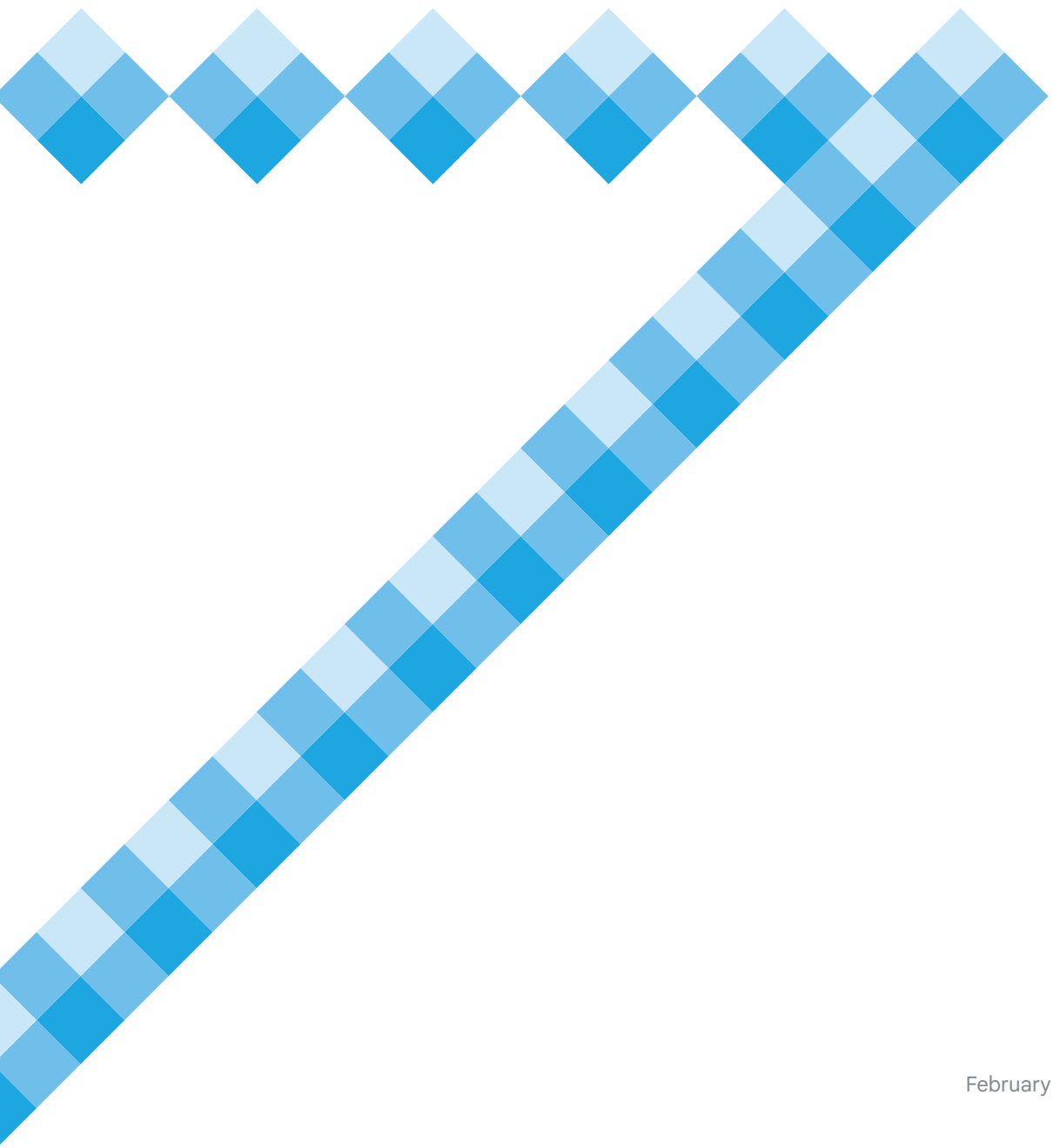
Google

Tool of First Resort

Israel-Hamas War in Cyber



February 2024

About the authors

Google's **Threat Analysis Group** (TAG) is responsible for countering threats to Google and our users from government-backed attackers, targeted 0-day exploits, coordinated information operations (IO), and serious cybercrime networks. We apply our intelligence to improve Google's defenses and protect users.

Mandiant, part of Google Cloud, is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to defend against and respond to cyber threats.

Google Trust & Safety safeguards Google products against abuse and provides trusted and safe experiences for all users.

Table of contents

Executive Summary

This report presents an analysis of cyber activity before and after the October 7, 2023 start of the Israel-Hamas war and dives into specific examples that support the following key observations, drawn from research by Google's Threat Analysis Group (TAG) and Mandiant Intelligence.

1 | Iran extensively employed cyber operations to gather information and cause disruption in the years before the attack and continues to do so after the attack. Disruptive operations focused on Israel, where Iran has long conducted cyber attacks against key Israeli organizations, but also affected American critical infrastructure. Iran's espionage operations likewise focused on Israel and the United States, but also impacted other countries in the region.

2 | Hamas-linked groups were active with typical operations through September 2023, with no observable increase in activity leading up to October 7, and we have not observed significant activity since then. Activity prior to the conflict included mass phishing campaigns targeting Palestine and its regional neighbors and persistent efforts to target Israeli entities with a variety of custom and open-source cyber capabilities, including Android malware. These campaigns were in line with historic cyber activity by Hamas-linked actors.

3 | Iranian critical infrastructure was targeted with disruptive attacks later claimed by the persona "Gonjeshke Darande" (Predatory Sparrow). The attack on gas stations followed public warnings from the persona, which Iran has attributed to Israel. Gonjeshke Darande has been tied to prior attacks in Iran.

> It is clear that cyber will play a role in every major conflict going forward. We hope the analysis and research contained in this report serves as a call to action for all defenders, and provides fresh insights to help every organization better defend against potential attacks.
>
> At Google, we are committed to doing our part to support collective defense. We will continue to take action to disrupt malicious activity to protect Google and our users, and do our part to support security for all online users. We look forward to partnering with others to drive continued progress, and help organizations, businesses, governments, and users stay safe online.

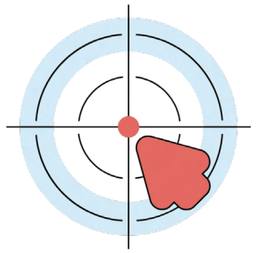
KEY OBSERVATIONS

While we have observed no evidence that Hamas' initial attack included a planned cyber component, regional actors immediately engaged in cyber operations following the assault. These operations served two main goals: first, gathering operational and strategic intelligence; and second, demonstrating involvement in the war to multiple target audiences, leveraging the cyber domain as a vector for aggression short of kinetic activity. As the conflict continues and the possibility for broader regional instability increases, we want to share deeper analysis on our key observations to help defenders manage potential risks.

First, Iran aggressively targeted Israel and the United States in earlier years and this continues after the attack, including destructive cyber attacks against key Israeli organizations and intelligence collection activities directed at Israeli and US decision makers. In the six months leading up to the October 7 attacks, Iran accounted for approximately 80% of all government-backed phishing activity we observed targeting users based in Israel. After October 7, we've seen a focused effort to undercut support for the war among both the Israeli public and the broader global populace, including hack-and-leak and information operations to demoralize Israeli citizens, erode their trust in national organizations, and cast Israel's actions in a negative light. These operations are consistent with longstanding Iranian efforts to target Western organizations across sectors, including recent attempts to compromise US critical infrastructure.

Second, Hamas-linked groups were active with typical operations through September 2023, with no observable increase in activity leading up to October 7, and we have not observed significant activity since then. Activity prior to the conflict included mass phishing campaigns targeting Palestine and its regional neighbors, mobile malware, and persistent efforts to target Israeli entities with a variety of custom and open-source cyber capabilities. These campaigns were in line with historic cyber activity by Hamas-linked actors. The tactics, techniques and procedures (TTPS) favored by these actors tend to be simple-but-effective; however, at least one recent campaign by a Hamas-linked group shows advances in their cyber capabilities, including elaborate social engineering campaigns to deliver custom malware to high-value Israeli targets.

