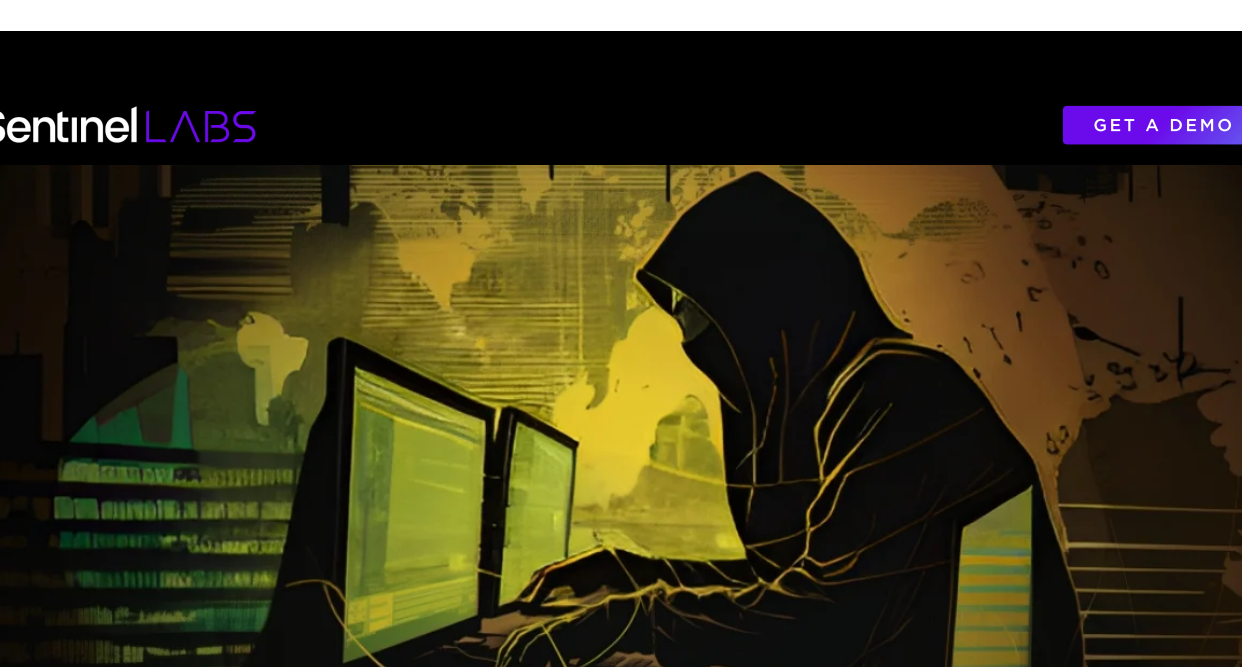
SentinelLABS

GET A DEMO



ADVANCED PERSISTENT THREAT

The Israel-Hamas War | Cyber Domain State-Sponsored Activity of Interest

TOM HEGEL / OCTOBER 24, 2023

By Tom Hegel and Aleksandar Milenkoski

Since the start of the Israel-Hamas war, the cyber domain has played a critical role in the conflict, albeit in ways the world may not have expected. Immediately following the attacks from Hamas on October 7th, social media became a hotbed of disinformation, inaccurate self-described OSINT investigators, and public confusion. Unfortunately, leading social media platforms continue to fail at stopping the spread of disinformation regarding this war. We will continue to see it abused as a go-to method to sway public perception of events with no signs of it ending soon.

However, outside of social media information abuse and opportunistic-hacktivism, we must not forget the likelihood of targeted attacks originating from specific, state-sponsored threat actors. Understanding and closely monitoring all-aspects of the quickly evolving conflict within the digital domain is critical as such targeted attacks will translate into real-world consequences. While we continue to collaborate privately with partners, we also seek to bolster the wider industry knowledge about where to place our efforts.

This is an updated compendium of actors for cybersecurity researchers, analysts, and network defenders to watch closely. These actors have potential for significant involvement as the war continues, including APTs across Hamas, Hezbollah, and Iran-based clusters of activity. While state-sponsored APTs should remain a strong focus, we must also carefully monitor the increasingly common use of hacktivist personas used to cloak state-sponsored operations.

In this post, we share recommended and publicly accessible information in effort to streamline the community's understanding of relevant actors across historical reports for reference. In addition, we are sharing our perspective of public actor naming overlaps. Please note that each source of public reporting may perform attribution and actor clustering uniquely from their perspective. Nonetheless, these sources should serve as starting points for readers looking to catch up on relevant open-source intelligence for your own defense posturing and analysis needs.

