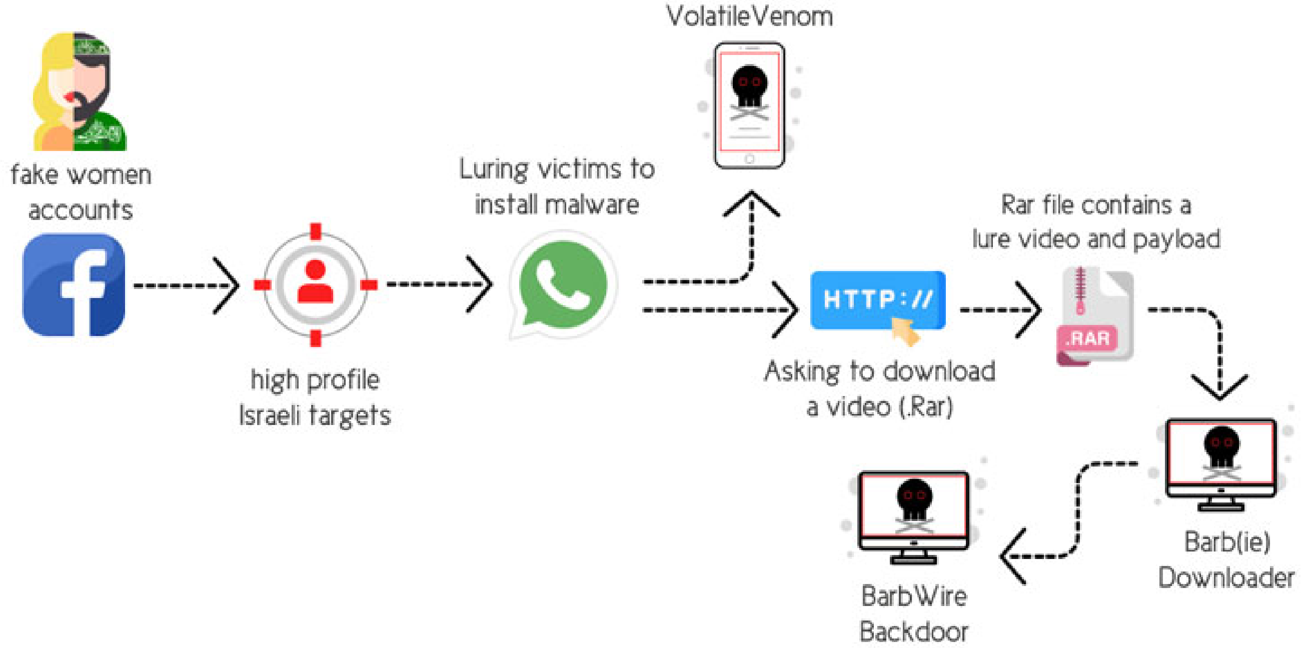
# Hamas-linked Hackers Targeting High-Ranking Israelis Using 'Catfish' Lures

thehackernews.com/2022/04/hamas-linked-hackers-targeting-high.html

April 7, 2022


fake women accounts
high profile Israeli targets
Luring victims to install malware
VolatileVenom
HTTP://
Asking to download a video (.Rar)
Rar file contains a lure video and payload
.RAR
Barb(ie) Downloader
BarbWire Backdoor

A threat actor with affiliations to the cyber warfare division of Hamas has been linked to an "elaborate campaign" targeting high-profile Israeli individuals employed in sensitive defense, law enforcement, and emergency services organizations.

"The campaign operators use sophisticated social engineering techniques, ultimately aimed to deliver previously undocumented backdoors for Windows and Android devices," cybersecurity company Cybereason said in a Wednesday report.

"The goal behind the attack was to extract sensitive information from the victims' devices for espionage purposes."