Third, Iranian critical infrastructure was disrupted by an actor who claimed to be responding to the October 7 attacks. The actor "Gonjeshke Darande" (Predatory Sparrow), which Iran has attributed to Israel, took credit for disruptions to gas stations in the country.



Cyber capabilities can be quickly deployed at minimal cost to regional rivals who may wish to avoid armed conflict — they are a tool of first resort.

ASSESSMENTS

These observations point to several broader, forward-looking assessments for the security community for 2024:

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

We further judge that hack-and-leak and information operations remain a key component in these and related threat actors' efforts to telegraph intent and capability throughout the war, both to their adversaries and to other audiences that they seek to influence.

We assess that Hamas intentionally did not use cyber operations to tactically support the October 7 attack. There was no shift in operations in the lead-up to the attack, and the majority of identified operations in the months prior involved intra-Palestinian and regional Middle East targeting consistent with their normal activity. This is potentially because the operational security risks from a cyber operation outweighed the assessed potential benefit.

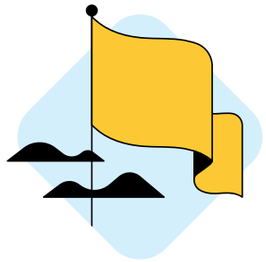
While the outlook for future cyber operations by Hamas-linked actors is uncertain in the near term, we anticipate Hamas cyber activity will eventually resume, with a focus on espionage for intelligence gathering on intra-Palestine affairs, Israel, the US, and other regional players in the Middle East.

The Israel-Hamas conflict is very different from other conflicts, such as the Russian invasion of Ukraine. In the Israel-Gaza region, we did not observe a spike in cyber operations against Israeli targets before the attack, in stark contrast to Ukraine, where we saw a large increase in Russian cyber threat activity targeting Kyiv in the lead up to the invasion. In addition, we saw no indication that cyber activity was integrated into Hamas battlefield operations, or that cyber was used to enable kinetic events. In comparison, we saw Russian cyber threat actors launch coordinated cyber attacks against Ukrainian targets before missile strikes.

Section 1

Iran continues to aggressively target US and Israel entities, often with mixed results

Iran aggressively targeted Israel and the United States in the years leading up to Hamas' attack on October 7 and has continued to target them throughout the subsequent conflict. These consistent strategic priorities suggest that the war did not fundamentally shift Tehran's broader goals. However, after the attacks took place, we have seen a focused effort to undercut public support for the war. This includes destructive cyber attacks against key Israeli organizations; hack-and-leak operations and targeted information operations to demoralize Israeli citizens, erode trust in critical organizations, and turn global public opinion against Israel; and phishing activity directed at US and Israeli leaders to collect intelligence on key decision makers.



In the six months leading up to the October 7 attacks, Iran accounted for approximately 80% of all government-backed phishing activity we observed targeting users based in Israel.

Iran and its Proxies
Threat Actor Overview

APT42

Aliases
CALANQUE
CHARMING KITTEN
MINT SANDSTORM
TA453

DUSTYCAVE

Aliases
UNC4444
IMPERIAL KITTEN
CRIMSON SANDSTORM
TA456

DUNE

Aliases
BANISHED KITTEN
STORM-0842

MYSTICDOME

Aliases
UNC1530
CHRONO KITTEN
STORM-0133

MARNANBRIDGE

Aliases
EMENNET PASARGAD
COTTON SANDSTORM

GREATRIFT

Aliases
UNC4453
PLAID RAIN

	APT42	DUSTYCAVE	DUNE	MYSTICDOME	MARNANBRIDGE	GREATRIFT
Espionage	●	●	●	●	—	●
Information Operations	—	—	●	—	●	—
Destruction	—	—	●	—	—	—
Targeted Nations	Israel United States Middle East Europe	Israel United States Middle East Europe	Israel United States Middle East Europe	Israel — Middle East —	Israel United States Middle East Europe	Israel — — —
Primary Targets	Government Military and Defense Energy Financial Healthcare and Pharmaceuticals Heavy Industry — Education News Media NGOs and Civil Society — Legal and Professional Services —	Government Military and Defense Energy Financial Healthcare and Pharmaceuticals Heavy Industry High Tech and Telecom — News Media NGOs and Civil Society Shipping and Rail Legal and Professional Services Transportation	Government — — — Healthcare and Pharmaceuticals — High Tech and Telecom Education News Media NGOs and Civil Society — — —	Government Military and Defense Energy — — — High Tech and Telecom Education — — — — —	Government — Energy Financial — — High Tech and Telecom — — NGOs and Civil Society Shipping and Rail — —	— Military and Defense — — Healthcare and Pharmaceuticals — — — — NGOs and Civil Society — — —

CYBER OPERATIONS AGAINST ISRAEL BY IRAN AND ITS PROXIES SINCE OCTOBER 7

OCTOBER 2023

- GREATRIFT distributed malware via fake "missing persons" site targeting visitors seeking updates on abducted Israelis
- "Cyber Flood" hack-and-leak operation targeting Israeli municipalities
- "BiBi wiper" destructive attack targeting Israeli IT and data hosting companies, defense contractors, and government organization
- GREATRIFT campaign spoofed an Israeli hospital and used blood donation-themed lure documents to distribute malware

NOVEMBER 2023

- "Cyber Aveng3rs" hack-and-leak operation against US water utility that allegedly used Israeli-made hardware/software
- APT42 phishing activity targeting high-profile Israel- and US-based users
- "Malek Team" hack-and-leak operation against Ziv hospital

DECEMBER 2023

- "Handala Hack" persona claims credit for destructive attack targeting Israeli government and financial sectors

Disruptive attacks targeting Israel

In 2012, a suspected Iranian group used the SHAMOON wiper malware to disrupt organizations in the Middle East. Since then, Iran-nexus actors have continued to demonstrate a capability and willingness to conduct destructive and disruptive attacks against targets spanning a range of regions and sectors, including those in Israel. In the weeks following the October 2023 Hamas attack, we saw an increase of destructive cyber attacks, including wiper malware deployed in campaigns targeting the Israeli government, financial institutions, tech companies, and defense contractors. These attacks are not a major shift in Iran's modus operandi — destructive activity, amplified by fabricated personas, has long been a feature of Iranian operations targeting Israel. Following the October 7 Hamas attacks, Iranian actors also leveraged newly created personas to incorporate rhetoric intended to undermine public confidence in Israeli leadership and promote pro-Palestine messaging.

While these attacks have caused temporary disruptions to the affected entities, and difficulties for everyday Israelis, we assess that they have not had a sustained impact across wider sectors and have not meaningfully interfered in Israel's military operations.

We anticipate Iran will continue to leverage destructive capabilities against Israel and its allies to achieve Tehran's strategic objectives, and that they may expand their use of destructive attacks in response to perceived escalation against Iran and its proxies in the context of the current conflict. Iran has escalated its use of destructive cyber attacks in response to perceived threats in the past. In 2022, for example, the Iran-backed group DUNE targeted Albania — a NATO member state — ahead of a planned Iranian opposition organization's conference in the country; an incident reflecting Iran's risk tolerance when engaging in such attacks against its adversaries.

Attackers reportedly sent instructions to printers at target organizations to mass-produce a flyer (left) advertising the Karma Telegram channel (right) and an anti-Netanyahu slogan

Iran-backed attackers deploy BiBi wiper in late October

In late October 2023, attackers likely connected to the Iranian government-backed group DUNE, targeted Israeli organizations in a destructive attack leveraging wiper malware for both Linux and Windows. The malware, dubbed "BiBi wiper," referenced Israeli Prime Minister Benjamin Netanyahu and overwrote files with random data including randomly generated filenames containing the string "BiBi." Public reporting noted that attackers also changed machine names at affected organizations to "NO2BIBI" and sent instructions to printers to mass-print an anti-Netanyahu slogan.

The attack's targets included Israeli IT and data hosting companies, defense contractors, and government organizations. Threat actors used a hacktivist persona on Telegram, "Karma", to publicize the attacks and post the same anti-Netanyahu slogan that attackers printed out at victim organizations.

