LILY HAY NEWMAN MATT BURGESS SECURITY OCT 9, 2023 6:21 PM

Activist Hackers Are Racing Into the Israel-Hamas War—for Both Sides

Since the conflict escalated, hackers have targeted dozens of government websites and media outlets with defacements and DDoS attacks, and attempted to overload targets with junk traffic to bring them down.

A salvo of rockets is fired by Palestinian militants from Gaza towards Israel on October 9, 2023. PHOTOGRAPH: IBRAHIM HAMS/GETTY IMAGES

AFTER AN ATTACK on Israel by Hamas on Saturday, Israel declared war and fighting escalated throughout the weekend. As the death toll mounts on both sides and the Israeli Defense Force (IDF) prepares an offensive, hacktivists in the region and around the world have joined the fight.

Within hours of Hamas militants and rockets entering Israel, such "hacktivist" attacks started to spring up against both Israeli and Palestinian websites and applications. In the short period since the conflict escalated, hackers have targeted dozens of government websites and media outlets with defacements and DDoS attacks, attempts to overload targets with junk traffic and bring them down. Some groups claim to have stolen data, attacked internet service providers, and hacked the Israeli missile alert service known as Red Alert.

"I saw at least 60 websites get DDoS attacks," says Will Thomas, a member of the cybersecurity team at the internet infrastructure company Equinix who has been following the online activity. "Half of those are Israeli government sites. I've seen at least five sites be defaced to show 'Free Palestine'–related messages."

Most prominently seen in the war between Russia and Ukraine, it is increasingly common for both ideologically motivated hackers and cybercriminals to remotely

join the chaos on either side of an escalating conflict by attacking government systems or other institutions.

Alex Leslie, a threat intelligence analyst at the security firm Recorded Future, says that he and his colleagues have identified three subsets of activity within the digital pandamonium of the Israel-Hamas war so far. The majority of the digital attacks seem to stem from preexisting groups or a broader context of similar activity adjacent to other conflicts. “The scope is international, but rather limited to preexisting ideological blocs within hacktivism,” Leslie says.

The subgroups that Recorded Future has identified so far are “self-proclaimed ‘Islamic’ hacktivists that claim to support Palestine. These groups have historically targeted India and have been around for years” Leslie says. “Pro-Russian hacktivists that are pivoting to target Israel, likely with the intent of sowing chaos and spreading Russian state narratives. And groups that are ‘new,’ in that they were launched within the last [days] and have limited activities prior to this weekend.”

Since Russia’s 2022 invasion of Ukraine, some prominent hacktivist groups backing Russian interests have emerged, including gangs known as “Anonymous Sudan” and “Killnet,” both of which appeared to wade into the conflict between Hamas and Israel this weekend. Some groups have also been active in reaction to India’s support of Israel, both in favor of and against this support.
Hackers from the group known as AnonGhost, who are seemingly conducting pro-Palestinian campaigns, have been launching DDoS attacks and attempting to target infrastructure and application programming interfaces (APIs). The group claimed the alleged attack on the Israeli Red Alert missile warning platform. Researchers from the threat intelligence firm Group-IB said on Monday that the hackers exploited bugs in Red Alert’s systems to intercept data, send spam messages to some users, and possibly even send fake missile strike warnings. The app’s developers did not return a request from WIRED for comment. The Red Alert app has been targeted by hacktivists in the past, and Hamas itself has previously been accused of circulating malicious imposter versions of Israeli missile alert apps.

Meanwhile, the hacktivist group ThreatSec, which says it has “attacked Israel” previously, claimed it targeted Alfanet, an internet service provider based in the

Gaza Strip. In a post on Telegram, the group claimed to have taken control of servers belonging to the company and impacted its TV station systems.

Doug Madory, director of internet analysis at monitoring firm Kentik, says that Alfanet was inaccessible for around 10 hours on Saturday, October 7—before the hacktivists posted their claim. The ISP's systems have since been back online and communicating with the wider world. "Some of their services could still be broken," Madory says, pointing to an Alfanet TV website and a web portal that were inaccessible on Sunday evening.

In response to a request for comment from WIRED via Facebook Messenger, Alfanet shared a statement in Arabic saying that communications were cut off due to "the complete destruction" of its headquarters. "Crews are working with all their might to restore service after the bombing of the headquarters and the main tower, despite the difficult and dangerous circumstances," the message says via machine translation. The company did not comment on the role of a cyberattack, if any, in the outage.

Internet connectivity in Gaza has also been broadly disrupted by electricity outages as Israel implements what Defense Minister Yoav Gallant called a "complete siege" on Monday, cutting off the region's electricity and supply lines for water, food, and fuel.

