blog.sekoia.io /aridviper-an-intrusion-set-allegedly-associated-with-hamas/

AridViper, an intrusion set allegedly associated with Hamas

⁝ 10/26/2023

Given the recent events involving the Palestinian politico-military organisation Hamas which conducted on 7 October 2023 a military and terrorist operation in Israel, Sekoia.io took a deeper look into **AridViper**, an intrusion set suspected to be associated with Hamas.

Context

Hamas, officially the Islamic Resistance Movement, is a Sunni-Islamic fundamentalist and nationalist movement in Palestine. It is considered a terrorist organisation by the European Union. Hamas won the 2006 Palestinian legislative elections – the last held in the Palestinian territories – against its rival Fatah, the historical Palestinian independence movement.

Hamas is *de facto* the **governing authority** of **the Gaza Strip** since its takeover in June 2007, while the **Fatah**-ruled Palestinian National Authority **administers** the Palestinian **West Bank**. Both movements are in **competition** for the Palestinian independence leadership.

Hamas is supported by the Islamic Republic of Iran and the Lebanese-based Hezbollah movement, both adversaries of Israel. Relations between Iran and Hamas consist of military, financial and political aid to Hamas.

Background

AridViper, also known as APT C-23, MoleRATs, Gaza Cyber Gang or Desert Falcon, is an alleged Hamas-associated intrusion set active since at least 2012. The group, first exposed by Trend Micro in February 2015, was observed by multiple cybersecurity vendors carrying cyber **espionage operations** on **both Palestinian and foreign targets**, mostly located in Israel and in the Middle-East. AridViper leverages Windows-based, iOS and Android malwares.

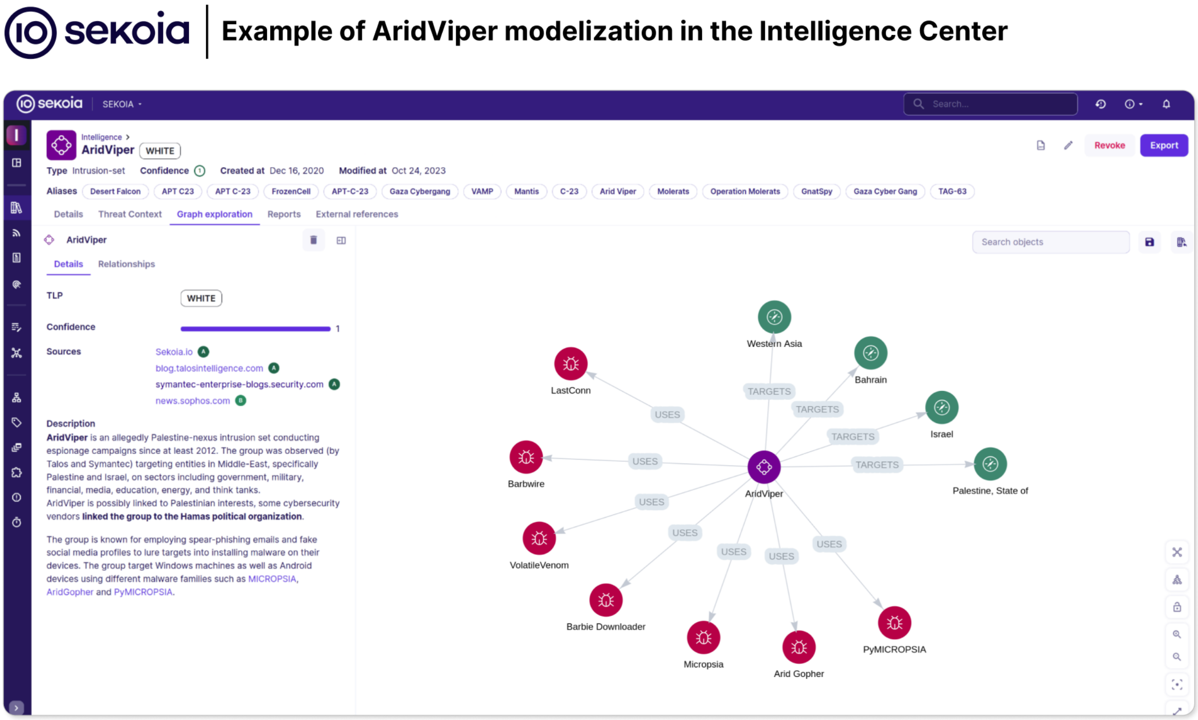
In recent years, their malware arsenal was mainly designed to exfiltrate data from compromised hosts. The group is known for its use of targeted phishing emails and fake social media profiles to entice targets into installing malicious software on their devices.