The persona "Handala Hack" claimed to be behind COOLWIPE and CHILLWIPE activity targeting Israeli government and financial entities

December 2023 wiper activity targets Israeli government, financials

In mid-December 2023, cyber threat actors leveraged wiper malware for Linux and Windows to target government and financial institutions in Israel. Phishing emails impersonated a US-based multi-cloud applications and security company to entice targets to download and run the malware, dubbed COOLWIPE and CHILLWIPE, in the guise of a security update; the malware overwrites and then deletes files in the system.

A persona named "Handala Hack," a reference to a symbol of Palestinian resistance, then publicized the wiper activity associated with COOLWIPE and CHILLWIPE along with rhetoric citing Palestine. The Israel National Cyber Directorate (INCD) attributed the activity to an Iranian attack group, but did not provide further information on the attackers' identity.

IRAN'S LONG HISTORY OF DESTRUCTIVE ATTACKS

2012 — SHAMOON attack targeting Saudi oil entities

2014 — Wiper attack targeting Las Vegas Sands

2016 — SHAMOON 2 attacks against industrial organizations in Saudi Arabia, UAE, and potentially other European countries (2016–2018)

2019 — ZEROCLEAR, DUSTMAN wipers targeting Middle Eastern entities

2020 — THANOS, APOSTEL ransomware disruptive activity targeting Middle Eastern, North African entities (2020–2021)

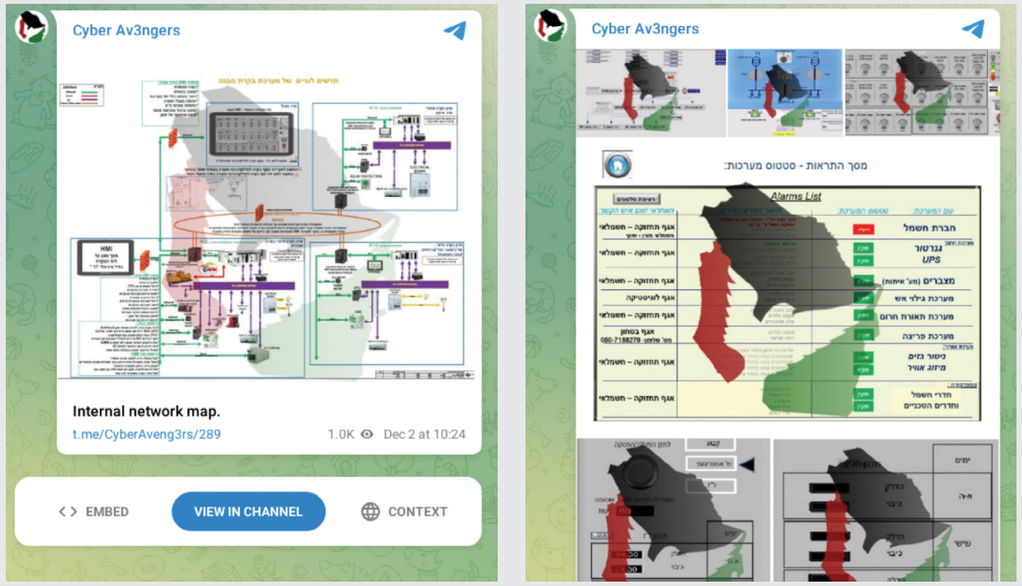
2022 — ROADSWEEP/ZEROCLEAR disruptive attack against Albanian entities (August)

2023 — DARKBIT ransomware attack against Israeli university (February)

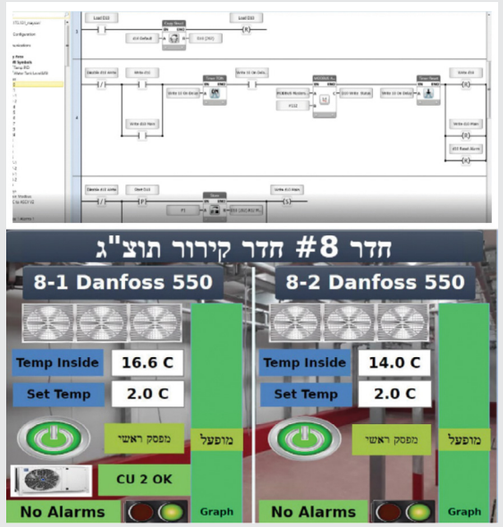
BiBi wiper attack against Israeli entities (October)

COOLWIPE/CHILLWIPE wiper attack against Israeli entities (December)

LOWERASER disruptive activity targeting Albanian entities (December)



Posts on Telegram by "Cyber Aveng3rs" showing leaked data from alleged hacks. Pro-Iran hack-and-leak claims have been largely exaggerated and misleading.



Screenshots from "Abnaa Al-Saada" Telegram posts claiming to compromise OT (Operational Technology) systems belonging to an Israeli company

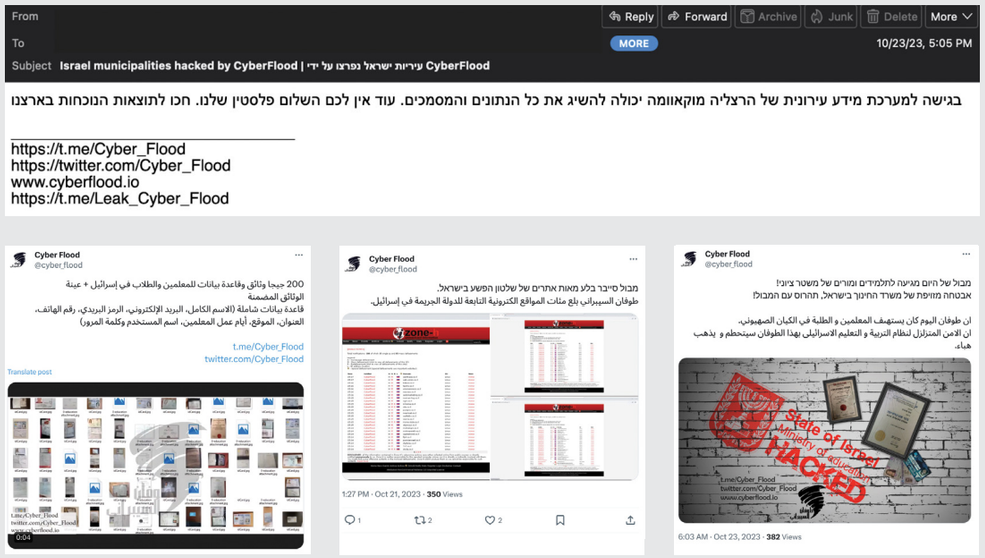
Conducting hack-and-leak and targeted information operations

Over the past several years, Iran has committed significant resources to digital influence efforts, including hack-and-leak and information operations. Hack-and-leak operations involve a two-step process to compromise potential victims and subsequently release extracted data with intent to influence. Iranian actors have typically followed a common template: conduct intrusion activity against a target; announce the hack using a fictitious persona; and use sock puppet accounts on social media to amplify the leak or defacement. Recent operations have used personas including Cyber Aveng3rs, Soldiers of Solomon, Abnaa Al-Saada, Karma, Malek Team, Cyber Flood, and CyberToufan.

Recent pro-Iran hack-and-leak groups have made claims — largely exaggerated and misleading — of hacks against Israeli critical infrastructure, including energy infrastructure. These groups publicized their claims on social media and via email, citing evidence demonstrating their alleged access to security cameras and other webcams in Israel. The claims of attack are likely intended as much to shape the information environment and create the perception of weakness in Israeli defenses, as for any tangible physical effect.

“Cyber Flood” targets Israeli municipalities following October 7 attack

We have also observed hack-and-leak operations targeting Israel by MARNANBRIDGE, an information operations group likely connected to the Iranian company Emennet Pasargad. Emennet Pasargad previously carried out attacks that blended cyber and information operations and was sanctioned by the US government for attempts to influence the 2020 US presidential election.



In mid-October 2023, MARNANBRIDGE compromised and abused Israeli local government email accounts to send emails publicizing a hack-and-leak operation targeting Israeli municipalities. The operation, designed primarily to inspire fear among Israelis by demonstrating access to their municipal systems, also included messaging disseminated via compromised accounts to further sow uncertainty. The emails were intended for thousands of users in Israel and contained claims that a hacker persona, “Cyber Flood,” had obtained data including personally identifiable information (PII) from Israeli municipalities, alongside a pro-Palestine slogan and links to the persona’s X and Telegram channels, where it posted updates and “proof” of its activity. Fortunately, Google users were protected by Gmail, which automatically detected the emails and marked them as spam. Cyber Flood's Telegram and X accounts also posted claims that the persona defaced hundreds of Israeli websites and compromised the Israeli Ministry of Education.

