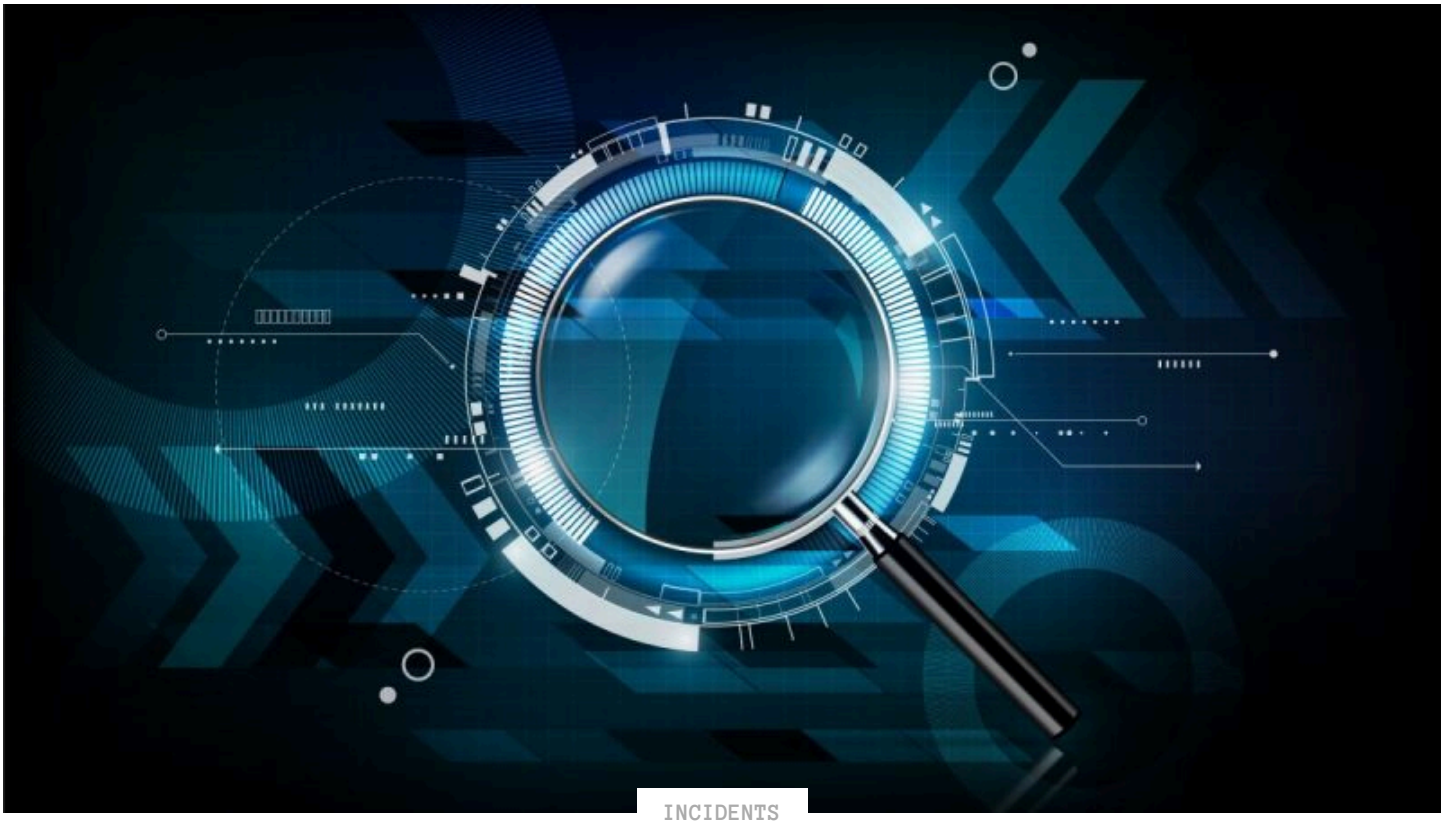

INCIDENTS

A hack in hand is worth two in the bush

16 OCT 2023 4 minute read

Table of Contents

Dissecting the alleged hack of a private power station in Israel

The ongoing conflict between Israel and Hamas has also extended into the digital domain. The involvement of hackers highlights the evolving nature of warfare in the 21st century, where traditional military operations are complemented by sophisticated cyber tactics, and where the boundaries between state-sponsored, hacktivist, and independent actors blur.

So far, various cyber activities in the digital realm have been observed, including DDoS-attacks, information warfare, and hacktivism campaigns. As the conflict continues, we anticipate potential wiper or ransomware malware attacks in the future.

On October 8, a major hack on the Israeli Dorad private power station was announced on underground channels by the Cyber Av3ngers group. The group shared photos of the alleged hack with a logo that has the Palestinian flag colors and political messages, inferring the hack was in support. This claim was announced in parallel with another one about targeting the Dorad website with a DoS-attack to add credibility to the hack: the attackers also presented evidence of their DDoS success. We analyzed the data published by Cyber Av3ngers and found it to be sourced from older leaks by another hacktivist group called Moses Staff.

It has been alleged that Moses Staff is an Iranian hacker group, first identified on underground forums in September 2021. Their main activity is to damage Israeli companies by stealing and publishing sensitive data. The group also targets organizations from other countries like Italy, India, Germany, Chile, Turkey, UAE and the US. It's important to mention that no evidence was found linking the Cyber Av3ngers group and the Moses Staff actors.