Hamas -Aligned Clusters

Arid Viper

Aliases:

- APT-C-23
- Grey Karkadann
- Desert Falcon
- Mantis

Description:

Arid Viper is a threat group conducting cyber espionage and information theft operations since at least 2017, predominantly against targets in the Middle East. Based primarily on the geopolitical context of its activities, Arid Viper is suspected to operate on behalf of Hamas with further conclusive information needed to solidify this assessment. For example, the Israeli Defence Forces (IDF) have reported on a campaign targeting soldiers stationed near the Gaza border, which is suspected to be orchestrated by Hamas. This campaign has been separately attributed with medium confidence to Arid Viper based on victimology and similarities with previous activities attributed to this actor such as overlaps in initial infection techniques.

Targeting individuals is a common practice of Arid Viper. This includes pre-selected Palestinian and Israeli high-profile targets as well as broader groups, typically from critical sectors such as defense and government organizations, law enforcement, and political parties or movements. Common initial infection vectors include social engineering and phishing attacks using themed lure documents. The latter often involves establishing rapport with targets over social media, such as Facebook and Instagram, with catfishing being a frequently used technique.

Arid Viper uses a variety of malware as part of its operations, including stagers, backdoors, and mobile spyware applications for the iOS and Android platforms. Arid Viper's malware is actively maintained and upgraded to meet the group's operational requirements. This threat actor has consistently demonstrated innovation by adopting new malware development practices across a range of programming and scripting languages, such as Delphi, Go, Python, and C++.

Gaza Cybergang

Aliases:

- Molerats
- TA402
- Gaza Hackers Team
- Moonlight
- Extreme Jackal
- Aluminum Saratoga
- JEA/Jerusalem Electronic Army (Low to Medium Confidence)

Description:

Gaza Cybergang is a threat actor that has been active since at least 2012. The group primarily targets throughout the Middle East, including Israel and Palestine, while also less-observed in the EU and US. Targeted entities include government, defense, energy, financial, media, technology, telecommunication, and civil society. Current assessment of Gaza Cybergang indicates a medium to high level of confidence in Hamas affiliation.

The group has historically used a variety of custom and publicly available tools in their attacks, showing a notable preference for spear phishing as a method of initial access. They have been known to use malicious documents and email attachments to deliver malware and link lures, and they often deploy implants to maintain persistence on compromised systems. Tools include Molerat Loader, XtremeRAT, SharpStage, DropBook, Spark, Pierogi, PoisonIvy, and many others observed uniquely over the years.

The overall objectives of Gaza Cybergang appear to be primarily intelligence collection and espionage. They seek to gather intelligence, monitor political developments in the region, and support their cause through cyber activities. The group has been active for many years, and their persistence and adaptability in the face of evolving tensions make it a notable actor in the cyber threat landscape moving forward.

Hezbollah-Aligned Clusters

Plaid Rain

Aliases:

- Aqua Dev 1
- Polonium

Description:

Plaid Rain is a threat actor first documented in 2022 with a primary focus on targeting entities in Israel across a broad range of verticals, including defense, government, manufacturing, and financial organizations. Plaid Rain is considered to be based in Lebanon, however, its activities indicate potential coordination with Iran-nexus actors affiliated with Iran's Ministry of Intelligence and Security (MOIS). Some indicators supporting this assessment include observed overlaps in targeting and TTPs. The potential collaboration between MOIS and Plaid Rain positions this threat group in the nexus of actors that serve as proxies, providing plausible deniability to the government of Iran, such as Cobalt Sapling.

For initial infection, Plaid Rain is suspected to rely primarily on vulnerability exploitation, downstream compromises, and stolen credentials. The group's arsenal consists of a wide range of well-maintained custom tooling exemplified by the Creepy malware toolset. Plaid Rain's malware supports a broad range of complementing functionalities following the latest trends in the malware landscape. For example, the CreepyDrive malware uses Cloud services for command and control purposes, likely in an attempt to evade detection by making malicious traffic look legitimate.

Lebanese Cedar

Aliases:

- Volatile Cedar
- DeftTorero

Description:

Lebanese Cedar is a lesser-reported APT with a history of successful intrusions across Lebanon, Israel, Palestine, Egypt, United States, United Kingdom, and more. The group was first observed in 2015 and has since maintained limited security industry attention. Similar to Plaid Rain, we associate Lebanese Cedar with Lebanese Shiite militant group Hezbollah attribution as well as potential coordination with Iran-nexus actors affiliated with the Ministry of Intelligence and Security (MOIS).

