Hacktivists take sides in Israel-Palestinian war

therecord.media/hacktivists-take-sides-israel-palestinian

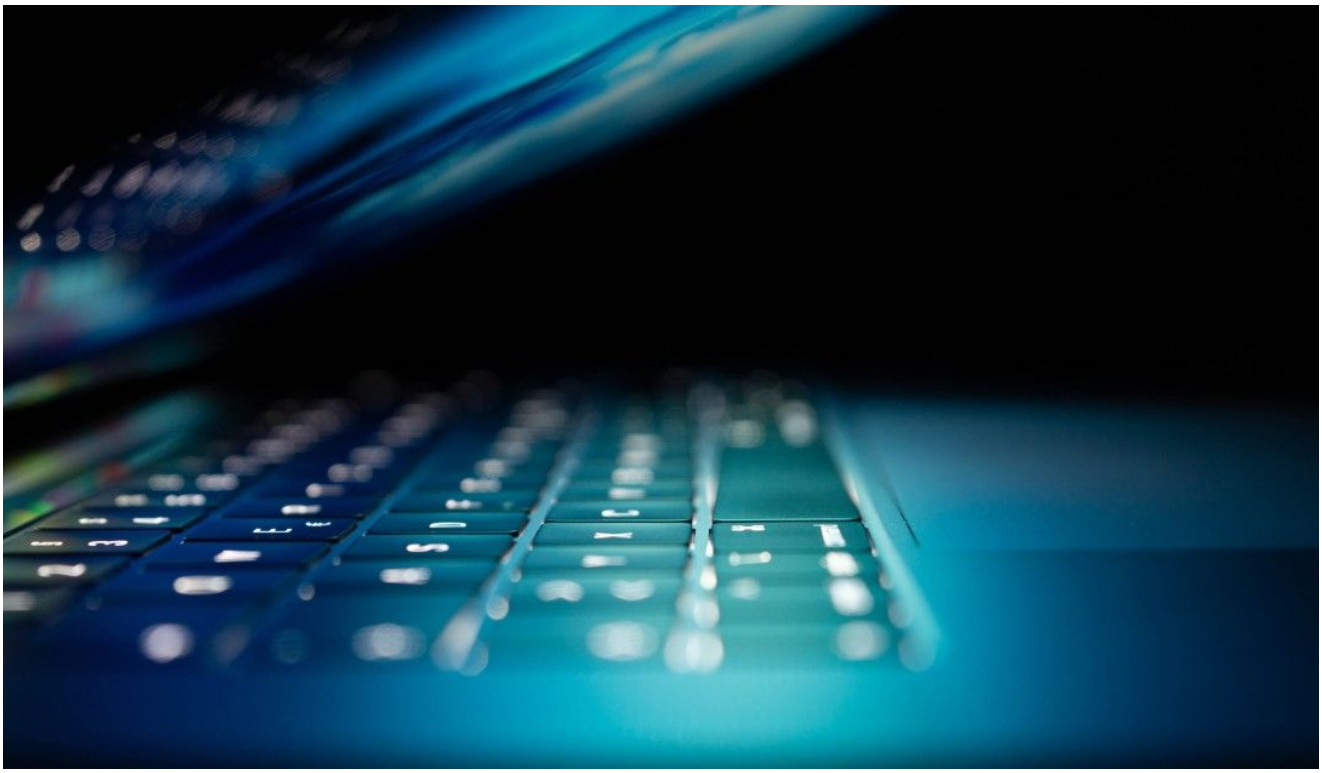

Image: Philipp Katzenberger via Unsplash

Politically-motivated hackers from all over the world have leapt into the escalating conflict between Israel and the Palestinian group Hamas.

Hacktivists are using tactics similar to what was seen at the beginning of the Ukraine-Russia war: leaking stolen documents and launching distributed denial-of-service and defacement attacks on government websites, media outlets, and critical infrastructure.

The recent surge in hacktivism comes on the heels of the Red Cross issuing ethical guidelines for civilian hackers participating in armed conflicts, encouraging them to be more "humane."

Since Hamas fighters launched their assault on Saturday, nearly 60 groups have targeted entities connected with either Palestine or Israel, mostly with denial-of-service attacks (DDoS) attacks.

Read More: Social media platforms foment disinformation about war in Israel

Cyberattacks on Israel have mainly come from hacktivists based in Russia, Bangladesh, Pakistan, Morocco, and Iran, according to Will Thomas, a cyber threat intelligence researcher who has been monitoring the activity.

The attacks include sharing credentials for Israeli websites, leaking stolen data, launching DDoS attacks, and hijacking application programming interfaces (APIs) to send mobile push messages, he said.

