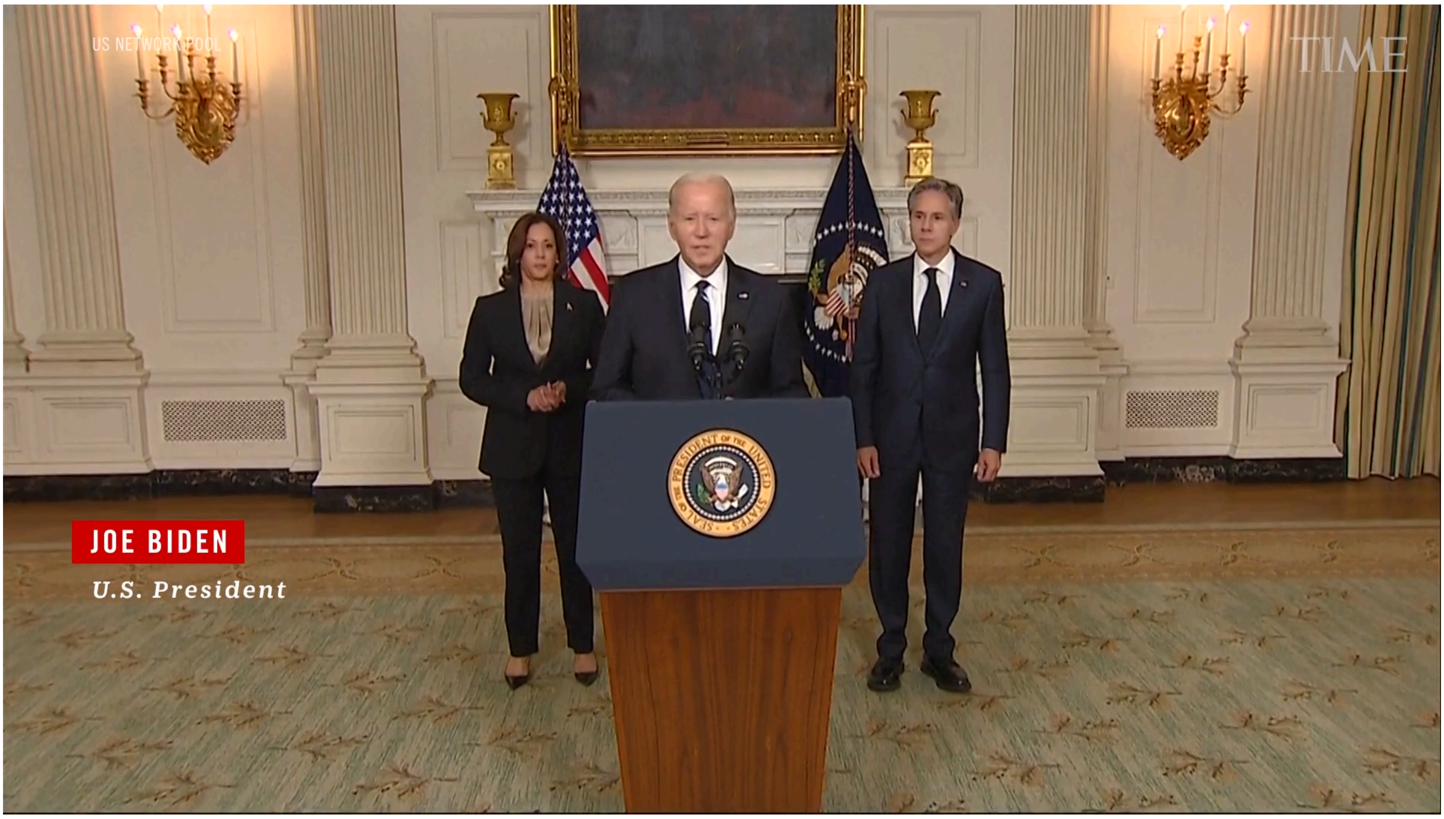
TIME SUBSCRIBE

TECH SECURITY

Cyberattacks Targeting Israel Are Rising After Hamas Assault

4 MINUTE READ



BY RYAN GALLAGHER AND JORDAN ROBERTSON / BLOOMBERG

OCTOBER 10, 2023 4:23 PM EDT

Hacking groups, including some tied to Russia, are attacking Israeli government and media websites, allying themselves with the Palestinian military group Hamas that launched a series of deadly strikes on the country over the weekend.

Killnet, a group that purports to be made of up patriotic Russian volunteer hackers, announced on Sunday that it would target all Israeli government systems with distributed denial-of-service attacks, a type of cyberattack known as DDoS that floods websites with traffic and forces them offline. The group said it blamed Israel for the bloodshed and accused the country of supporting Ukraine and NATO. Killnet then claimed it brought down an Israeli government website and the website of security agency Shin Bet for a period of time on Sunday.

