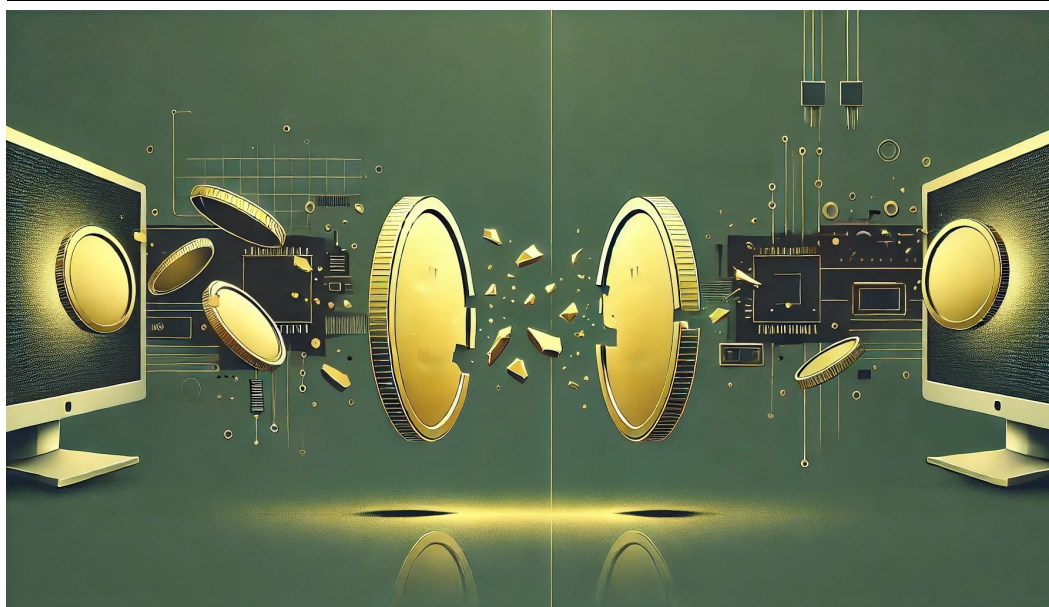


Hamis-affiliated Threat Actor WIRTE Continues its Middle East Operations and Moves to Disruptive Activity

11/12/2024



November 12, 2024

Key findings:

- Check Point Research has been tracking ongoing activity of WIRTE threat actor, previously associated with the Hamas-affiliated group Gaza Cybergang, despite the ongoing war in the region.
- The conflict has not disrupted the WIRTE's activity, and they continue to leverage recent events in the region in their espionage operations, likely targeting entities in the Palestinian Authority, Jordan, Iraq, Egypt, and Saudi Arabia.
- Our research indicates that WIRTE group has expanded beyond espionage to conduct disruptive attacks. We have identified clear links between the custom malware used by the group and SameCoin, a wiper malware targeting Israeli entities in two waves in February and October 2024.
- While WIRTE's tools have evolved since the group emerged, key aspects of their operations remain consistent: domain naming conventions, communication via HTML tags, responses limited to specific user agents, and redirection to legitimate websites.

Introduction

WIRTE is a Middle Eastern Advanced Persistent Threat (APT) group [active](#) since at least 2018. The group is primarily known for engaging in politically motivated cyber-espionage, focusing on intelligence gathering likely linked to regional geopolitical conflicts. WIRTE is [believed](#) to be a subgroup connected to Gaza Cybergang, a cluster affiliated with Hamas.

Since late 2023, Check Point Research has been monitoring a campaign conducted by the WIRTE group that targets entities in the Middle East, specifically the Palestinian Authority, Jordan, Egypt, and Saudi Arabia. This campaign utilizes custom loaders like IronWind, first [disclosed](#) in November 2023 as part of a TA402 operation.

In addition to espionage, the threat actor recently engaged in at least two waves of disruptive attacks against Israel. Unique code overlaps reveals ties between the group's custom malware and [SameCoin](#), a custom wiper deployed in two waves in February and October 2024.

Unlike other Hamas- associated threats, such as [SysJoker](#), this cluster's activity has persisted throughout the war in Gaza. On one hand, the group's ongoing activity strengthens its affiliation with Hamas; on the other hand, it complicates the geographical attribution of this activity specifically to Gaza.

In this publication, Check Point Research reveals the activities of WIRTE in 2024, provides a technical analysis of its campaigns, and connects the group's activities to previous activity of the group.

WIRTE – Espionage Campaigns

As tensions continue in the Middle East, multiple threat actors have exploited the conflict to create deceptive lures in recent months. Among them, one prominent group is WIRTE, which is believed to have ties to Hamas. WIRTE remains highly active throughout the war, carrying out attacks across the region. The group's activities were first [documented](#) in 2019 by Lab52, with further [analysis](#) released in 2021. In 2023, Proofpoint researchers identified a campaign associated with a threat actor they refer to as TA402. The campaign utilized IronWind, a loader that enables communication with command and control (C2) servers and executes malicious code hidden within HTML elements. Since then, we have observed multiple campaigns leveraging IronWind.