IRGC-linked “Cyber Aveng3rs” targets Israeli-made hardware / software in US water utility

On November 26, 2023, the Municipal Water Authority of Aliquippa in Pennsylvania announced that attackers had compromised a machine in a booster station that regulated water pressure. The machine used a system that included software or had components from an Israeli-owned company. A Water Authority representative claimed there was never any threat to the availability of water, and that once they realized the hack occurred, the utility switched to manual operations. “Cyber Aveng3rs” — a hacker persona likely backed by Iran’s Islamic Revolutionary Guard Corps (IRGC) — claimed credit for the attack, and took over a control panel’s digital display screen to make it read: “Every equipment ‘Made in Israel’ is Cyber Av3ngers legal target.”

The Cyber Aveng3rs persona was created in 2020, but it was mostly inactive from July 2020 to July 2023. It has previously targeted critical infrastructure, oil and gas, transportation, and technology companies through distributed denial-of-service (DDoS) attacks, hack-and-leak operations, data destruction and other disruptive activities. Despite multiple broad claims of activity against significant targets, we have not observed significant impact associated with these claims, and we judge that the persona has likely overstated or fabricated its attacks. As with other pro-Iran hacktivist personas, these activities are likely intended primarily to create the perception that Israel is endangered or besieged, rather than cause significant physical impact.

Cyber Aveng3rs claimed credit for the attack and took over a control panel’s digital display to amplify their message

Targeted phishing for intelligence collection against key targets

In the six months prior to the October 7 attacks, Iran accounted for approximately 80% of all government-backed phishing activity we observed targeting users based in Israel. APT42 (a.k.a., CALANQUE) and DUSTYCAVE (a.k.a., UNC4444) accounted for the bulk of this activity, with targets including national and municipal governments, diplomatic organizations, academia, think tanks, NGOs, media, tech companies, aerospace and defense, and the shipping sector. Following October 7, phishing activity levels remained consistent with what we typically see from Iran-backed actors. Targets included national security think tanks, diplomats, former military, and a crisis-focused NGO — all standard targets for Iranian APT actors, though they were likely especially valuable intelligence targets at the time in light of the ongoing conflict.

Likely IRGC-linked activity targets high-profile US and Israeli decision makers and media, NGOs

In late October and November 2023, we observed continued phishing activity from APT42, an Iranian-sponsored cyber espionage group that we believe to operate on behalf of the IRGC. The timing and targets of the campaigns suggested a specific interest in Israeli and US decision making related to the conflict. In October, APT42 registered new domains likely for use in credential harvesting and phishing campaigns. In a separate operation, UNC2448 distributed POWERPUG, a PowerShell backdoor, via a spear-phishing campaign. Targeted industries included media, non-governmental organizations (NGOs), and policy work associated with US higher education. Domains and the executable file used in the UNC2448 operation appeared to masquerade as a Saudi Arabia-based NGO that focuses on Iranian studies.

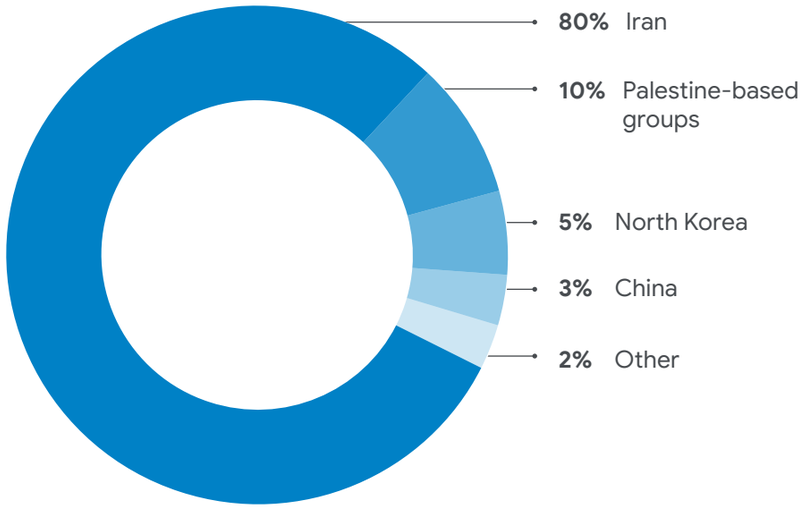
Subsequently in November 2023, APT42 conducted phishing activity against several high-profile users based in Israel and the US, including current and former government officials, diplomats, and individuals who work on US-Israel relations. This activity is in line with the group's normal operations, but is nonetheless notable for its focus on individuals who are likely to possess insights into the inner thinking and decision making of the US and Israeli governments.

GOVERNMENT-BACKED
PHISHING TARGETING ISRAEL

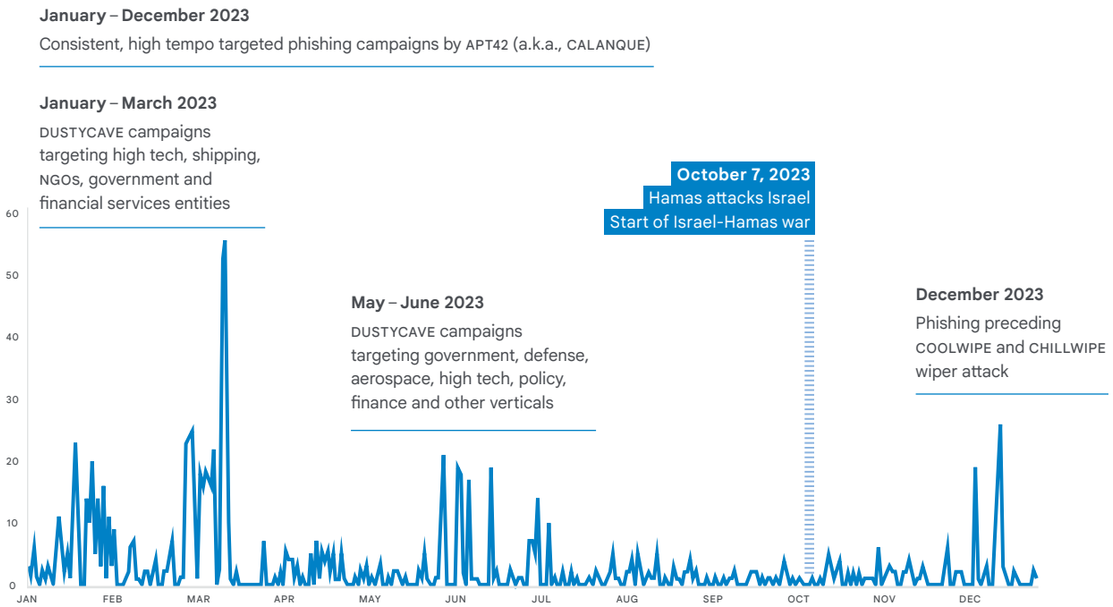
APRIL 1 – OCTOBER 7, 2023

Iran typically accounts for the majority of government-backed phishing activity TAG observes in Israel.