sekoia
Examples of AridViper decoy documents
STATE OF PALESTINE
COUNCIL OF MINISTERS
CABINET SECRETARIAT
دولــــة فلسطــــين
مجلس الوزراء
الأمانة العامة
DEPUTY
Manal Sh CV
GRAPHIC DESIGNER
CONTACT
OBJECTIVE
EDUCATION
SKILL
WORK EXPERIENCE
LANGUAGES
HOBBIES
Courses
REFERENCES

(Click on the image for a better view)

Once the host is compromised, the attacker can download or upload arbitrary files onto the victim's system, capture data from input devices such as keyboards or microphones, and execute system commands directly via a Command and Control (C2) server.

Since 2020, Arid Viper uses PyMICROPSIA Trojan, a Python-adapted version of the original Delphi-based Micropsia, along with the Arid Gopher backdoor. Infections pathways employed by this group of malware are documented, and their persistence throughout 2023 is attributed to the ongoing functionality of their infrastructure. On October 6, 2023, in an abstract for a Virus Bulletin conference, ESET announced the discovery of a new Rust-developed backdoor called Rusty Viper, suggesting that the group continues to enhance its offensive capabilities.



Example of AridViper modelization in the Intelligence Center

Intelligence >
AridViper WHITE

Type Intrusion-set Confidence 1 Created at Dec 16, 2020 Modified at Oct 24, 2023

Aliases Desert Falcon APT C23 APT C-23 FrozenCell APT-C-23 Gaza Cybergang VAMP Mantis C-23 Arid Viper Molerats Operation Molerats GnatSpy Gaza Cyber Gang TAG-63

AridViper

TLP WHITE

Confidence 1

Sources Sekoia.io A
blog.talosintelligence.com A
symantec-enterprise-blogs.security.com A
news.sophos.com B

Description
AridViper is an allegedly Palestine-nexus intrusion set conducting espionage campaigns since at least 2012. The group was observed (by Talos and Symantec) targeting entities in Middle-East, specifically Palestine and Israel, on sectors including government, military, financial, media, education, energy, and think tanks.
AridViper is possibly linked to Palestinian interests, some cybersecurity vendors **linked the group to the Hamas political organization**.

The group is known for employing spear-phishing emails and fake social media profiles to lure targets into installing malware on their devices. The group target Windows machines as well as Android devices using different malware families such as MICROPSIA, AridGopher and PyMICROPSIA.

(Click on the image for a better view)

AridViper’s victimology analysis

The victimology presented here is based on the analysis of open source reports on AridViper APT or MoleRATS, an intrusion set Sekoia.io assess to be an alias of the same group.

AridViper carrying operations on Israel and Middle-Eastern targets since at least 2015

AridViper was reported targeting multiple sectors based in the Middle-East, such as telecommunications, insurance, retail, media, academics, high ranking military and government officials. The group mostly impacted Israel, but operations targeting Arabic countries were also reported, including an organisation in Bahrain, a media organisation in Algeria, as well as human rights activists and journalists in Turkey.

In 2015, a wide spearphishing campaign was observed by TrendMicro – *dubbed AridViper Operation, the alias then being used to follow the intrusion set* – impacting an Israeli government office, a military organisation and an academic institution in Tel Aviv, among others. In 2017 and 2020, Israel Defense Force reported cyber espionage campaigns targeting Israeli soldiers, an operation CheckPoint associated with AridViper activities. In 2022, Cyber Reason reported a campaign that targets Israeli officials aiming to collect information from individuals working for law enforcement, military and emergency services.