Check Point Research's analysis suggests that this tool is primarily deployed by the WIRTE group, which Proofpoint identifies as a subgroup of TA402.

September 2024 campaign – Havoc delivery

In September, we identified a new infection chain that began with a PDF file showing an error and containing an embedded URL [https://theshortner\[.\]com/fxT1j](https://theshortner[.]com/fxT1j), which mimics a URL shortener service.

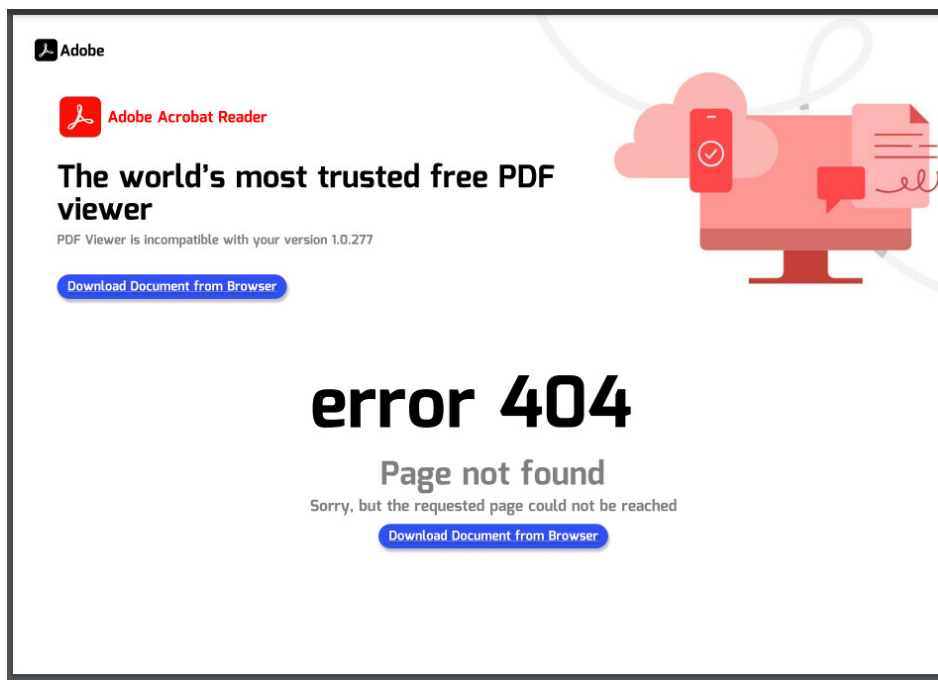


Figure 1 – Lure PDF (SHA-256:b7c5af2d7e1eb7651b1fe3a224121d3461f3473d081990c02ef8ab4ace13f785).

This link redirected users to a RAR archive named RAR 1178 - بيروت - تطورات الحرب في لبنان 2 (translated from Arabic: RAR 1178 - Beirut - Developments of the War in Lebanon 2). The archive contained three files intended to employ DLL-Sideloadng:

- **PinEnrollmentBroker.exe**, a legitimate executable that has been renamed to match the name of the archive.
- A PDF lure.
- **propsys.dll**, which serves as the first stage of the infection process.

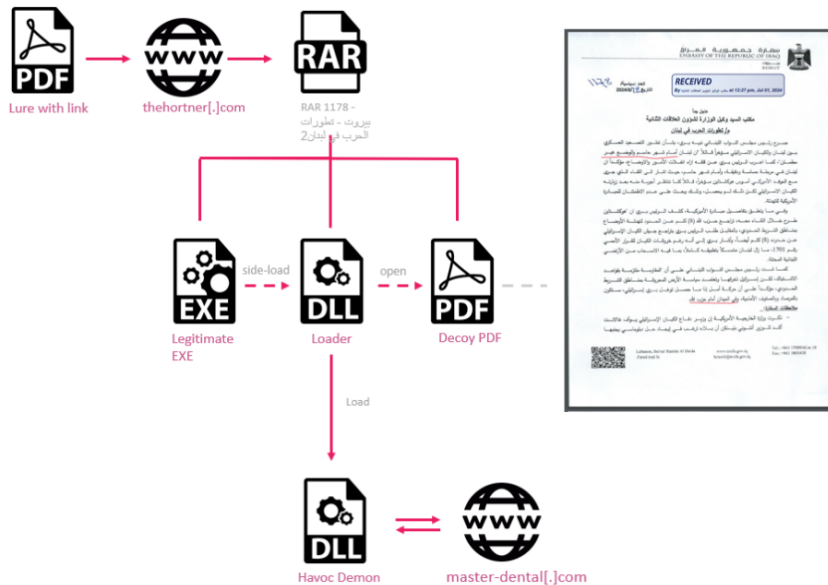


Figure 2 – Havoc Infection Chain.