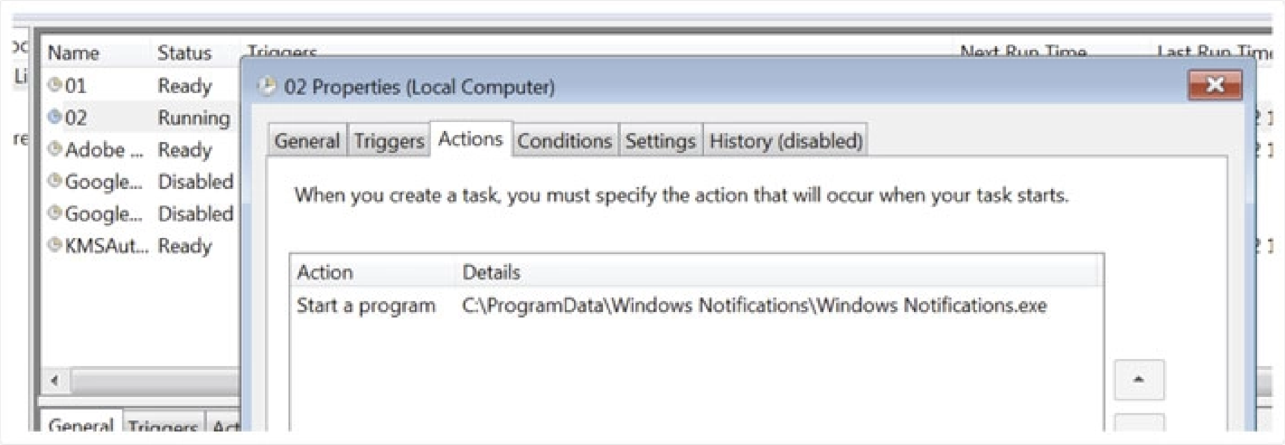
The monthslong intrusions, codenamed "**Operation Bearded Barbie**," have been attributed to an Arabic-speaking and politically-motivated group called Arid Viper, which operates out of the Middle East and is also known by the monikers APT-C-23 and Desert Falcon.

Most recently, the threat actor was held responsible for attacks aimed at Palestinian activists and entities starting around October 2021 using politically-themed phishing emails and decoy documents.

The latest infiltrations are notable for their specific focus on plundering information from computers and mobile devices belonging to Israeli individuals by luring them into downloading trojanized messaging apps, granting the actors unfettered access.

The social engineering attacks involved the use of fake personas on Facebook, relying on the tactic of catfishing to set up fictitious profiles of attractive young women to gain the trust of the targeted individuals and befriend them on the platform.

"After gaining the victim's trust, the operator of the fake account suggests migrating the conversation from Facebook over to WhatsApp," the researchers elaborated. "By doing so, the operator quickly obtains the target's mobile number."



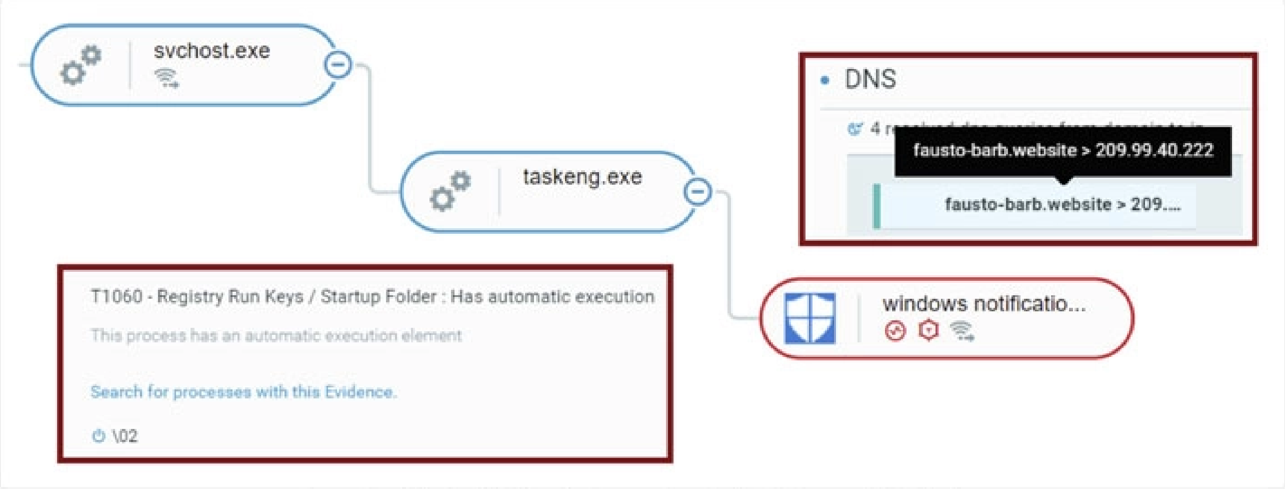
| Name | Status | Triggers | Next Run Time | Last Run Time |
|---|---|---|---|---|
| 01 | Ready | | | |
| 02 | Running | | | |
| Adobe ... | Ready | | | |
| Google... | Disabled | | | |
| Google... | Disabled | | | |
| KMSAut... | Ready | | | |