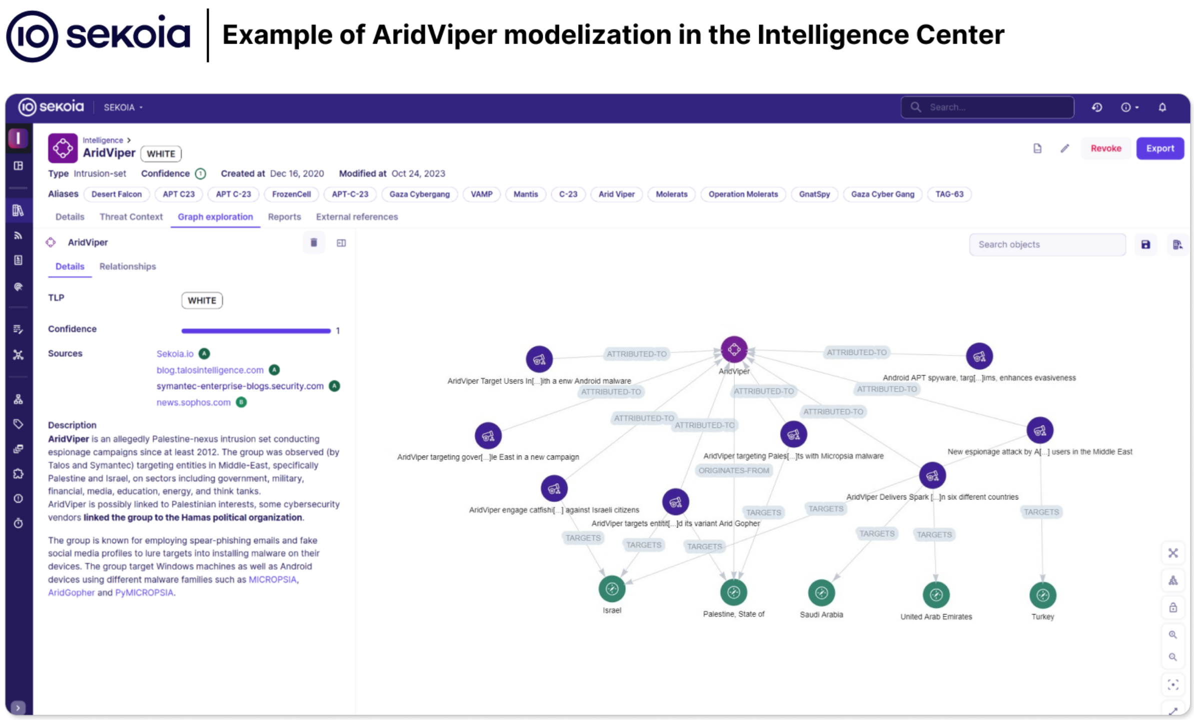
Sekoia.io assess it is likely **AridViper contributes to Hamas efforts on intelligence collection** about its **geopolitical adversaries**, from strategic to operational espionage.

AridViper long standing surveillance operation on Palestinian targets

On another side, AridViper was observed carrying multiple operations targeting Palestinian entities. Among the known targets are high value individuals working in the banking sector in Palestine, linked to Palestinian political parties or involved in NGOs operating in Gaza and in the West Bank, as reported by Zscaler in 2020.

Other campaigns were observed leveraging politically themed spearphishing related to geopolitical conflicts between Israel and Palestine, targeting individuals located in Palestine, a focus confirmed by Symantec in April 2023. For instance, some lures used by AridViper include topics such as the assassination of Iranian general Qasem Soleimani in January 2020 or the ongoing conflict between Hamas and Fatah movements.

Sekoia.io assess it is possible that **AridViper** contributes to **Hamas surveillance** intelligence **against political opposition** within Palestine – on **Fatah**, **Palestinian Authority**, or any civil society entities – NGO members or journalists susceptible to be critical against Hamas.



Example of AridViper modelization in the Intelligence Center

Intelligence >
AridViper WHITE

Type Intrusion-set   Confidence 1   Created at Dec 16, 2020   Modified at Oct 24, 2023

Aliases: Desert Falcon, APT C23, APT C-23, FrozenCell, APT-C-23, Gaza Cybergang, VAMP, Mantis, C-23, Arid Viper, Molerats, Operation Molerats, GnatSpy, Gaza Cyber Gang, TAG-63

AridViper

TLP: WHITE

Confidence: 1

Sources: Sekoia.io A, blog.talosintelligence.com A, symantec-enterprise-blogs.security.com A, news.sophos.com B

Description

AridViper is an allegedly Palestine-nexus intrusion set conducting espionage campaigns since at least 2012. The group was observed (by Talos and Symantec) targeting entities in Middle-East, specifically Palestine and Israel, on sectors including government, military, financial, media, education, energy, and think tanks.
AridViper is possibly linked to Palestinian interests, some cybersecurity vendors **linked the group to the Hamas political organization**.

The group is known for employing spear-phishing emails and fake social media profiles to lure targets into installing malware on their devices. The group target Windows machines as well as Android devices using different malware families such as MICROPSIA, AridGopher and PyMICROPSIA.

