'Cyber Toufan' Hacktivists Leaked 100-Plus Israeli Orgs in One Month

By Nate Nelson

Published: 2024-01-04 · Archived: 2026-04-05 18:37:16 UTC

Source: Issam Elhafti via Alamy Stock Photo

Since mid-November, one Iran-linked hacktivist group has managed to breach more than 100 organizations in and around Israel, wiping servers, leaking sensitive data, and spreading follow-on attacks down the supply chain.

Since October 7, anti-Israel hacktivists have proven largely ineffectual — quick to make grandiose claims on social media, less likely to provide evidence to back those claims up. Not so with "Cyber Toufan al-Aqsa" ("Toufan" in Arabic meaning flood).

On November 16, the group compromised Signature-IT, an Israeli company that specializes in hosting international websites for businesses. Through it, the hacktivists managed to reach dozens of significant companies and government organizations in Israel, as well as international companies doing business with Israel. And though the leaks have slowed (but not stopped) in recent days, the group continues to twist the knife by performing follow-on email attacks against victims' employees and customers.

"We've seen over 150 hacktivist groups operating in the cyber war in Israel," says Check Point Software's chief of staff, Gil Messing. "CyberToufan is by far the most prominent one."

Israel's Most Prolific Hacktivist Enemy

Cyber Toufan first announced itself to the world by creating a Telegram channel a month into the Gaza war, and releasing a statement.

"Stage one of #OpCyberToufan involved the complete wiping out and destruction of over a [sic] 1,000 servers and critical databases of the enemy," it read, in part. The operation compromised more than 150 targets, it continued, spread across government, manufacturing, e-commerce, cybersecurity, and other sectors. "The attack was carried out successfully without so much as a hitch," it added.

Empty claims like these have been made ad nauseum since October 7, but this time it was actually true.

Shortly after founding its Telegram channel, Cyber Toufan published data belonging to ACE Israel, a branch of ACE Hardware. The next day it was Shefa Online, an Israeli e-commerce company.

Then the group started publishing two leaks per day. On day three it was Radware and Max Security, two Israeli cybersecurity companies. On day four, the Israel Innovation Authority and Ikea Israel.

Other government targets followed, including Israel's Ministry of Health, National Archive, Nature and Parks Authority, Ministry of Welfare and Social Security, Securities Authority, and State Payment Gateway. Israeli branches of multinational companies like Toyota and Toys 'R' Us were attacked, as well as companies that simply did business with Israeli firms, like Berkshire eSupply, a subsidiary of Berkshire Hathaway, and SpaceX.

The Extent of the Damage

Many of these victims appear to derive from an initial breach and wiping of servers belonging to Signature-IT.

This supply chain link bears significantly on the nature of the leaked data. In each case, Messing explains, "the data was always exactly what these companies were using in their specific [Signature-IT hosted] websites. So it could be CRM data, it could be order — like for IKEA, there were names and what exactly they bought from IKEA."

The leaks were only part of the story, though, as even after its leak schedule ceased on December 27, Cyber Toufan is continuing to cause damage to its victims, as well as those connected to them.

On one front, the group is using its victims' corporate email domains to blast hacktivist messages to as many people as possible. For example, in an email sent to contacts stored in Radware's customer relationship management (CRM) platform, the group asks that recipients "don't have the blood of our children on your hands," because "purchasing Israeli cyber and tech products/services is financial contribution towards the murder of our children in Gaza and the destruction of their homes, schools, and hospitals."

Meanwhile, as a result of having their servers wiped, websites belonging to many Cyber Toufan victims — more than a dozen as of last week, according to a blog post by cyber researcher Kevin Beaumont

— remain down.

For example, more than a month after its breach was first announced, at the time of this writing, the website for Berkshire eSupply is down. The company has since filed a data breach notification with the Maine Attorney General, estimating that 16,736 people were affected. In a public disclosure, the company acknowledged that "we

do not have the precise scope or content of the data that was accessed," but added that it was acting out of an abundance of caution, and "in line with the opinion of cyber experts who investigated the matter, these (our) systems remained fully secured and were unaffected by the event."

"You cannot compare Cyber Toufan to any other Gaza hacktivist group because the damage they've created is by far at a larger scale, and very systematic," Messing says. He argues that the scale and sophistication seen here — alongside overlaps in methodology and the wiper malware utilized against victims, as well as the nature of the targets and data leaked — suggests links between Cyber Toufan and Iran.

"Cumulatively, we're talking about millions of records of Israelis. This is very serious," he emphasizes. "It did not cripple the Israeli economy, but it did create a lot of damage, and some companies are still paying the price."

About the Author

Contributing Writer

Nate Nelson is a journalist and scriptwriter. He writes for "Darknet Diaries" — the most popular podcast in cybersecurity — and co-created the former Top 20 tech podcast "Malicious Life." Before joining Dark Reading, he was a reporter at Threatpost.