Name	Size	Packed Si...	Created	Modified
1178 - بيروت - تطورات الحرب في لبنان 2.exe	112 128	46 908		2024-05-23 20:03
Document	1 160 053	1 022 667		2024-09-23 12:06
propsys.dll	667 736	187 169		2024-05-23 20:04

Figure 3 – Contents of the malicious archive.

Upon executing the legitimate executable file, the **propsys.dll** is side loaded. The execution is divided into two threads:

1. The first thread searches for a file named "Document," appends a PDF extension to the found file, and then opens it using the command line. All strings in this process are XOR encrypted with the key 01-01-1900.
2. The second thread reads the long list of embedded IP addresses and decodes them by calling the `RtlIpv4StringToAddressA` API, which converts an IP-formatted string to a byte array and concatenates the decoded bytes to create the next-stage payload.

```

RtlIpv4StringToAddressA_str db 'YkVBuUFbBWPq1lfSmRebFVdQ1VDQmw=',0
                                ; DATA XREF: sub_180001250+1A10
                                ; .rdata:0000000180054FD810

a8672137230 align 8
            db '86.72.137.230',0 ; DATA XREF: .rdata:list_of_ips10
            align 8
a72131228240 db '72.131.228.240',0 ; DATA XREF: .rdata:0000000180054FE810
                                ; .rdata:000000018005B8D010 ...

a7213123632 align 8
            db '72.131.236.32',0 ; DATA XREF: .rdata:0000000180054FF010
                                ; .rdata:000000018005741010 ...

a2321500 align 8
            db '232.15.0.0',0 ; DATA XREF: .rdata:0000000180054FF810
            align 8
a072137244 db '0.72.137.244',0 ; DATA XREF: .rdata:000000018005500010
            align 8
a9419510246 db '94.195.102.46',0 ; DATA XREF: .rdata:000000018005500810
            align 8

```

Figure 4 – IP addresses that are converted into bytes of the payload.

The next-stage payload delivered by **propsys.dll** is Havoc Demon, the agent of an open-source framework configured to communicate with the domain `master-dental[.]com`. **Havoc** is an open-source post-exploitation framework designed for advanced cyber operations. Havoc allows attackers to maintain persistent access to compromised systems, facilitating various malicious activities such as data exfiltration, lateral movement, and remote control.

Earlier 2024 activity – IronWind loader

Since October 2023, multiple cases observed use the IronWind loader as the infection vector. The infection chain starts with a RAR archive which includes three files: a legitimate executable `setup_wm.exe` renamed to `الممثلون الوطنيون لرؤساء الأركان لاتفاق على هيكل الأمن الإقليمي.exe` (National Representatives of

Chiefs of Staff Meet to Agree on Regional Security Architecture), a lure PDF and **version.dll**, which serves as the first stage of the infection process.

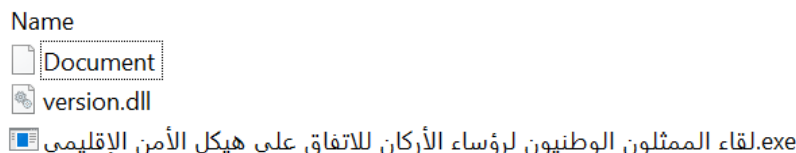


Figure 5 – RAR archive.

The malware execution starts by saving the lure document as a PDF file and opening it via CMD (Command Prompt). It then sends an HTTP request containing the victim's Office version, OS version, computer name, username, and list of programs to requestinspector.com to inform the attackers about a new victim.

