This article was published more than **1 year ago**

Democracy Dies in Darkness

TECH POLICY

Pro-Hamas hackers send fake rocket alerts, knock websites offline

The attacks have added a cyber dimension to the conflict

2 min 26

By Joseph Menn

October 9, 2023 at 7:52 p.m. EDT

A wave of hacking attacks on Israeli targets has added a cyber dimension to the conflict with Hamas.

The most significant measures by the Palestinians may prove to be preparation early in the year, when a Gaza Strip group that Microsoft calls Storm-1133 went after energy, defense and telecommunications companies inside Israel.

The group used fake LinkedIn profiles and posed as software developers or project managers to send malware to employees at those targets and install back doors for later communications, Microsoft said in a recent report. The reference was short and did not provide details.

Other hacks, mainly by self-proclaimed hacktivist allies of the Palestinians, were aimed at sowing confusion or alarm.

Various groups launched dozens of denial-of-service attacks at government and private websites, knocking them offline but causing no lasting damage.

One of the most effective was against the website of the Jerusalem Post, a major source of reporting on the fast-changing conflict. The attacks began Sunday morning and continued through much of Monday.

That denial-of-service was claimed by Anonymous Sudan, which previously mustered enough electronic firepower to make Microsoft services hard to reach. The group, which says it supports causes important to Muslims, is allied with KillNet, a Russian nationalist hacking group.

The Sudan group has added significantly to KillNet's prowess, leading some to speculate that both are fronts for Russian government services.

Pro-Palestinian hackers AnonGhost said it was behind an attack on an Israeli app that warns residents of incoming rocket strikes.

The group said it sent fake rocket alerts and even said a nuclear bomb was incoming.

The attack was confirmed by analysts at security companies Group-IB and Recorded Future, which said the hackers had abused an application programming interface to send the alerts as if it were a legitimate source of military information.

There are many such apps, and the app in question only had between 10,000 and 20,000 users, said Recorded Future analyst Alexander Leslie.

“For those who did use that specific application prior to its removal from the Google Play Store — there are obvious security and safety risks for false missile alerts at a time like this,” Leslie said. “It is a serious escalation in targeting and intent, regardless of its impact.”