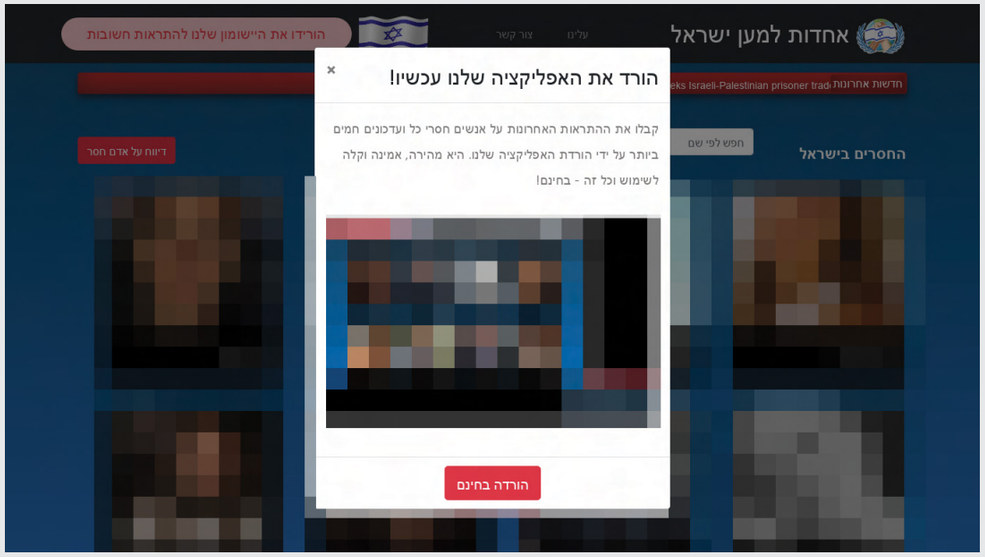
Source: Google's Threat Analysis Group (TAG)



TARGETING ISRAEL: PHISHING ACTIVITY
BY IRANIAN GOVERNMENT-BACKED ACTORS



Source: Google's Threat Analysis Group (TAG)



Fake missing persons site prompted visitors to install an applet for updates on abducted Israelis (image intentionally blurred for privacy)

Likely Hezbollah-linked group used conflict-themed phishing lures to distribute malware

Iran's proxy, Hezbollah, also conducted cyber operations targeting Israel immediately following the October 7 attacks. GREATRIFT, a Lebanon-based group likely linked to Hezbollah, took advantage of the surge in interest in emergency services immediately following the initial attack to impersonate legitimate Israeli services in phishing lures, demonstrating its agility to rapidly tailor activity to current events. Masquerading as critical or emergency services in order to deliver malware could additionally serve the purpose of undermining trust in public institutions.

In one instance, GREATRIFT created a fake missing persons website that prompted visitors to download a likely malicious applet purportedly providing notifications on the whereabouts of abducted Israelis. Separately, the group created and used a website impersonating Israel's Sheba Medical Center to distribute malware with a blood donation theme. In both cases, we took steps to disrupt these activities and added the sites to Safe Browsing's blocklist. As the war continues with a possible expansion into kinetic conflict on Lebanese territory, Hezbollah-related actors may both conduct opportunistic attacks and respond to kinetic attacks in the cyber realm.

Section 2

Cyber attacks on Iran conducted by "Gonjeshke Darande"

On October 10, 2023, the persona "Gonjeshke Darande" (Predatory Sparrow) posted a Persian-language message on Telegram claiming to have returned, stating: "Do you think this is scary? We returned. We hope you're following what is happening in Gaza." Previously, Gonjeshke Darande claimed responsibility for multiple attacks in Iran between October 2021 until January 2023 via Telegram and X (formerly Twitter).

In December 2023, Gonjeshke Darande claimed another major attack, saying that they had taken a majority of gas stations in Iran offline. Iran's Oil Minister, who blamed Israel and the US for the attacks, confirmed the impact. In the posts claiming these attacks, Gonjeshke Darande said, "This cyberattack comes in response to the aggression of the Islamic Republic and its proxies in the region." The hacking group has claimed restraint, emphasizing that their operations were designed to disrupt and demonstrate capability, rather than cause lasting damage.

Iran has stated that it believes Israel is behind the Gonjeshke Darande attacks. We do not have sufficient evidence to evaluate claims of attribution for Gonjeshke Darande activity.

Iranian critical infrastructure was disrupted by an actor who referenced the Israel-Hamas conflict in its messaging. The actor “Gonjeshke Darande” (Predatory Sparrow) took credit for disruptions to gas stations and their payment systems throughout the country. Iran attributes this activity to Israel.

Gonjeshke Darande claimed to compromise gas stations and their payment systems throughout Iran, including images demonstrating that they were inside the network and its central communication systems.

Section 3

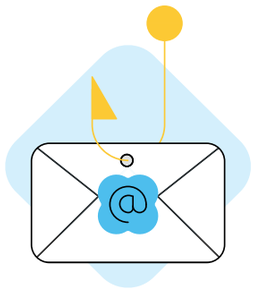
Typical Hamas-linked cyber espionage prior to October 7

Hamas-linked groups have shown high levels of interest in Israel in the past and have actively engaged in cyber operations to collect intelligence from targets within the Palestinian Territories and Israel. This includes mass phishing campaigns targeting users in Palestine and its regional neighbors, and persistent efforts to target Israeli entities with a variety of custom and open-source cyber capabilities, including Android malware. Their standard activity includes a steady cadence of intra-Palestine targeting, as well as regular targeting of Israel, the United States, Europe, and countries neighboring Israel and Palestine. Through September 2023, Hamas-linked groups were active with typical operations, with no observable increase in activity leading up to October 7, and we have not observed significant activity since then. We did not observe a shift in operations in the lead up to the October 7 attack, and assess that Hamas did not use cyber operations to tactically support the attack.

Hamas-linked cyber actors have historically relied on simple-but-effective TTPS to conduct their campaigns. They use phishing and malware lures with topical political themes, basic custom backdoors and widely available remote access tools such as njRAT and Xtreme RAT, and malware obfuscation tools purchased on underground forums. Mobile spyware is also common, including custom and open source Android backdoors distributed via phishing. More recently, however, we have observed at least one Hamas-linked actor, BLACKATOM, show signs of more advanced capabilities, including elaborate social engineering tailored to software engineers and custom malware developed for Windows, Mac, and Linux. While the future of Hamas cyber operations remains uncertain, the recent indications of evolving capabilities are notable and worth monitoring going forward.

Hamas-linked Groups
Threat Actor Overview

	BLACKSTEM	DESERTVARNISH	BLACKATOM
	Aliases MOLERATS EXTREME JACKAL	**Aliases** UNC718 RENEGADE JACKAL DESERT FALCONS ARID VIPER	
Espionage	●	●	●
Information Operations	—	—	—
Destruction	—	—	—
Targeted Nations	Israel United States Palestine Middle East Europe	Israel United States Palestine Middle East Europe	Israel — — — —
Primary Targets	Government Military and Defense Energy Financial Healthcare and Pharmaceuticals Heavy Industry — Education News Media NGOs and Civil Society — Legal and Professional Services —	Government Military and Defense Energy Financial — Heavy Industry High Tech and Telecom Education News Media NGOs and Civil Society — Legal and Professional Services Transportation	— Military and Defense — — — — — — — — — — — Transportation



Prior to October 7, Hamas-linked groups were active with mass phishing campaigns targeting Palestine and its regional neighbors, mobile malware, and persistent efforts to target Israel.

Conducting phishing and malware campaigns

In the weeks leading up to the October 7 attack, we observed actors associated with Hamas conduct multiple campaigns, including mass phishing to deliver malware and efforts to steal email data. In September 2023, for example, Hamas-linked group BLACKSTEM (a.k.a., Molerats) sent multiple waves of phishing emails to over 1,000 users located in Palestine, Egypt, Tunisia, and Jordan. A small number of users in Israel were also targeted. The emails contained links to an imitation news site impersonating Al Jazeera that ultimately delivered a backdoor to targets. The payload was MAGNIFI, a simple backdoor written in C++. The backdoor supports downloading and executing additional files that will be saved and periodically executed from a specific directory.

In a separate September 2023 campaign, BLACKSTEM sent phishing emails with a URL that redirected to a request via Microsoft for authentication tokens. Users logged into Microsoft would receive a prompt to permit access to an attacker-controlled Azure / Microsoft app. The requested token included read / write permissions for mail, and, if granted, the token would be sent back to an attacker-controlled URL.