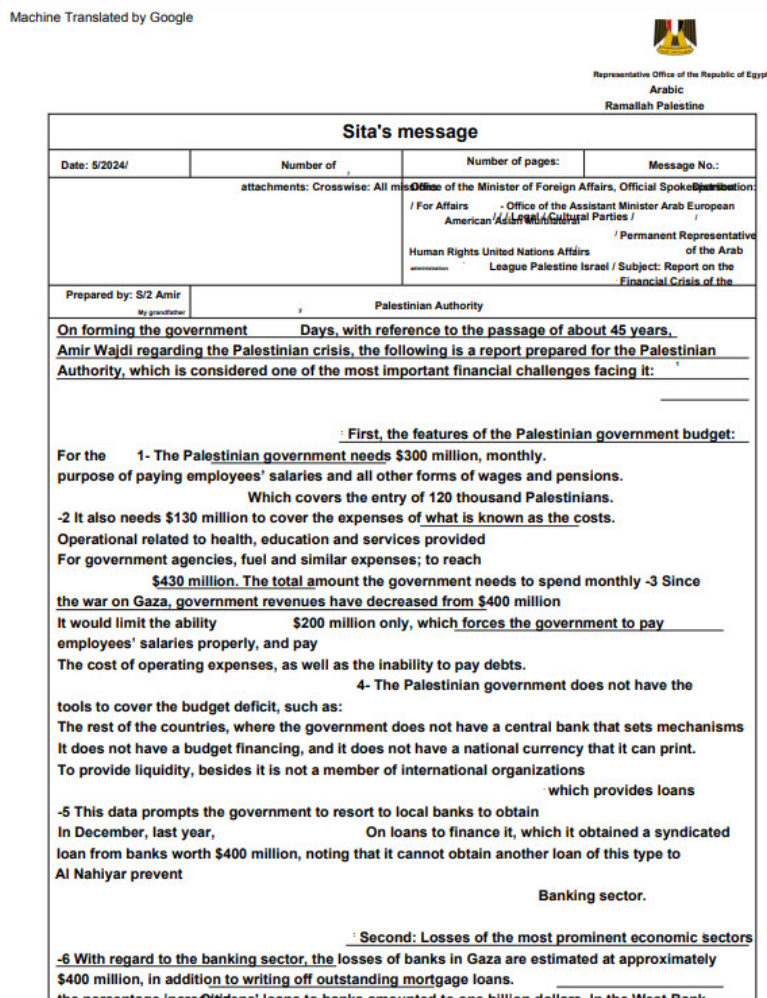


Figure 6 – Translated lure, allegedly written by Egypt Representative in Ramallah about PA budget

Next, the malware decrypts the next-stage payload, **propsys.dll**, using Base64 decoding and an XOR operation with the key "53." The primary function of this payload (internally named **stagerx64**) is to send HTTP requests with a hardcoded user agent to the C2 and scan for the encrypted payload embedded within HTML tags.



Figure 7 – Base64 encoded payload embedded between HTML tags.

The only final stage artifact we identified is donut shellcode loading a .NET DLL named **exit-DN4-core.dll**. The sole function of this DLL is to terminate the executing process, likely as a cleanup tactic pushed to infected machines that

the actors chose not to exploit.

```
using System;

// Token: 0x02000002 RID: 2
public class TestClass
{
    // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00002050
    public static void Run(string domain, string tag, string auth)
    {
        Environment.Exit(0);
    }
}
```

Figure 8 – exit-DN4-core.dll.

SameCoin and WIRTE – Disruptive Operations

In October 2024, a malicious email campaign was sent from the email address of a legitimate email of Israeli [ESET reseller](#), targeting multiple Israeli organizations, including hospitals and municipalities. The email contained a newly created version of the SameCoin Wiper, which was deployed in attacks against Israel earlier this year. In addition to minor changes in the malware, the newer version introduces a unique encryption function that has only been seen in WIRTE malware.

ESET Reseller SameCoin Wiper

The email alerts on alleged attack, and prompts recipients to click on the link which directs victims to a ZIP file named `ESETUnleashed_081024.zip`, which contains 4 legitimate DLLs and a malicious file `Setup.exe`.

