a8d3dec1675fd8ba0a73fb5b8eee3bef0214aa78a7aab73b8ba9814651f9f, b447ba4370d9becef9ad084e7cdf8e1395bafde1d15e82e23ca1b9808fef13a7, 9b2a16cbe5af12b486d31b68ef397d6bc48b2736e6b388ad8895b588f1831f47, c51952f2caf55b455e7c7eb8048422bb477e3a616cb68f6fa524e15892b9f328, d3a53be1f64325c566bb71222b3747da81439dea8fc9a458fb459355cfa9e7f2, ac227dd5c97a36f54e4fa02df4e4c0339b513e4f8049616e2a815a108e34552f, c068b9e7130f6fb5763beb9564e92a89644755f223b2f65dc762ed5c77c5b8e3, c22f0544e29c803d2cacbca3a57617496e3691389e9b65da84c374c90e699433, 76a543a49e46ad9163b2a06f6cea7a5e8eb5183cd3213e64446a8c66310fac3a, e2ba2d3d2c1f0b5143d1cd291f6a09abe1c53e570800d8ae43622426c1c4343c, 02902a5e07a80aa56c24c6a8d4cca9fcfb32f32bb074f9c449cad5b3b18a070c, e6d2f43622e3ecdce80939eec9fffb47e6eb7fc0b9aa036e9e4e07d7360f2b89, 3b4ee3d5c1a7202b053159becac4d0b622641e2e4a7b27f339c03a90f287d381, f2de8a5daed043ef3ab1f52156a4f7ff8f9a382f7f58ace6abb463f5cbab060c, fca0b3e57b3f9a14d18c435e564fe6db3620ba446e1b863737a9b36cbcc7251a, eddd40d457088d8384784ce80eaf0aefb1485776e0916e60781befbd739d4608, 6ab5a0b7080e783bba9b3ec53889e82ca4f2d304e67bd139aa267c22c281a368, 2abff990d33d99a0732ddbb3a39831c2c292f36955381d45cd8d40a816d9b47a, 9fe7b2f4c17dd0c7a00aaa6a779c30e2cb3faa4b14766e02f616d00e6f6e9007, 3d2409c7834287178f61116c9b653e3520172a10ebef58f58f99d27a34b839bd, 5b7e8e685f6ee6b4810ed94b4420e08a10a977516b47fea356173cfaec2c41a0, 41112f36fc17f57f0e476c9ffa9e1ecbff796dc31a7ff0372d0d8708a5e9c50b, 2d55c68aa7781db7f2324427508947f057a6baca78073fee9a5ad254147c8232, b7c5af2d7e1eb7651b1fe3a224121d3461f3473d081990c02ef8ab4ace13f785

TYPE	VALUE
SAH256	75c2fb3ae08502a57c8c96ea788ef946a8bb35fb4a16e76deefae4c94fd03fd7, 86791aa96bac086330bf927ea5c2725ff73aaedfadc2571f4f393aa4d3a6b690, 8ce87eefded0713c9258f8f2086dcc51028fb404ceb526f832df4c93108c8146, 8818c7c2cbd60521b8eb59ff9a720840535651343b30c1b279515d42d8036a8a, 7e0d0f77fe1dcb1e7a0a0a2fc0c25a68eee551c7045935449ae64dcbd1310958, 795b997c248b2f344f813cd0c15d3d435e6218c91d0f0f54a464d739feead4c5, 9fc4c7cdcaa3c3c03ba65f138386e875d02f7fcaf10de720dfde20167e393f38,
Domains	saudiday[.]org, jordansons[.]com, egyptican[.]com, healthcarb[.]com, inclusive-economy[.]com, king-pharmacy[.]com, microsoftwindowshelp[.]com, economystocking[.]com, wellhealthtech[.]com, microsoftliveforums[.]com, master-dental[.]com, dentalaccord[.]com, economymentor[.]com, bankjordan[.]com, egyptskytours[.]com, microsoftteams365[.]com, finance-analyst[.]com, trendingcharts[.]finance-analyst[.]com, finances-news[.]com, pushservice_api[.]finances-news[.]com, support-api[.]financecovers[.]com, jordanrefugees[.]com, egypttourism-online[.]com, healthoptionstoday[.]com, ellemedic[.]com, easybackupcloud[.]com, financeinfoguide[.]com, healthscratches[.]com, printspoolerupdates[.]com, saudiarabianow[.]org, suppertools[.]com, theshortner[.]com