HAMAS-LINKED CYBER OPERATIONS

SEPTEMBER 2023

- BLACKSTEM mass phishing campaigns targeting Palestine, Egypt, Tunisia, and Jordan
- BLACKSTEM OAuth phishing campaign targeting Microsoft users
- BLACKSTEM exploited XSS bug on Palestinian police website to deliver malware
- BLACKSTEM developed Android spyware mimicking an official Palestinian government app
- BLACKATOM targeted Israeli software developers with coding assignment lure

OCTOBER 2023

- Last confirmed cyber activity by Hamas-linked actors on October 4

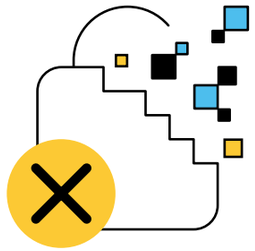
Legitimate Palestine Police website exploited via reflected XSS

Intra-Palestine targeting

In the weeks leading up to October 7, Hamas-linked actors launched multiple campaigns targeting users and organizations based in Palestine, including organizations in the Fatah-led government. Intra-Palestine targeting has long been a focus of Hamas-linked cyber campaigns, and we have consistently seen such activity, likely at least in part due to longstanding political rivalries and factionalism. However, the recent campaigns illustrate Hamas' dedicated focus on collecting intelligence about internal Palestinian affairs, even weeks prior to launching a major attack on Israel.

Starting in early September 2023, BLACKSTEM exploited a reflected cross-site scripting (XSS) vulnerability on the website of the Palestinian Civil Police Force (palpolice[.]ps). The link created a browser popup that redirected the visitor to a "news.rar" archive containing an exploit for a known bug (CVE-2023-38831) in the popular Windows file archiver tool WinRAR. The final payload was the MAGNIFI backdoor.

In September 2023, we also identified initial efforts by BLACKSTEM to create Android spyware that mimicked a legitimate application used by employees of Palestine's Ministry of Interior (MOI). The legitimate app allows MOI employees to access internal data on their mobile devices. We suspect the spyware app was still in early stages of development when discovered. The app has not been published to the Google Play store, and we have not seen any evidence of it being distributed widely.

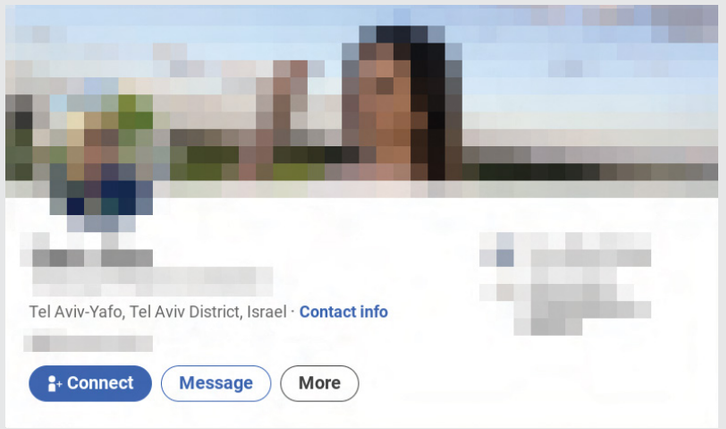


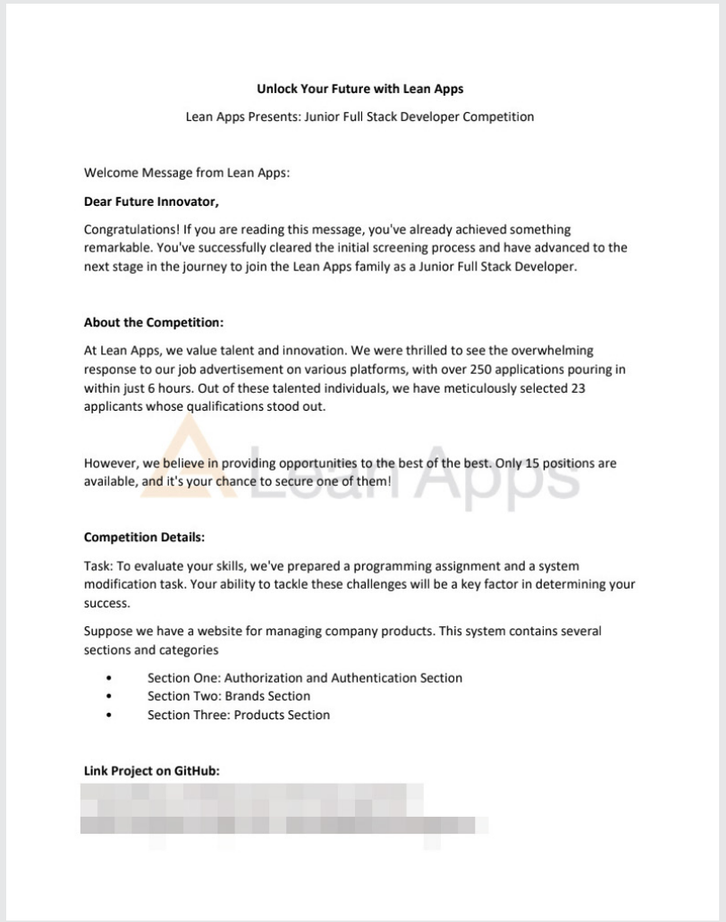
In the weeks leading up to October 7, Hamas-linked actors launched multiple campaigns targeting users and organizations based in Palestine, including organizations in the Fatah-led government.

BLACKATOM targeting Israeli software engineers with SYSJOKER multi-platform malware

Recent campaigns suggest Hamas-linked actors may be advancing their TTPs to include intricate social engineering lures specially crafted to appeal to a niche group of high value targets. In September 2023, a Palestine-based group likely linked to Hamas targeted Israeli software engineers using an elaborate social engineering ruse that ultimately installed malware and stole cookies. The attackers, which Google's Threat Analysis Group (TAG) tracks as BLACKATOM, posed as employees of legitimate companies and reached out via LinkedIn to invite targets to apply for software development freelance opportunities. Targets included software engineers in the Israeli military, as well as Israel's aerospace and defense industry.

After establishing initial communication, BLACKATOM sent targets a lure document with instructions for participating in a coding assessment. The instructions directed targets to download a Visual Studio project from an attacker-controlled Github or Drive page, add features to the project to prove their coding skills, and then send it back for evaluation. The project appeared to be a benign HR management app, but included a function to download a malicious ZIP, extract the ZIP, and execute malware inside on the target's system. Pivoting on indicators from the initial activity, we also identified trojanized React apps BLACKATOM used in a variation of the campaign.





Unlock Your Future with Lean Apps

Lean Apps Presents: Junior Full Stack Developer Competition

Welcome Message from Lean Apps:

Dear Future Innovator,

Congratulations! If you are reading this message, you've already achieved something remarkable. You've successfully cleared the initial screening process and have advanced to the next stage in the journey to join the Lean Apps family as a Junior Full Stack Developer.

About the Competition:

At Lean Apps, we value talent and innovation. We were thrilled to see the overwhelming response to our job advertisement on various platforms, with over 250 applications pouring in within just 6 hours. Out of these talented individuals, we have meticulously selected 23 applicants whose qualifications stood out.

However, we believe in providing opportunities to the best of the best. Only 15 positions are available, and it's your chance to secure one of them!

Competition Details:

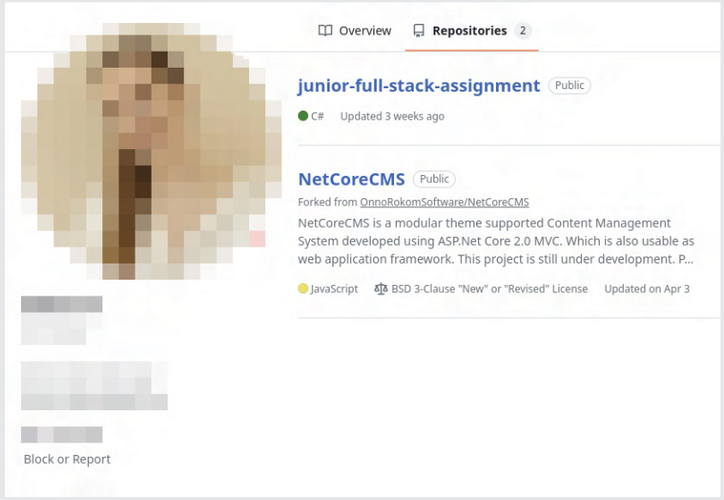
Task: To evaluate your skills, we've prepared a programming assignment and a system modification task. Your ability to tackle these challenges will be a key factor in determining your success.