Amid the chaos of any erupting kinetic war, hacktivism often fuels disinformation, misinformation, and panic. This can lead to unintended consequences. For some digital actors, unpredictability itself is the goal. "The Indian cyber force actually claimed to DDoS hamas.ps and webmail.gov.ps," Equinix's Thomas says. Meanwhile, "there's one group called the Cyber Avengers who are claiming to steal documents from Israel's national electricity authority. They claimed they stole documents from Israel's Dorad power plant. [But] they are actually known for making up stuff and creating sort of fake infrastructure and screenshotting."

Victoria Kivilevich, director of threat research at the Israeli cybersecurity firm Kela, says that while hacktivist activity may add to the turmoil, she doesn't expect that it will significantly impact warfare on the ground.

"We can expect to see more groups and DDoS attacks because of the severity of the conflict and general evolution of hacktivist groups, however, so far we don't

expect any significant impact on the overall threat landscape."

Last week, the International Committee of the Red Cross put forth rules of engagement for "civilian hackers" wading into a conflict. The eight directives, which are based on international human rights law, came primarily in the context of Russia's war on Ukraine, but they are relevant globally. They emphasize minimizing threats to civilians' safety and ban cyberattacks on health care facilities. They also ban use of computer worms and require that actors "comply with these rules even if the enemy does not."

In response to the release, some hacktivist groups active on both sides of Russia's war in Ukraine said they would attempt to follow the rules when possible, but others said it wasn't feasible or rejected the premise entirely. In its efforts to gather grassroots support, Ukraine has encouraged a sort of legitimized version of hacktivism by establishing a volunteer "IT Army" for its war effort against Russia. All of this has created a nuanced and unpredictable element in the digital component of kinetic wars.

"What we saw in Ukraine with hacktivism has set a precedent moving forward," Recorded Future's Leslie says. "We believe that many of these groups are motivated by attention. That's why we see so many groups that probably shouldn't be active in this conflict for geopolitical reasons jumping into the fray. They want people to know that they're active and capable of reacting to any event—even if the intentions are disingenuous. Hacktivism is intertwined with information and influence operations, and it is here to stay."

Updated at 10:45 am ET, October 10, 2023, to clarify Will Thomas' role at Equinix.

You Might Also Like ...

Lily Hay Newman is a senior writer at WIRED focused on information security, digital privacy, and hacking. She previously worked as a technology reporter at Slate, and was the staff writer for Future Tense, a publication and partnership between Slate, the New America Foundation, and Arizona State University. Her work... Read more

SENIOR WRITER

Matt Burgess is a senior writer at WIRED focused on information security, privacy, and data regulation in Europe. He graduated from the University of Sheffield with a degree in journalism and now lives in London. Send tips to Matt_Burgess@wired.com.

SENIOR WRITER

TOPICS ISRAEL ISRAEL-HAMAS WAR SECURITY HACKING CYBERATTACKS WAR

READ MORE

Hacker Charged With Seeking to Kill Using Cyberattacks on Hospitals

The US has accused two brothers of being part of the hacker group Anonymous Sudan, which allegedly went on a wild cyberattack spree that hit hundreds of targets—and, for one of the two men, even put lives at risk.

ANDY GREENBERG

Iranian Hackers Tried to Give Hacked Trump Campaign Emails to Dems

Plus: The FBI dismantles the largest-ever China-backed botnet, the DOJ charges two men with a $243 million crypto theft, Apple's MacOS Sequoia breaks cybersecurity tools, and more.

ANDY GREENBERG

ICE Signs $2 Million Contract With Spyware Maker Paragon Solutions

US Immigration and Customs Enforcement's one-year contract with Paragon's US subsidiary comes amid the Biden administration's years-long crackdown on commercial spyware vendors.

VAS PANAGIOTOPOULOS

A Mysterious Hacking Group Has 2 New Tools to Steal Data From Air-Gapped Machines

It's hard enough creating one air-gap-jumping tool. Researchers say the group GoldenJackal did it twice in five years.

DAN GOODIN, ARS TECHNICA

Pig Butchering Scams Are Going High Tech

Scammers in Southeast Asia are increasingly turning to AI, deepfakes, and dangerous malware in a way that makes their pig butchering operations even more convincing.

MATT BURGESS

Internet Archive Breach Exposes 31 Million Users

The hack exposed the data of 31 million users as the embattled Wayback Machine maker scrambles to stay online and contain the fallout of digital—and legal—attacks.

LILY HAY NEWMAN

Notorious Evil Corp Hackers Targeted NATO Allies for Russian Intelligence

UK law enforcement and international partners have released new details about the cybercriminal gang Evil Corp, including its use of the Lockbit ransomware platform and ties to Russian intelligence.

LILY HAY NEWMAN

The War on Passwords Is One Step Closer to Being Over

“Passkeys,” the secure authentication mechanism built to replace passwords, are getting more portable and easier for organizations to implement thanks to new initiatives the FIDO Alliance announced on Monday.

LILY HAY NEWMAN