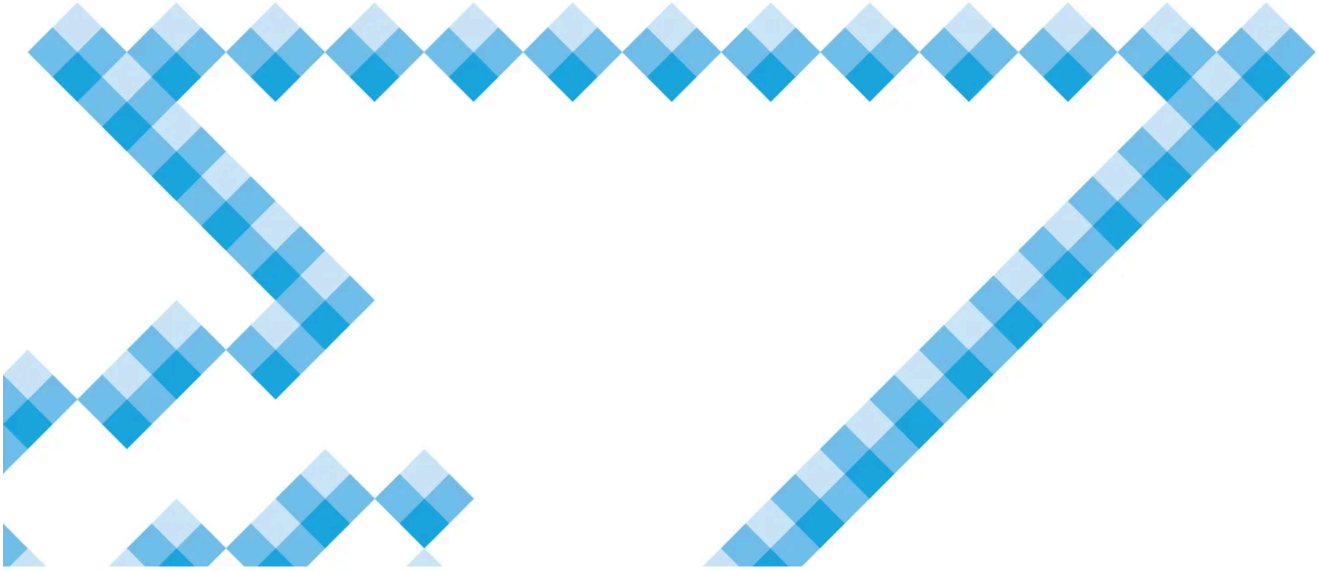
Tool of First Resort: Israel-Hamas War in Cyber

Feb 14, 2024 · 4 min read

Share

Sandra Joyce
VP, Mandiant Intelligence - Google Cloud

Shane Huntley
Senior Director, Threat Analysis Group



Listen to article 8 minutes

Cybersecurity plays a critical role in geopolitics — particularly during times of conflict. While offensive cyber operations have become nearly universal, the tactics, timing and objectives of threat actors can differ greatly. With Russia's invasion of Ukraine, for example, we observed and shared our report on how cyber tactics can be used to support military action.

In our latest report, Tool of First Resort: Israel-Hamas War in Cyber, we share our findings on a different tactical approach — and the escalation in offensive cyber operations in the wake of the October 7 terrorist attacks. Notably, after the terrorist attacks by Hamas, we observed the steady stream of cyber operations by Iran and Hezbollah-linked groups become more focused, more concentrated, and — among other objectives — geared toward undercutting public support for the war.

Today's report offers the latest example of how cyber operations are tools of first resort, providing a lower-cost, lower-risk way for rivals to engage in conflict, gather information, disrupt daily life, and shape public perceptions — all while still remaining below the line of direct confrontation.

Google has been tracking and protecting users from cyber threat activity before, during, and after the Hamas terrorist attacks on October 7. Today's report, based on analysis from Google's Threat Analysis Group (TAG), Mandiant, and Trust & Safety teams, encompasses new findings on Iranian-government backed phishing campaigns, hack-and-leak and information operations (IO), as well as disruptive attacks targeting Iran and Hamas-linked cyber operations.