Suppose we have a website for managing company products. This system contains several sections and categories

- Section One: Authorization and Authentication Section
- Section Two: Brands Section
- Section Three: Products Section

Link Project on GitHub:

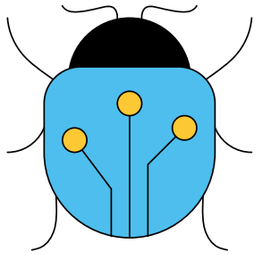
BLACKATOM sent targets instructions for participating in a coding assignment (image intentionally blurred for privacy)



Attacker-owned Github repositories, including a malicious coding assignment (image intentionally blurred for privacy)

The payload was SYSJOKER, a multi-platform backdoor first reported on in 2022, including variants for Windows, Linux and Mac that reached out to Drive to retrieve a C2 address. The latest variant from September 2023 used Microsoft's OneDrive to host the C2 address. Upon discovering the activity, we disrupted attacker-controlled Drive URLs and have deployed updated malware signatures for SYSJOKER to protect users.

This campaign demonstrated more finely tuned operational targeting than we've typically seen from Hamas-linked groups in the past. We've seen similar advances in other clusters of threat actor groups as they mature and evolve. It is possible we are at the start of a similar evolution with Hamas-linked groups.



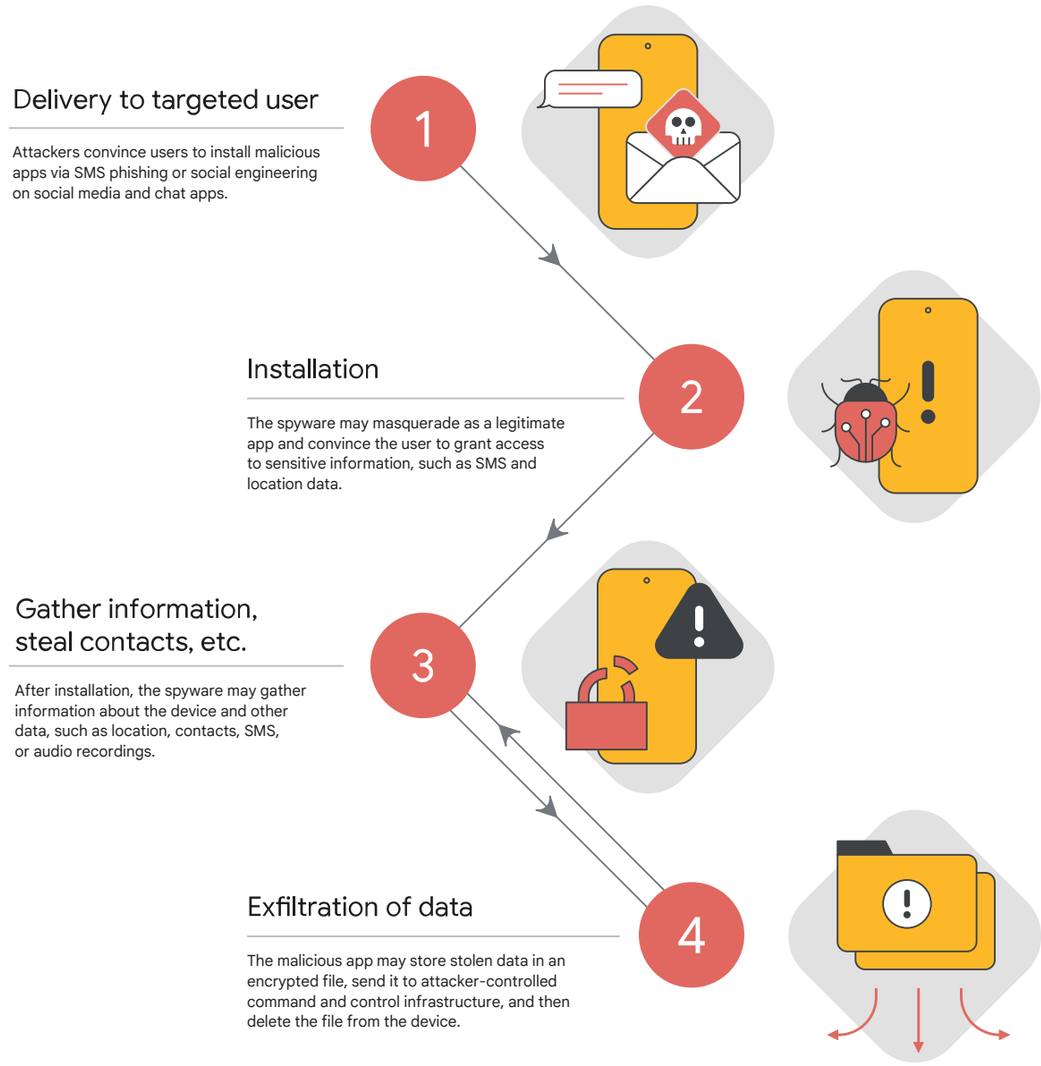
Hamas-linked cyber operations tend to be simple but effective. However, one recent campaign demonstrated more advanced capabilities, including elaborate social engineering to deliver custom malware to high-value targets.

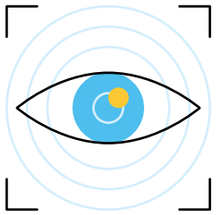
Section 4

Mobile malware is often a tool-of-choice in cyber espionage campaigns targeting Israel

Mobile malware is a key component in the operational toolkit of Iran- and Palestine-based actors, who use malicious mobile apps to collect intelligence on users' communications, contacts, real time location, and other device activity. Prior to October 7, cyber actors linked to Hamas and Iran targeted users based in Israel with Android malware. This activity was in-line with their standard operations, and was likely part of ongoing efforts to collect intelligence about targets-of-interest. Immediately following the Hamas attack on October 7, mobile malware was a central part of efforts to collect intelligence on Israel-based users. Just days after the conflict began, unidentified cyber actors attempted to exploit Israel-based users' need for real-time emergency alerts, distributing malicious apps that masqueraded as Israel's "Red Alert" missile warning app.

ANATOMY OF A MOBILE SPYWARE CAMPAIGN





Hamas-linked groups regularly use mobile spyware in attempts to gather intelligence on their targets. In 2023, we discovered and disrupted multiple Android malware campaigns tied to Hamas-affiliated actors.

Hamas-linked actors targeting Android users in Israel and Palestine

Hamas-linked groups regularly use mobile spyware in attempts to gather intelligence on their targets, and in 2023 we discovered and disrupted multiple Android malware campaigns tied to Hamas-affiliated actors. In August 2023, for example, Hamas-linked group DESERTVARNISH distributed MOAAZDROID Android spyware, which masquerades as Telegram, to users based in Israel and Palestine. The app was not on the Play store, and DESERTVARNISH likely distributed it via WhatsApp messages. MOAAZDROID includes standard mobile spyware functionality, including the permissions to read contacts and SMS data. MOAAZDROID also has permissions to send SMS messages, which may be used for phishing additional targets. The app stores stolen data in an encrypted file, sends it to an attacker-controlled command and control infrastructure, and then deletes the file from the device.

In October 2023, we discovered updated versions of LOVELYDROID, Android spyware linked to DESERTVARNISH, including several active infections impacting devices in Israel. The updated samples had creation times dating back to mid-2023, and were not published to the Play store. The updated LOVELYDROID had a similar code flow to prior versions and included a command and control communications mechanism commonly used by IoT devices. It included standard spyware features, including stealing SMS messages and contacts and the ability to record calls. For impacted users who were infected with LOVELYDROID, including several users based in Israel, we issued a warning to prompt them to uninstall the malware from their device.

Iran targeting mobile devices for intelligence collection

For years, Iran has heavily used mobile spyware for domestic surveillance, targeting Iranian dissidents, activists, and perceived threats to regime stability with a variety of malicious apps. These apps often masquerade as utilities like VPNs and Telegram clones, but also include standard backdoor features for monitoring a user's device. Iranian groups typically distribute Android spyware outside of the Play store through vectors like SMS phishing and social engineering on social media and chat apps.