TYPE	VALUE
IPv4	185[.]158[.]248[.]161, 193[.]168[.]141[.]29, 140[.]99[.]164[.]56, 160[.]119[.]251[.]181, 188[.]92[.]78[.]148, 185[.]165[.]169[.]76, 45[.]134[.]9[.]202, 37[.]120[.]247[.]22, 195[.]123[.]210[.]42, 140[.]99[.]164[.]86, 213[.]252[.]244[.]234, 5[.]42[.]221[.]151, 37[.]221[.]65[.]254, 80[.]77[.]25[.]49, 193[.]168[.]141[.]61, 185[.]247[.]224[.]28, 185[.]158[.]248[.]201

References

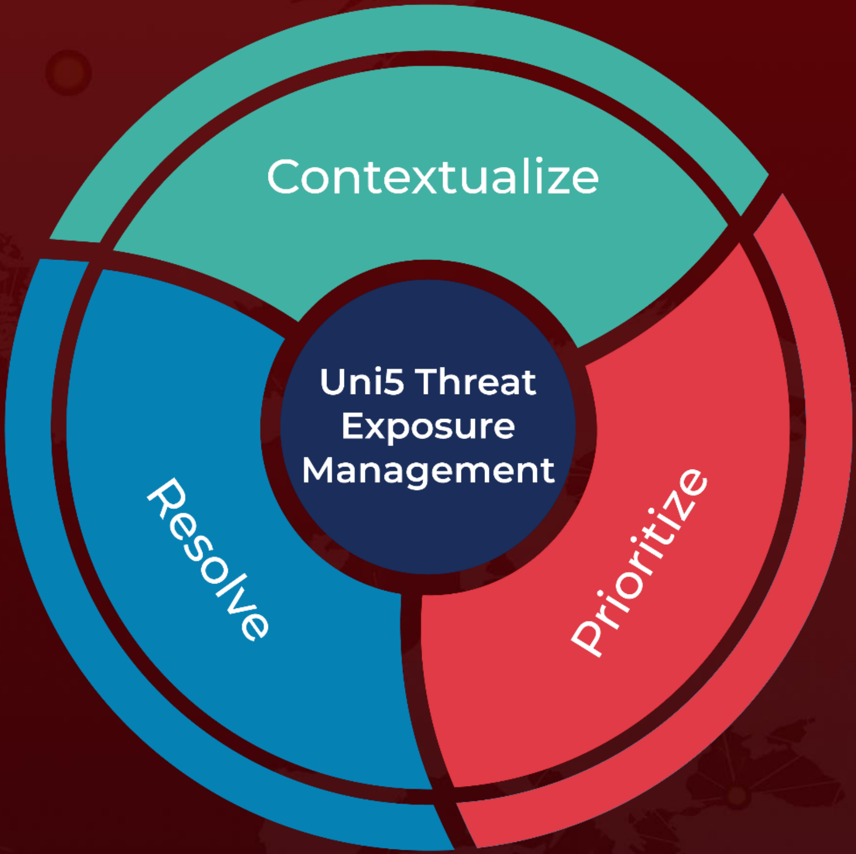
https://research.checkpoint.com/2024/hamas-affiliated-threat-actor-expands-to-disruptive-activity/

https://attack.mitre.org/groups/G0090/

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 15, 2024 • 5:30 AM

More at www.hivepro.com