Introduction on Cyber Av3ngers

There is a group with a similar name called "Cyber Avengers", a threat actor that has been active since at least 2020. There is little evidence connecting Cyber Avengers with Cyber Aveng3rs or Cyber Av3ngers. However, with the current geopolitical conflict, they started to attract publicity to their activities and show support to the cause. They mainly target Israeli organizations, mostly those responsible for operating the critical infrastructure of the country. In 2020, Cyber Avengers claimed responsibility for the power cut and railway infrastructure hack. Later that year, the VP of the corresponding electrical company made a statement saying the power outage was not caused by a cyber attack but a "technical fault".

On September 15 2023, a new channel was created on Telegram messenger with the handle @CyberAveng3rs. The channel started with messages that link its owners to the past activities done by "Cyber Avengers", then adding information on their ideas to target Israeli critical infrastructure, including electrical and water systems.
The latest post on the channel was about a security guidance, which had been prepared for infrastructure security and published by the Israeli government. The Cyber Avengers group sent the guidance across the list of targets as a mockery. The list contains eight companies with the eighth yet to be updated.

Analysis of the Cyber Av3ngers files

The original Moses Staff leak files from 2022 are not available anymore from the original links. However, the files still can be found on other underground channels.

File Name	POC-IPC.rar
MD5	f9a34ac80a4f98b5491594a1eedc74e3
SHA256	f3b4ee57c46839c2305f68962dff5cd5c3cab0e48d1fbf4f5f4d11f7258ea99b
Comments	Archive file with leaked data from multiple organizations
Create Time/Date	14-Jun-22 11:59AM
File size	159,574 KB

The archive was first published by Moses Staff in June 2022, it included leaked data from multiple companies in Israel. The files related to the Dorad private power station hack (11 files), had timestamps from August 2020, and the compression timestamps point to June 14 2022. The data in the archive was in PDF documents in addition to PNG and JPEG photos. A video was also published by the attackers in parallel with the data leak.
Comparing the photos posted by Cyber Av3ngers and the originals from the Moses Staff archive, we were able to observe the following:

- Cyber Av3ngers took photos from the Moses Staff leaked PDF documents and video.
- Cyber Av3ngers cropped the photos and added the logo image before publishing.

The comparison between the images from the Moses StaffJune 2022 leak and the images from the Cyber Av3ngers October 8 2023 alleged leak, can be found below.
Overall, the leaked data seems to be the result of hacking operations by Moses Staff: the files seem to have been exfiltrated through the use of malware from computers belonging to the targeted organization, and this behavior has been carried out by this threat actor using custom tools, such as PyDCrypt, DCSrv, and StrifeWater. PyDCrypt is a program written in Python and built with PyInstaller that is used to infect other computers on the network and ensure that the main payload DCSrv is executed properly. DCSrv is a malicious process masquerading as the legitimate "svchost.exe" process. DCSrv blocks all access to the computer and encrypts all its volumes using the legitimate open-source encryption utility DiskCryptor. StrifeWater is a stealthy Remote Access Trojan (RAT) that is used in the initial stage of the attack to cover traces. In addition, it has the ability to execute remote commands and capture the screen.
Since the Moses Staff group is not attempting financial gain, and its main objective is to cause damage, there is usually no way to pay the ransom and decrypt the data.

Conclusion

Based on the information provided and its analysis, the Cyber Av3ngers alleged hack is recycled or repurposed from a prior security breach and is not the result of any new unauthorized access to data. Nevertheless, threat actors such as MosesStaff, targeting users and organizations, especially in critical infrastructure environments, are still active.

It's important to investigate such incidents thoroughly to understand the nature of the compromised data, how it was obtained, and whether any security vulnerabilities were exploited. Additionally, it emphasizes the importance of maintaining strong cybersecurity measures to protect against both new and recurring threats to IT and OT systems.

Indicators of Compromise

File hashes
48220a3a4c72317ae0fbb08e255b8350

4cba27111c5fca7a1ae78566de2df5b3
a7704fbccaeb78678a5f94714993567c
aa579d5f062f02d9ff76910560bb312c
f8c06e955718639ba9ffdd4265965593

Leaks comparison data

Images from the Moses StaffJune 2022 leak	Images from the Cyber Av3ngers October 8 2023 leak claim

DATA LEAKS HACKTIVISTS INDUSTRIAL THREATS MALWARE SOCIAL NETWORKS TARGETED ATTACKS

Authors

Expert GREAT

A hack in hand is worth two in the bush

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

// LATEST POSTS

Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia

KASPERSKY

SAS CTF and the many ways to persist a kernel shellcode on Windows 7

IGOR KUZNETSOV, BORIS LARIN

Beyond the Surface: the evolution and expansion of the SideWinder APT group

GIAMPAOLO DEDOLA, VASILY BERDNIKOV

Whispers from the Dark Web Cave. Cyberthreats in the Middle East

VERA KHOLOPOVA, KASPERSKY SECURITY SERVICES

// LATEST WEBINARS

THREAT INTELLIGENCE AND IR

04 SEP 2024, 5:00PM 60 MIN

Inside the Dark Web: exploring the human side of cybercriminals

ANNA PAVLOVSKAYA

TECHNOLOGIES AND SERVICES

13 AUG 2024, 5:00PM 60 MIN

The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise

OLEG GOROBETS, ALEXANDER LISKIN

CYBERTHREAT TALKS

16 JUL 2024, 5:00PM 60 MIN

Cybersecurity's human factor – more than an unpatched vulnerability

OLEG GOROBETS

TRAININGS AND WORKSHOPS

09 JUL 2024, 4:00PM 60 MIN

Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

// REPORTS

Beyond the Surface: the evolution and expansion of the SideWinder APT group

Kaspersky analyzes SideWinder APT's recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

BlindEagle flying high in Latin America

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

APT trends report Q2 2024

// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

Subscribe

I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

Threats

Categories

Archive
Webinars
Statistics
Threats descriptions

All tags
APT Logbook
Encyclopedia
KSB 2023