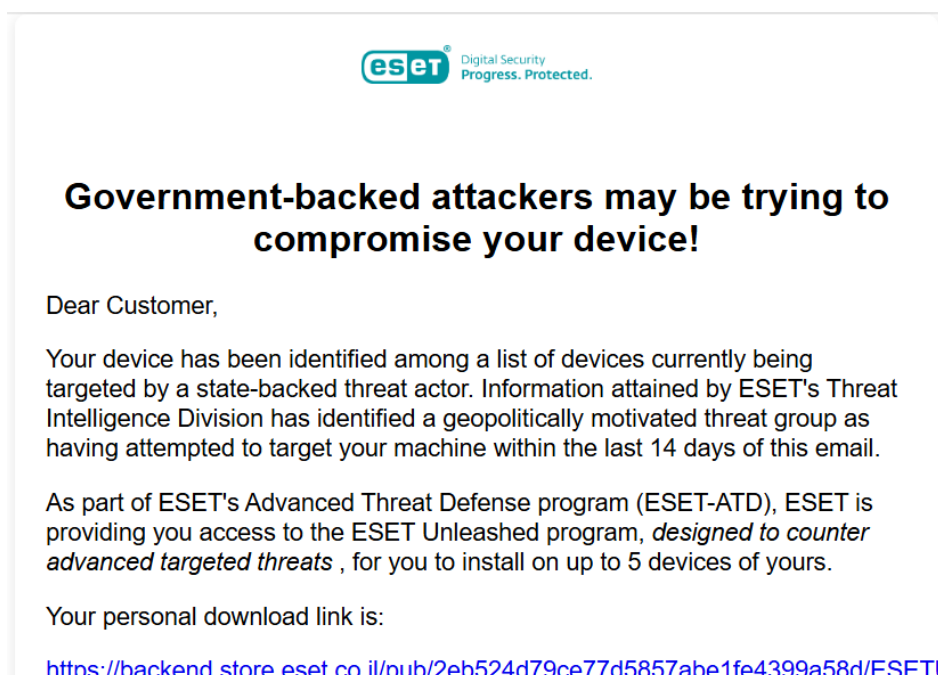


Figure 9 – Malicious email delivering the wiper

When launched, `Setup.exe` tries to connect to the Israel Home Front Command site [oref.org.il](#). It then uses the first bytes of the response as its XOR key. This website is accessible only from inside Israel; by using the response, the malware additionally verifies that the target is indeed Israeli.

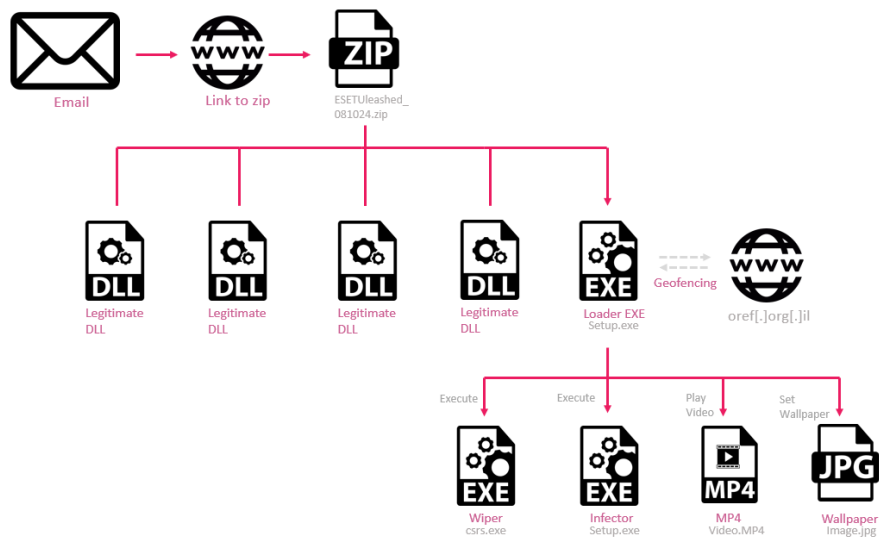


Figure 10 – Wiper Infection Chains.

The malware then drops and decrypts the next files to be executed:

- `image.jpg` – A wallpaper.



Figure 11 – Translated wallpaper mentioning Al-Qassam Brigades, the military wing of Hamas.

- `video.mp4` – Hamas propaganda video showing graphic attacks from October 7.
- `MicrosoftEdge.exe` – A **wiper** component.
- `csrs.exe` – An **Infector** component implementing two functions:
 - **InfectOutlook**: Sends `Setup.exe` as an attachment to other addresses in the same organization.
 - **InfectAD**: Copies the wiper file to remote machines within the same Active Directory and schedules it for execution using a Scheduled Task.

The wiper begins by listing all system files outside specified protected directories (e.g., Program Files, Windows, and Users). If a file's name doesn't contain "desktop.ini" or "conf.conf," it is overwritten with random bytes.

The [complete analysis](#) of the malware components was published by other researchers.

Code overlaps with IronWind loader

The XOR function used in the above wiper component (`MicrosoftEdge.exe`) is unique. It can only be found in a newer IronWind loader variant (`propsys.dll`). The IronWind variant uses the key `msasn1.dll`, and the wiper uses the key `Saturday, October 07, 2023, 6:29:00 AM`:



Figure 12 – Comparison of the encryption function in the IronWind sample and MicrosoftEdge.exe wiper.

This function implementation suggests that the same actor developed both tools and possibly were compiled in the same environment.

INCD SameCoin Wiper

This ESET wiper is a newer version of a previously reported [Samecoin](#) wiper, which was deployed on February 24 in a malicious campaign impersonating the Israeli National Cyber Directorate (INCD). SameCoin is a multi-platform wiper with Android and Windows versions, and in both cases, it impersonated an INCD security update.

The Windows variant starts by checking if the system language is configured to Hebrew, and if so, it drops 4 four additional files:

- Video.mp4 – Pro-Hamas propaganda video.
- Microsoft Connection Agent.jpg – Hamas wallpaper.
- Microsoft System Manager.exe – A **Wiper component**.
- Windows Defender Agent.exe – A **Tasks Spreader**: A component that tries to copy the loader to other machines in the network and executes tasks using remote schedule tasks.