Iran has also recently targeted mobile devices in Israel, likely for intelligence collection. In September 2023, we discovered Android spyware linked to Iran-backed group MYSTICDOME (a.k.a., UNC1530). We identified and disrupted three new samples of MYTHDROID, also known publicly as AhMyth. MYTHDROID is an Android backdoor with basic functionality that has been widely used by various APT actors since it was originally released in 2017 on Github as an open source research project. To distribute MYTHDROID, MYSTICDOME created Israel-themed domains where they hosted the malicious APK. We suspect social engineering was used to convince users to download the applications. We did not observe distribution via the Play store.

MYSTICDOME has also used social engineering to distribute a new Android spyware tool that we call SOLODROID. Four total instances of SOLODROID were observed, all of which masqueraded as social media and dating applications targeting users in Israel. SOLODROID is capable of collecting files from a user device. MYSTICDOME distributed SOLODROID using Firebase projects that 302-redirected users to the Play store, where they were prompted to install the spyware. We've disrupted this effort by taking down the Google Cloud and Firebase projects, while also blocking and removing the apps from the Play store. Iran-backed groups typically adapt and retool in response to defensive measures, and we expect them to continue their attempts to develop and deploy mobile malware capabilities in the future.

PROTECTING USERS FROM MOBILE SPYWARE

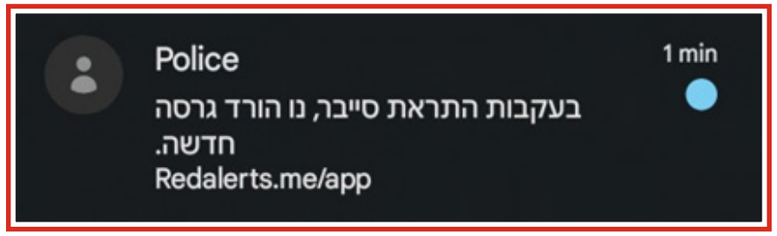
Google continuously monitors for Android spyware, both within and outside the Play store. We deploy and constantly update detections that protect users' devices and prevent malicious actors from publishing malware to the Play store. In the event we identify spyware, we take action to disrupt not just the spyware itself, but the infrastructure supporting the application. These actions include:

- Adding malicious domains / URLs / files to Safe Browsing blocklists, which protects users from exploitation across Chrome and other browsers, Gmail, Search, Ads, Drive, and Android
- Authoring detections to deploy in Google Play Protect, which offers users protection in and outside of Google Play, checking devices for potentially harmful apps regardless of the install source
- Banning malicious apps and their developers from Google Play
- Takedown of infrastructure connected with the spyware, such as attacker-controlled cloud projects and Firebase applications
- Authoring detections for spam classifiers in Gmail and Drive

Safe Browsing also protects Chrome users on Android by showing them warnings before they visit dangerous sites. App scanning infrastructure protects Google Play and powers Verify Apps to additionally protect users who install apps from outside Google Play.

Malicious “Red Alert” apps impersonating Israel’s air strike alert app

In October 2023, just days after the October 7 attack, we identified Android malware with themes designed to exploit concerns surrounding the Israel-Hamas conflict. In at least two cases, the malware masqueraded as Israel’s “Red Alert” app, an application that notifies users in Israel of incoming rocket attacks.

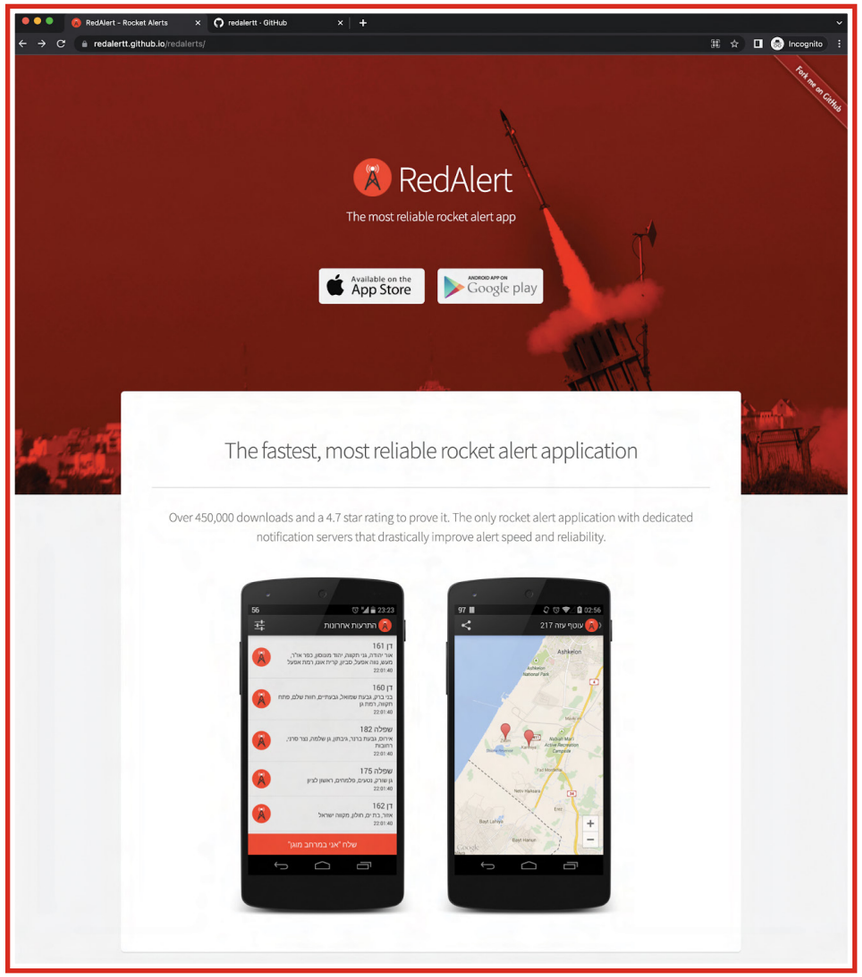


SMS phishing message distributing REDRUSE, a trojanized clone of Israel’s “Red Alert” app

REDRUSE: a trojanized clone of Red Alert

Within days of the outbreak of the conflict, an unidentified actor created a trojanized clone of the Red Alert app. The fake application, distributed as “redlalerts”, contained a backdoor that exfiltrated contacts, messaging data and location. Threat actors targeted Israeli users and spread the trojanized Red Alert app via SMS phishing (smishing). The SMS messages were sent from a spoofed sender impersonating the police and included a link masquerading as the official rocket alert application. The malware was also distributed via a GitHub repository.

We deployed detections to protect Android devices, and added malicious domains associated with the app to Safe Browsing to protect users from further exploitation. The infrastructure was taken down in conjunction with partners.



GitHub repository distributing REDRUSE

AHMYTHRAT masquerading as Red Alert app

Later in October 2023, we identified a second Android backdoor impersonating Israel’s Red Alert app. The malware, AHMYTHRAT, is a variant of the publicly available AhMyth Android backdoor, which is designed to enable remote control of a compromised device. Its features include enumerating device location, capturing microphone recordings, retrieving contact lists, accessing call data, SMS, and downloading and uploading files. The Red Alert-themed AHMYTHRAT sample was configured to connect to an attacker-controlled command and control (C2 or C&C) .

Conclusion

Cyber operations are a key feature of conflict, affecting those closest to the epicenter of warfare as well as those far away. Each conflict is unique, and the operations detailed here represent a blueprint for how cyber operations can impact a region, even when they are not employed by the belligerents in direct support of the kinetic conflict.

As this report reflects, cyber capabilities can be quickly deployed at minimal cost by actors who may wish to avoid armed conflict — they are a tool of first resort. These tools give regional rivals the ability to quickly gather information and disrupt daily life — all while remaining below the level of direct military action. Adversaries can also use these operations to telegraph intent and influence how a conflict is perceived, without escalating or directly taking part in on-the-ground confrontation. This limits potential blowback while also giving regional players the opportunity to project power through the cyber domain. We anticipate that lessons learned recently will be valuable in periods of global uncertainty as we work together to foster a safer and more secure future.

Google is committed to protecting the safety and security of online users and our platforms. Across all Google products, we incorporate industry-leading security features and protections to keep our users safe. We also use the results of our research to improve the safety and security of our products. We believe one of the best ways we can help is by sharing our findings with the security community to raise awareness. We hope that improved understanding of threats will lead to stronger protections across the industry.

This report includes extensive research from dozens of sources and comes in print and online versions. The online version contains links to relevant sources.