

Israel Braces for Possible Cyber Attack

Israel is bracing for a “potentially crippling” cyberattack against the country’s major companies and websites, Israel Hayom learned Tuesday. The attack is set to take place on April 7, which this year will be the eve of Holocaust Remembrance Day.

The planned assault is part of hacktivist group Anonymous’ ongoing #OpIsrael campaign, which was launched in March in a show of solidarity with the Palestinians. As part of the campaign, Anonymous—which has since been joined by several other hacktivist groups including Sector404 and RedHack—said that on April 7 that it would “launch a coordinated, massive cyberattack on Israeli targets with the intent of erasing Israel from the Internet.”

Last week, the three groups claimed they breached the Mossad’s mainframe, accessed classified information and leaked the personal details of over 34,000 of the intelligence agency’s officers and agents worldwide online. The Mossad did not comment on the matter.

According to Shai Blitzblau, CEO of Maglan Information Defense Technologies Research, the attack is likely to target government websites as well as major banks and credit cards companies.

Israel’s financial system was targeted in a series of cyberattacks in early 2012: Two of Israel’s major banks, Hapoalim and Leumi, as well as three major credit card companies—Isracard, Leumi Card and Visa Cal—were hacked, as was the Tel Aviv Stock Exchange.

Hackers are also constantly trying to target Israel’s critical infrastructure, such as its power and water grids: In

September 2012, Yiftach Ron-Tal, chairman of the Israel Electric Corporation's board of directors, revealed that IEC sees between 10,000 and 20,000 attempted cyberattacks a day. Ron-Tal was speaking at the annual cyber summit, hosted by the Israel Institute for National Security Studies.

"Cyberattacks worldwide are becoming more powerful every day, but the [coming] attack won't be substantially different from what we've seen before," Blitzblau said. "The hackers are likely to target the top 100 Israeli websites and they will probably try introducing Trojan horses into their servers, to infect as many users as possible."

The systems used by the majority of Israel's banks, credit card and telecommunication companies are susceptible to denial-of-service attacks that use the availability of virtual host-servers to create massive traffic backlogs, which eventually crash the websites using their services.

Meanwhile, the military is also gearing for an increase in cyberattacks: In mid-February, the Israel Defense Forces set up an official cyber war room, meant to improve the IDF's ability to thwart what military sources called "the constant attempts" to hack into the IDF's computer systems.

The IDF officially defined cyber warfare as the fifth arena of warfare, alongside land, sea, air and space, in 2012.

For the original article, visit .