02 Properties (Local Computer)

When you create a task, you must specify the action that will occur when your task starts.

| Action | Details |
|---|---|
| Start a program | C:\ProgramData\Windows Notifications\Windows Notifications.exe |

*Two scheduled tasks created by Barb(ie) downloader for persistence*



fausto-barb.website > 209.99.40.222

fausto-barb.website > 209....

T1060 - Registry Run Keys / Startup Folder : Has automatic execution

This process has an automatic execution element

Search for processes with this Evidence.

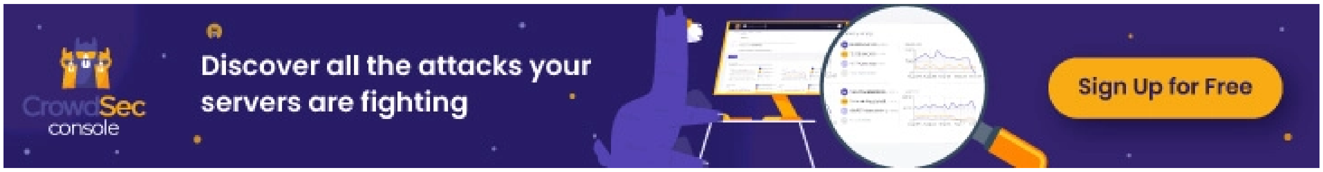
\02

*Execution of the Barb(ie) downloader as shown in the Cybereason XDR Platform*

Once the chat shifts from Facebook to WhatsApp, the attackers suggest the victims that they install a secure messaging app for Android (dubbed "VolatileVenom") as well as open a RAR archive file containing explicit sexual content that leads to the deployment of a malware downloader called Barb(ie).

Other hallmarks of the campaign have included the group leveraging an upgraded arsenal of malware tools, including the BarbWire Backdoor, which is installed by the downloader module.

The malware serves as a tool to completely compromise the victim machine, allowing it to establish persistence, harvest stored information, record audio, capture screenshots, and download additional payloads, all of which is transmitted back to a remote server.



VolatileVenom, on the other hand, is Android spyware that's known to spoof legitimate messaging apps and masquerade as system updates and which has been put to use in different campaigns by Arid Viper since at least 2017.

One such example of a rogue Android app is called "Wink Chat," where victims attempting to sign up to use the application are presented an error message that "it will be uninstalled," only for it to stealthily run in the background and extract a wide variety of data from the mobile devices.

"The attackers use a completely new infrastructure that is distinct from the known infrastructure used to target Palestinians and other Arabic-speakers," the researchers said.

"This campaign shows a considerable step-up in APT-C-23 capabilities, with upgraded stealth, more sophisticated malware, and perfection of their social engineering techniques which involve offensive HUMINT capabilities using a very active and well-groomed network of fake Facebook accounts that have been proven quite effective for the group."

SHARE □ □ □ □ ךָ
SHARE □