Key findings on cyber operations related to the Israel-Hamas war

1. Iran continues to aggressively target Israeli and US entities, often with mixed results. This steady focus suggests that Hamas' attack did not fundamentally shift Tehran's strategy, but after the attack took place, we saw a more focused effort, concentrated on undercutting public support for the war. This includes:

- Destructive attacks against key Israeli organizations
- Hack-and-leak operations including exaggerated claims of attacks against critical infrastructure in Israel and the US
- IO to demoralize Israeli citizens, erode trust in critical organizations and turn global public opinion against Israel
- Phishing campaigns directed toward users based in Israel and the US to collect intelligence on key decision makers

2. Iranian critical infrastructure was disrupted by an actor claiming to be responding to the conflict. "Gonjeshke Darande" (Predatory Sparrow) claimed it had taken a majority of gas stations in Iran offline, attacking their infrastructure and payment systems. Iran has attributed Gonjeshke Darande activity to Israel, however we do not have sufficient evidence to evaluate these claims.

3. Hamas's cyber espionage followed its typical pattern in the leadup to October 7, and we have not observed significant activity since then. Our observations suggest Hamas did not use cyber operations to tactically support the terrorist attack on October 7th. Through September 2023, Hamas-linked groups engaged in cyber espionage consistent with their normal operations, including:

- Mass phishing campaigns to deliver malware and steal data
- Mobile spyware, including Android backdoors, distributed via phishing
- Persistent targeting of Israel, Palestine, and their regional neighbors in the Middle East, as well as regular targeting of the US and Europe

What's different from the Russian war in Ukraine

Since our 2023 report of the Russian war in Ukraine, we've seen several of our assessments play out. This included Russian government-backed attackers continuing their cyber attacks against Ukraine and NATO partners, and Russian-government backed attackers continuing to target multiple sectors in Ukraine and regionally, including high profile individuals in NGOs, former intelligence and military officials and NATO governments. During the lead up to Ukraine's counteroffensive in June 2023, we also saw an increase in the frequency and scope of APT29 phishing operations, including an intensification of operations centered on foreign embassies in Ukraine and later, a spike in destructive attacks against Kyivstar and Parkovy. Moscow also continues to pair cyber attacks with kinetic activity.

Cyber activity surrounding the Israel-Hamas war, however, is very different from the war in Ukraine. Unlike the attack on Ukraine, we did not observe a spike in cyber operations against Israeli targets before the attack, and have no indication that cyber activity was integrated into Hamas battlefield operations, or used to enable kinetic events.

What we can expect to see in 2024

Our observations in the report point to several broader forward looking assessments for the security community in 2024:

- Iran-linked groups are likely to continue to conduct destructive cyber attacks, particularly in the event of any perceived escalation to the conflict, to include kinetic activity against Iranian proxy groups in various countries, such as Lebanon and Yemen.

- Hack-and-leak operations and IO will remain a key component in these efforts to telegraph intent and capability throughout the war, both to Iran's adversaries and to other audiences that they seek to influence.

- While the outlook for future cyber operations by Hamas-linked actors is uncertain in the near term, we anticipate Hamas cyber activity will eventually resume, with a focus on espionage for intelligence gathering on intra-Palestine affairs, Israel, the US, Europe, and other regional players in the Middle East.

It is clear that cyber will play a prominent role in major armed conflicts going forward. We hope the analysis and research contained in this report helps to inform defenders globally, providing fresh insights for collective defense. At Google, we are committed to supporting the safety and security of online users everywhere and will continue to take action to disrupt malicious activity to protect our users and help make the Internet safe for all.

More details are available in the full report. To help network defenders protect against the activity described in the report, we've also published indicators of compromise (IOCs) on Github.

POSTED IN:

Safety & Security

Threat Analysis Group