SEKOIA
Search...
Revoke
Export
Details
Threat Context
Graph exploration
Reports
External references
Details
Relationships
Search objects
AridViper Target Users In[...]ith a enw Android malware
ATTRIBUTED-TO
AridViper
ATTRIBUTED-TO
Android APT spyware, targ[...]ims, enhances evasiveness
AridViper targeting gover[...]le East in a new campaign
AridViper targeting Pales[...]ts with Micropsia malware
ORIGINATES-FROM
New espionage attack by A[...] users in the Middle East
AridViper engage catfishi[...] against Israeli citizens
AridViper targets entitit[...]d its variant Arid Gopher
AridViper Delivers Spark [...]n six different countries
TARGETS
Israel
Palestine, State of
Saudi Arabia
United Arab Emirates
Turkey

(Click on the image for a better view)

A related infrastructure still up nowadays

On **11 October 2023**, Sekoia.io TDR analysts conducted an **extended analysis** on the command and control (C2) infrastructure used by AridViper, based on indicators of compromise (IOC) previously published by Symantec and CoreSec360.

We were able to find **new exclusive domain names** added to **AridViper C2 infrastructure** in 2023, which are **still active as of 24 October 2023**. The domains are as follows, sorted by their first seen date to an IPv4 address.

Domain name	First Seen	Current IPv4
izocraft[.]com	24/09/2023	91.199.147[.]84

cricket-live[.]net	07/08/2023	95.164.18[.]204
sports-et-loisirs[.]net	12/07/2023	146.19.106[.]37
leaf-japan[.]net	05/07/2023	94.131.98[.]3
london-sport[.]net	03/07/2023	185.231.207[.]23
anime-con[.]net	29/05/2023	185.231.207[.]84
lrxzklwmzxe[.]com	27/04/2023	95.164.46[.]44
im-inter[.]net	22/03/2023	185.33.24[.]249
dslam[.]net	14/03/2023	185.43.221[.]132
it-franch-result[.]info	06/02/2023	194.4.49[.]123
jasondixon[.]net	31/12/2022	146.19.233[.]28

Based on the ‘first seen’ dates of the resolution of these domains on the listed IP addresses, Sekoia.io analysts assess **AridViper infrastructure continues to be regularly maintained** and updated by its operators. Off note, the domains sports-et-loisirs[.]net, im-inter[.]net and dslam[.]net are no longer active as of 23 October 2023.

Among the domains uncovered by Sekoia.io investigation, some of them were **previously exposed by other cybersecurity vendors** and are still active as of 24 October 2023:

Domain name	First Seen	Current IPv4
gsstar[.]net	28/05/2023	185.231.204[.]16
acs-group[.]net	22/03/2023	91.228.10[.]119
tophatauc[.]com	31/01/2023	185.81.113[.]54
gmesc[.]com	30/01/2023	185.209.160[.]77
seomoi[.]net	18/01/2023	94.131.110[.]78

Conclusion

AridViper seems to be organised in **two subgroups**, one conducting **cyber espionage** activities towards **Israel** and any entities in the **Middle-East region** susceptible to be involved in Palestine affairs, the second focusing on **surveillance activities towards Palestinian Hamas opposition** including the Fatah rival movement or individuals linked to the Palestinian Authority.

Based on Sekoia.io technical investigation on AridViper infrastructure, we can confirm **the group was active the last months**, and **still currently operating**, although we did not find any clues whether AridViper increased its activities or not before and during the Hamas 7 October attack.

It is possible that the physical location of AridViper operators will be part of **Israeli Air Force bombings**, as the Israeli military already conducted raids against objectives in the Gaza Strip that **housed** centres for **Hamas** cyber operations in 2019 and 2021.

Based on the documented collaboration between Iran, Hamas and Lebanon-based Hezbollah, it is **worth questioning** whether Iran, known for its cyber offensive capabilities and Israel targeting, collaborates with AridViper or any Hamas cyber capacities, since Hezbollah-associated Polonium APT is suspected of coordination with intrusion sets affiliated with Iran intelligence. To date, Sekoia.io did not find any technical evidence in line with this hypothesis.

Indicators Of Compromise (IoCs)

Domains mentioned in this blog post, found during our investigation.

```
izocraft[.]com
cricket-live[.]net
sports-et-loisirs[.]net
leaf-japan[.]net
london-sport[.]net
anime-con[.]net
gsstar[.]net
lrxzklwmzxe[.]com
im-inter[.]net
acs-group[.]net
dslam[.]net
it-franch-result[.]info
delooyp[.]com
tophatauc[.]com
gmesc[.]com
seomoi[.]net
jasondixon[.]net
```

Thank you for reading this blogpost. **We welcome any reaction, feedback or critics about this analysis. Please contact us on tdr[at]sekoia.io**.

Feel free to read other TDR analysis here :