The Android variant deployed as `INCD-SecurityUpdate-FEB24.apk` displays the same propaganda video as the Windows version. The wiper's functionality lies within the native library `libexampleone.so`. It starts by listing the files to be deleted, filling them with zeros, and then deleting them from the file system.

```

v3 = 0;
sub_2EEA0(v2, "/storage/emulated/0/", "");
std::__fs::filesystem::__status(v4, v2, 0);
if ( (v4[0] - 1) <= 0xFDu && (std::__fs::filesystem::__status(v4, v2, 0), v4[0]
{
    deleteDirectoryInChunksIteration(v2, 0xBB800000);
    __android_log_print(4, "FileLister", "Directory chunks deleted.", 186481);
    result = 1;
    if ( (v2[0] & 1) == 0 )
        return result;
}
else
{
    __android_log_print(6, "FileLister", "Directory not deleted.", 186481);
    result = 0;
    if ( (v2[0] & 1) == 0 )
        return result;
}
v1 = result;

```

Figure 13 – Android Wiper main function.

Infrastructure

C2 Redirects

Each malware sample we observed is configured with a unique user agent string. If this specific user agent is detected, the C2 server responds, otherwise, the C2 redirects the request to a legitimate website. Among the redirection chains we identified are:

- saudiday[.]org → saudi.org
- jordansons[.]com → jordantimes.com
- egyptican[.]com → dailynewsegypt.com
- inclusive-economy[.]com → inclusiveeconomy.us
- healthcarb[.]com → healthline.com

Phishing activity

Some domains observed in the infrastructure were set up with phishing pages designed to mimic the Docdroid file-uploading service.

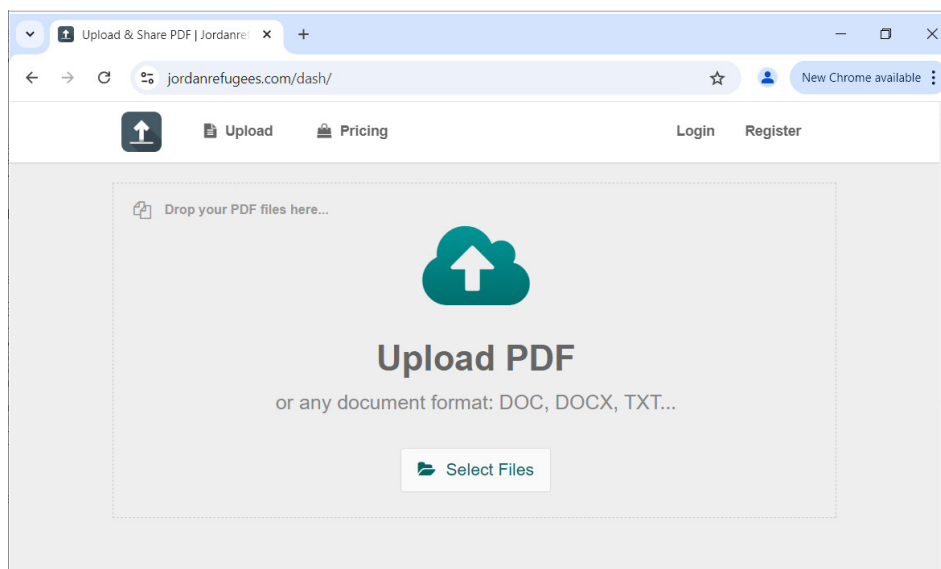


Figure 14 -WIRTE phishing page

These legitimate-looking websites contain specific URLs designed for phishing. When a victim accesses certain URLs, they are directed to phishing content or legitimate documents, possibly depending on the victim's IP address.

☐ Show password

Figure 15 – [https://suppertools\[.\]com/s/?uid=181b9056-7420-4cde-8523-5c609aface73](https://suppertools[.]com/s/?uid=181b9056-7420-4cde-8523-5c609aface73)



Figure 16 – [https://healthscratches\[.\]com/s/?uid=06d32218-178c-49d77-b3cf-59df77c93469](https://healthscratches[.]com/s/?uid=06d32218-178c-49d77-b3cf-59df77c93469)

WIRTE Attribution

We assess that WIRTE is likely connected to Hamas, based on the messaging observed in disruptive attacks, its consistent targeting of the Palestinian Authority (PA), and historical ties to groups associated with Hamas.

The most recent version of the SameCoin wiper alters the victim's background to display an image bearing the name of Hamas's military wing, the Al-Qassam Brigades. While this could be a potential false flag operation, we have not observed similar mentions in wiper attacks linked to other actors, including prominent Iranian groups.

The group's victims align strongly with Hamas's interests, focusing on Palestinian issues and frequently targeting the Palestinian Authority, Hamas's rival in the Palestinian political sphere.