The group's claim couldn't immediately be substantiated. Both websites were down for a period on Sunday, according to the website monitoring site check-host.net.

Meanwhile, Anonymous Sudan — a hacking group that cybersecurity experts suspect as being a Russian front group — declared its support for the "Palestinian resistance" and took credit for attacks on the Jerusalem Post's website, taking it offline briefly on Monday morning. The newspaper wrote in a statement posted on X, formerly known as Twitter, that it had been "targeted by multiple cyberattacks." Its website has since been restored.

"It is clear that other Russian hacktivists are also choosing sides and actively support Hamas in their war against Israel," said Mattias Wåhlén, threat intelligence expert at the cybersecurity firm Truesec AB. "Their actions look more like opportunistic strikes. The conflict creates headlines which attracts groups like Killnet that try to monetize DDoS attacks. It still sends the message that Russia is on the side of Hamas and against Israel."

Scores of other self-styled hacktivist gangs claimed they were launching hacks against Israeli infrastructure, targeting websites associated with power plants and missile alert systems. Many of the attacks couldn't be independently verified.

Cybersecurity firm Group-IB said a hacker group calling itself AnonGhost had compromised a mobile phone application that is used to issue missile alerts to Israelis during periods of conflict. The hackers exploited a vulnerability in the app to insert fake notifications, with phrases such as "death to Israel" and "the nuclear bomb is coming," alongside a swastika, according to Group-IB and screenshots posted by the hackers. Group-IB said the app since appeared to have been removed from Google's Play Store, where it had been downloaded 1 million times. The developers didn't respond to a request for comment.

AnonGhost said in a statement posted on Telegram on Tuesday that it was targeting several other Israeli apps that issue missile alerts and posted what it claimed was a phone number for an Israeli cyber official, whom it encouraged its supporters to “spam.”

Israel is often a target of cyberattacks, and Iranian hackers have been persistently blamed for some of them. However, it wasn’t yet clear if Iran’s hacking forces were engaged in the current conflict.

Read More: Israel Blames Iran-Backed Hackers for Recent University Breach

Pro-Israel groups have waged their own attacks, targeting Palestinian organizations with cyberattacks. One group, calling itself Indian Cyber Force, said it had downed the Palestinian National Bank’s website and Hamas’s website on Sunday. Both were still inaccessible on Monday. The bank couldn’t be located for comment.

Gil Messing, chief of staff for the Israeli cybersecurity firm Check Point Software Technologies Ltd. said the cyberattacks had little impact so far. “The last few days weren’t very prominent in terms of cyber. Some of the groups were carrying out DDoS attacks on some news websites and government websites but none of this was serious or long,” Messing said. “So all in all so far this front is not significant. This of course can change.”

Rob Joyce, director of cybersecurity at the National Security Agency, said there hasn’t been a major cyber component to the conflict yet. Instead, the agency has seen small denial-of-service attacks and minor web defacements, along with the expectation that outside parties would join in amplifying messaging on Hamas’s behalf.

“There may be significant events coming, more hacktivists, more people taking up cyber arms in defense of their cause,” he said, speaking at a security conference on Sea Island in Georgia. “It won’t be sophisticated in the early days. Some times you don’t need to be sophisticated to have an impact.”

(Updates with AnonGhost statement in eighth paragraph.)

--With assistance from Jamie Tarabay.

MORE MUST-READS FROM TIME

- **Nicola Coughlan** Bet on Herself—And Won
- What **Kind of President Would Kamala Harris** Be?
- Is **Adrenal Fatigue** Real?
- Why It's **So Hard to Quit Vaping**
- Our **Guide to Voting** in the 2024 Election
- The **10 Races** That Will Determine Control of the Senate
- Column: How **My Shame Became My Strength**
- Meet TIME's Newest Class of **Next Generation Leaders**

CONTACT US AT LETTERS@TIME.COM

TIME

Health

Sports

Business

Magazine

Tech

The TIME Vault

Personal Finance by TIME Stamped

TIME For Kids

Shopping by TIME Stamped

TIMECO2

Future of Work by Charter

Coupons

TIME Edge

Press Room

Video

TIME Studios

Masthead

U.S. & Canada Customer Care

Newsletters

Global Help Center

Subscribe

Contact the Editors

Digital Magazine

Reprints and Permissions

Give a Gift

Site Map

Shop the TIME Store

Media Kit

Careers

Supplied Partner Content

Modern Slavery Statement

About Us