Initial access methods best observed have been centered around the compromise of victim web servers via n-day vulnerabilities for the deployment of webshells, including ASPXSpy, devilzshell, and Caterpillar. Further use of Meterpreter and their custom Explosive RAT have been associated with objectives around maintaining access through theft of legitimate network credentials, ultimately pursuing espionage objectives.

Relevant Iranian Clusters

Iran hosts a diverse array of state-sponsored threat actors whose activities quickly expand past the specific focus on the Israel-Hamas war. These threat actors exhibit variability in terms of size, capability, and motivation, and they have been responsible for a wide spectrum of cyber operations. While some have clear affiliations with the Iranian government, many Iranian hacktivist personas claim to operate independently. It is crucial to acknowledge that emerging hacktivist collectives may serve as a means to obscure state sponsorship, influencing public opinion and concealing attribution of offensive actions. We strongly recommend that media outlets and industry colleagues exercise caution when publicly disseminating content produced by hacktivist collectives. The propagation of their claims, viewpoints, and actions aligns with an overarching mission, and endorsing these activities contributes to their success.Nonetheless, the diversity and adaptability of Iranian cyber threat actors make them a significant and multifaceted component of the global threat landscape moving forward. As we monitor the evolving situation in the Middle East, it is imperative to focus on Iran as a potential origin of both direct cyber offensive actions and proxy operations supported by Iran-linked groups like Hamas and Hezbollah.

ShroudedSnooper

Aliases:

- Storm-0861
- Scarred Manticore

Description:

ShroudedSnooper has been part of multiple recent intrusions across the Middle East, including Israel within the past two months, and elsewhere since at least 2020. Most recent observations and activity we can confirm, center around intrusions across the telecommunication and government sectors. The group is attributed to Iran's Ministry of Intelligence and Security (MOIS).

Our current understanding of the group is that they operate for intelligence collection and initial access to other MOIS entities. Initial access methods for ShroudedSnooper have, and potentially continue to be, accomplished through the compromise of publicly accessible web servers via n-day vulnerabilities. As observed in the recent Israeli telecom intrusions, the group has then made use of backdoors mimicking enterprise security software.

Cobalt Sapling

Aliases:

- Moses Staff
- Abraham's Ax
- Marigold Sandstorm

Description:

'Moses Staff' and 'Abraham's Ax' are hacktivist personas known for their anti-Israel rhetoric, disruptive and data exfiltration attacks, and penchant for leaking stolen data online along with propaganda content in the form of videos or imagery. Moses Staff and Abraham's Ax are potentially distinct groups. Since the emergence of Moses Staff in 2021 and Abraham's Ax in 2022 proclaiming allegiance with Hezbollah, the groups have continued to separately maintain their online presence. However, they share iconography, content editing and infrastructure management practices. This, and the alignment of their activities with the geopolitical interests of Iran, suggests that the two groups are likely part of a single cluster (also referred to as Cobalt Sapling) and serve as proxy groups providing plausible deniability to Iran.

Moses Staff has traditionally focused its efforts on business and government organizations primarily within Israel. In contrast, Abraham's Ax has asserted responsibility for attacks on entities located outside of Israel but with geopolitical relevance to the country. For example, the alleged intrusions into Saudi Arabian government entities by Abraham's Ax may have been an attempt to counter the normalization of relations between Israel and Saudi Arabia previously conditioned by resolving the Israeli-Palestinian issue.

Although the threat intelligence research community has identified custom offensive tooling observed in Moses Staff attacks, such as StrifeWater, PyDCrypt and DCSrv, we do not exclude the possibility of Moses Staff and Abraham's Ax sharing tooling and operational practices making accurate clustering challenging at this time. Operations attributed to Moses Staff have involved RATs and ransomware with no indications of financial motivations, but rather disruption, destruction, and concealment of cyber espionage activities.