On Sunday, the pro-Palestinian hacktivist group AnonGhost exploited an API bug in the RedAlert app, which provides Israelis with real-time missile warnings, to send a fake threat of nuclear attack, according to the cybersecurity firm Group-IB. The Red Alert app has over one million downloads on the Google Play store.

“Hacktivists are generally associated with conducting small-scale DDoS attacks and defacement. However, as the ongoing conflict shows, their actions can be far more devastating and costly,” the researchers said.

AnonGhost also claimed that it had hacked an Israeli flight booking website and the official app used by police officers in the Israel Defense Forces. The group shared the National Cyber Directorate head's phone number, encouraging others to spam him.

“We are very proud that we are defending Palestine. It's a duty to try to establish peace for humanity, spreading awareness. As you can see religion doesn't make us different, or nationality, we are united together," the hackers said on Telegram.

One of the most active Russian hacktivist groups, Killnet, also sided with Hamas.

On Sunday, the group posted a message on Telegram accusing the Israeli government of supporting Ukraine during the war with Russia and warning of cyberattacks.

"You've betrayed Russia. We will target all Israeli government systems with our attacks!" the group said.

Killnet then claimed that it had taken down an Israeli government website and the website of the security agency Shin Bet. Both websites were indeed offline for a period on Sunday.

In the past, Moscow has tried to act as a mediator in the conflict and play both sides, but its growing military alliance with Iran, an enemy of Israel and supporter of Hamas, has complicated the situation.

Anonymous Sudan, a religiously-motivated hacker group, said it is behind an attack on the Jerusalem Post, Israel's most-read English news website. As of Tuesday morning, the website was still down.

> The Jerusalem Post has been targeted by multiple cyberattacks this morning causing our site to crash.
>
> We'll be back soon and will continue to be the top source of information on Operation Swords of Iron and the murderous attacks by Hamas. pic.twitter.com/6S2GOl6Wma
>
> — The Jerusalem Post (@Jerusalem_Post) October 8, 2023

On Tuesday, Anonymous Sudan also claimed to have teamed up with the hacking group SiegedSec to target Israeli industrial control systems and navigational satellite systems.

Anti-Hamas hacktivist attacks

Fewer hacktivist groups have come out in support of Israel.

The Indian Cyber Force, a pro-India group known for its recent attacks on the Canadian military website, claimed responsibility for targeting a Palestinian telecommunications company, the National Bank's website, a government webmail service, and the official Hamas website. As of Tuesday morning, most of these websites were inaccessible.

In response, pro-Palestinian hackers launched cyberattacks on Indian government websites on Tuesday, accusing India of supporting Israel. Indian cyber officials said they had successfully countered these attacks.

Other pro-Israel hacking groups include the India-linked Team UCC Ops, the relatively new and previously unknown hacktivist gangs Garuna Ops and SilenOne.

> 9 OCT Israel-Palestine #cybertracker
>
> Current visible cyber landscape. A large group targeting #Israel - almost all these groups have been doing it for years. Current baseline , but will evolve.
>
> For awareness - report to follow#cybersecurity #infosec #IsraelPalestineWar pic.twitter.com/AJYY3bSp0Y
>
> — CyberKnow (@Cyberknow20) October 8, 2023

Some hacktivists, meanwhile, have chosen to attack both sides.
“As you might know, we don't like Israel, but we also don't like war! So, as we have attacked Israel in the past, we now attack the Gaza region,” the hacker group ThreatSec wrote on Telegram.

The group claimed it hacked a major Gaza internet provider called AlfaNet. When asked about the attack by Wired, AlfaNet said that its communications were disrupted because the headquarters had been completely destroyed, but the company did not mention any cyberattacks.

Chaos and uncertainty

As is common with hacktivist activity, not all of the claimed attacks are real. Some groups are merely seeking attention, while others want to fuel the disinformation and propaganda surrounding the conflict. Many of the attacks couldn't be independently verified.

On Sunday, the pro-Iranian hacker group Cyber Avengers claimed it successfully attacked Dorad power plant in Israel, but researchers discovered that the data posted was actually stolen by the ransomware gang MosesStaff back in 2022.

"This is yet another example of how hacktivists try to generate hype by posting data from past attacks and masquerading them as recent ones in order to attract attention," Group-IB said.

Digital attacks on Israel began long before Hamas launched its surprise attack.

According to a recent report from Microsoft, Israel is the most frequently targeted country for cyberattacks in the Middle East. This year, researchers have observed a surge in activity originating from the Gaza-based group known as Storm-1133, focusing on Israeli energy, defense, and telecom sectors.

Additionally, Iran, a longstanding ally of Hamas, has conducted influence operations in the region to support Palestinian resistance, sow panic among Israeli citizens, and counter the normalization of Arab-Israeli relations, according to Microsoft.

- News
- Government
- Nation-state

No previous article

No new articles

Daryna Antoniuk

Daryna Antoniuk is a freelance reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.