Historically, WIRTE has been associated with the Molerats and the Gaza Cyber Gang, both of which have previously been connected to Hamas. This association was first identified by [Kaspersky](#) and further supported by reports from Proofpoint. In earlier WIRTE campaigns, the threat actor employed various tools, such as VBS and PowerShell scripts, while the signature techniques remained the same in the attacks discussed in this report:

- The C2 server responds only to specific user agents unique to each sample; otherwise, it redirects to a legitimate site.
- Retrieval of next-stage payloads embedded within HTML tags.

- Utilization of CloudFlare services.
- A consistent domain-naming theme focused on health, finance and countries in the region.

Victimology

The threat actor focused on various entities across the Middle East, mainly targeting the Palestinian Authority and Jordan, based on volumes of samples from those countries and the lures content Additional activity Indicators, including file submissions, lures, and domain references, also suggest likely targeting related to, Iraq, Saudi Arabia, and Egypt.

Samples in this campaign were uploaded from several major cities in the Middle East, including Ramallah, Baghdad, and Amman, with the following names:

Original Sample Name	Sample Name Translation
لقاء الممثلون الوطنيين لرؤساء الأركان للاتفاق على هيكل الأمن الإقليمي	National Representatives of Chiefs of Staff Meet to Agree on Regional Security Architecture
تقرير عن الوضع المالي للسلطة الفلسطينية	Report on the financial situation of the Palestinian Authority
سري – موافقة الأردن على إجراء حوار امني 12 مع ايران	12 Secret – Jordan agrees to hold security dialogue with Iran
بيروت – تطورات الحرب في لبنان 2 – 1178	1178 – Beirut – Developments of the war in Lebanon 2

Additionally, the majority of the phishing URLs were initially submitted to Virus Total from Jordan.




2024-04-01	https://healthscratches.com/s/?uid=06d32218-178c-4d77-b3cf-59df77c93469	 JORDAN	0	1
2024-06-12	https://mail.jordanrefugees.com/owa/auth/logo.n.aspx?uid=10d4925f-33b8-473e-90b7-cc8356cc4b81	 JORDAN	0	1
2024-06-12	https://mail.jordanrefugees.com/owa/auth/logo.n.aspx?uid=ffd7ba11-e7cb-4f59-a7f6-2a89c2ebe2a0	 JORDAN	0	1

Figure 17 – Phishing Urls submissions

Some of the domains associated with this operation referenced specific countries, which likely hints targeting of those :

- saudiarabianow[.]org
- saudiday[.]org
- jordanrefugees[.]com
- bankjordan[.]com
- jordansons[.]com
- egyptican[.]com
- egyptskytours[.]com
- egypttourism-online[.]com

On the disruptive side, the group solely focuses on Israel. The Wiper activity utilized propaganda content and themes aimed explicitly at Israeli audiences, with phishing emails targeting Israeli recipients. Additionally, the Wiper activates only if the target country is Israel or the system language is set to Hebrew.

The distinct techniques and payloads deployed against Israel differ from those employed in other Middle Eastern countries, indicating a dual purpose: to cause disruption in Israel and to conduct espionage in other Middle Eastern nations.

Conclusion

We revealed the activities and tools deployed by the longstanding WIRTE APT group over the past year. Despite ongoing conflict in the Middle East, the group has persisted with multiple campaigns, showcasing a versatile toolkit that includes Wipers, Backdoors, and Phishing pages used for both espionage and sabotage.

Our investigation also highlights WIRTE's continued reliance on tactics such as user agent filtering, payload building with HTML tags, redirection to news sites, and a consistent infrastructure style.

Despite previous analyses lacking definitive conclusions, our evaluation suggests that WIRTE is likely aligned with Hamas. This assessment is drawn from a close examination of WIRTE's operational history, which reveals patterns that resonate with Hamas's activities. Additionally, WIRTE's selection of targets, coupled with the nature of the content it distributes, further reinforces the connection between the conclusion.

Protections:

Threat Emulation:

- APT.Wins.Wirte.ta.A/B/C/D/E/F

Harmony End Point:

- ransom.win.honey
- infostealer.win.blackguard.d

IOCs

PE files:

2700142c0b78fdbf3df30125a72443e2317d5079a01ff26022a66d0b7bd4c5b1
3fc92e8a440ca16172f7d93bd9de3c6f9391e26d3a1cb964e966ee1ee31770df
5d773e734290b93649a41ccda63772560b4fa25ba715b17df7b9f18883679160
5fa809c0e5dff03bd202b86cd334e80c7ed5dbad9aed7b12a3799ea0800e5f31
0a4397f7d5da024b10c778910d6db84a6ba0fc3375fe6fe9b470f7e269ddc716
26cb6055be1ee503f87d040c84c0a7cacb245b4182445e3eee47ed6e073eca47
75c2fb3ae08502a57c8c96ea788ef946a8bb35fb4a16e76deefae4c94fd03fd7
86791aa96bac086330bf927ea5c2725ff73aaedfadc2571f4f393aa4d3a6b690
8ce87eefded0713c9258f8f2086dcc51028fb404ceb526f832df4c93108c8146
8818c7c2cbd60521b8eb59ff9a720840535651343b30c1b279515d42d8036a8a
7e0d0f77fe1dcb1e7a0a0a2fc0c25a68eee551c7045935449ae64dcbd1310958
795b997c248b2f344f813cd0c15d3d435e6218c91d0f0f54a464d739fee4dc5
9fc4c7cdcaa3c3c03ba65f138386e875d02f7fcaf10de720dfde20167e393f38
7c0a8d3dec1675fd8ba0a73fb5b8eee3bef0214aa78a7aab73b8ba9814651f9f
b447ba4370d9becf9ad084e7cdf8e1395bafde1d15e82e23calb9808fef13a7
9b2a16cbe5af12b486d31b68ef397d6bc48b2736e6b388ad8895b588f1831f47
c51952f2caf55b455e7c7eb8048422bb477e3a616cb68f6fa524e15892b9f328
d3a53be1f64325c566bb71222b3747da81439dea8fc9a458fb459355cfa9e7f2
ac227dd5c97a36f54e4fa02df4e4c0339b513e4f8049616e2a815a108e34552f
c068b9e7130f6fb5763beb9564e92a89644755f223b2f65dc762ed5c77c5b8e3
c22f0544e29c803d2cacbca3a57617496e3691389e9b65da84c374c90e699433
76a543a49e46ad9163b2a06f6cea7a5e8eb5183cd3213e64446a8c66310fac3a
e2ba2d3d2c1f0b5143d1cd291f6a09abe1c53e570800d8ae43622426c1c4343c
02902a5e07a80aa56c24c6a8d4cca9fcfb32f32bb074f9c449cad5b3b18a070c
e6d2f43622e3ecdce80939eec9fffb47e6eb7fc0b9aa036e9e4e07d7360f2b89
3b4ee3d5c1a7202b053159becac4d0b622641e2e4a7b27f339c03a90f287d381
f2de8a5daed043ef3ab1f52156a4f7ff8f9a382f7f58ace6abb463f5cbab060c
fca0b3e57b3f9a14d18c435e564fe6db3620ba446e1b863737a9b36cbcc7251a
eddd40d457088d8384784ce80eaf0aefb1485776e0916e60781befbd739d4608
6ab5a0b7080e783bba9b3ec53889e82ca4f2d304e67bd139aa267c22c281a368
2abff990d33d99a0e7ceddbb3a39831c2c292f36955381d45cd8d40a816d9b47a

Archives:

9fe7b2f4c17dd0c7a00aaa6a779c30e2cb3faa4b14766e02f616d00e6f6e9007
3d2409c7834287178f61116c9b653e3520172a10ebef58f58f99d27a34b839bd
5b7e8e685f6ee6b4810ed94b4420e08a10a977516b47fea356173cfaec2c41a0
41112f36fc17f57f0e476c9ffa9e1ecbfff796dc31a7ff0372d0d8708a5e9c50b
2d55c68aa7781db7f2324427508947f057a6baca78073fee9a5ad254147c8232

PDF:

b7c5af2d7e1eb7651b1fe3a224121d3461f3473d081990c02ef8ab4ace13f785

Infrastructure:

Domain	Backend Server IP
saudiday[.]org	185.158.248[.]161
jordansons[.]com	193.168.141[.]29
egyptican[.]com	140.99.164[.]56
healthcarb[.]com	160.119.251[.]181
inclusive-economy[.]com	188.92.78[.]148
king-pharmacy[.]com	185.165.169[.]76
microsoftwindowshelp[.]com	45.134.9[.]202
economystocking[.]com	37.120.247[.]22
wellhealthtech[.]com	195.123.210[.]42
microsoftliveforums[.]com	140.99.164[.]86
master-dental[.]com	213.252.244[.]234

dentalaccord[.]com	5.42.221[.]151
economymentor[.]com	37.221.65[.]254
bankjordan[.]com	80.77.25[.]49
egyptskytours[.]com	193.168.141[.]61
microsoftteams365[.]com	185.247.224[.]28
finance-analyst[.]com	185.158.248[.]201
trendingcharts.finance-analyst[.]com	
finances-news[.]com	185.165.169[.]117
pushservice_api.finances-news[.]com	
support-api.financecovers[.]com	45.59.118[.]145
jordanrefugees[.]com	37.120.247[.]100
egypttourism-online[.]com	185.225.70[.]168
healthoptionstoday[.]com	80.77.25[.]216
ellemedic[.]com	38.180.151[.]206
easybackupcloud[.]com	
financeinfoguide[.]com	
healthscratches[.]com	
printspoolerupdates[.]com	
saudiarabianow[.]org	
suppertools[.]com	
theshortner[.]com	