APPENDIX: Recommended Public Reporting

Arid Viper

- 02/2015: Operation Arid Viper: Bypassing the Iron Dome – Trend Micro
- 02/2015: The Desert Falcons targeted attacks – GReAT
- 2017: Delphi Used To Score Against Palestine – Cisco TALOS
- 04/2021: Taking Action Against Arid Viper – Meta
- 02/2022: Arid Viper APT targets Palestine with new wave of politically themed phishing attacks, malware – Cisco TALOS
- 03/2022: What is Arid Gopher? – Deep Instinct
- 04/2022: Operation Bearded Barbie: APT-C-23 Campaign Targeting Israeli Officials – Cybereason
- 04/2023: Mantis: New Tooling Used in Attacks Against Palestinian Targets – Symantec
- 10/2023: Arid Viper Disguising Mobile Spyware as Updates for Non-Malicious Android Applications

Gaza Cybergang

- 11/2012: Systematic cyber attacks against Israeli and Palestinian targets going on for a year – Norman
- 08/2013: Operation Molerats: Middle East Cyber Attacks Using Poison Ivy – FireEye
- 06/2014: Molerats, Here for Spring! – FireEye
- 04/2015: Attacks against Israeli & Palestinian interests – PwC
- 09/2015: Gaza cybergang, where's your IR team? – GReAT
- 01/2016: Operation DustySky – Clearsky
- 06/2016: Operation DustySky Part 2 – Clearsky
- 10/2016: Moonlight – Targeted attacks in the Middle East – Vectra
- 11/2016: MoleRats: there's more to the naked eye – Pwc
- 01/2017: Downeks and Quasar RAT Used in Recent Targeted Attacks Against Governments – Unit42
- 10/2017: Gaza Cybergang – updated activity in 2017 – GReAT
- 01/2018: The TopHat Campaign: Attacks Within The Middle East Region Using Popular Third-Party Services – Unit42
- 04/2018: Operation Parliament, who is doing what? – GReAT
- 04/2019: The Gaza cybergang and its SneakyPastes campaign – GReAT
- 05/2019: Israel Defense Force bombing of alleged operations center
- 10/2019: Suspected Molerats' New Attack in the Middle East – 360
- 11/2019: Report on the attack on the Palestinian government by the APT organization "Pat the Bear" (Translated) – Rising
- 01/2020: Analysis of Threat Groups Molerats and APT-C-37 – AT&T
- 02/2020: New Cyber Espionage Campaigns Targeting Palestinians – Part 1: The Spark Campaign – Cybereason
- 03/2020: Molerats Delivers Spark Backdoor to Government and Telecommunications Organizations – Unit42
- 12/2020: New Malware Arsenal Abuses Cloud Platforms in Middle East Espionage Campaign – Cybereason
- 12/2020: Molerats APT: New Malware and Techniques in Middle East Espionage Campaign – Cybereason
- 04/2021: Threat Group Uses Voice Changing Software in Espionage Attempt – Cado
- 06/2021: New TA402 Mole Rats Malware Targets Governments in the Middle East – Proofpoint
- 01/2022: New espionage attack by Molerats APT targeting users in the Middle East – Zscaler
- 02/2022: Ugg Boots 4 Sale: A Tale of Palestinian-Aligned Espionage
- 10/2022: Analysis of a Management IP Address linked to Molerats APT – Team Cymru

Plaid Rain

- 06/2022: Exposing POLONIUM activity and infrastructure targeting Israeli organizations – Microsoft
- 10/2022: Polonium Targets Israel With Creepy Malware – ESET
- 12/2022: Polonium APT Group: Uncovering New Elements – Deep Instinct

Lebanese Cedar

- 03/2015: Volatile Cedar Technical Report – Checkpoint
- 03/2015: Sinkholing Volatile Cedar DGA Infrastructure – GReAT
- 06/2015: New Data: Volatile Cedar Malware Campaign – Checkpoint
- 01/2021: "Lebanese Cedar" APT – Global Lebanese Espionage Campaign Leveraging Web Servers – Clearsky
- 10/2022: DeftTorero: tactics, techniques and procedures of intrusions revealed – Kaspersky

ShroudedSnooper

- 09/2023: New ShroudedSnooper actor targets telecommunications firms in the Middle East with novel Implants – Talos
- 10/2023: From Albania to the Middle East: The Scarred Manticore Is Listening

Cobalt Sapling

- 02/2022: StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations – Cybereason
- 02/2022: Moses Staff Campaigns Against Israeli Organizations Span Several Months – Fortinet
- 01/2023: Abraham's Ax Likely Linked to Moses Staff – Secureworks
- 11/2021: Uncovering MosesStaff Techniques: Ideology Over Money – Checkpoint

ADVANCED PERSISTENT THREAT | CYBER ESPIONAGE | CYBER WARFARE | HACKTIVISM | ISRAEL-HAMAS

TOM HEGEL

Tom Hegel is a Senior Threat Researcher with SentinelOne. He comes from a background of detection and analysis of malicious actors, malware, and global events with an application to the cyber domain. His past research has focused on threats impacting individuals and organizations across the world, primarily targeted attackers.