DragonForce Malaysia attacks Israeli institutions: Radware

By Gaurav Sharma

Published: 2023-04-14 · Archived: 2026-04-02 10:38:13 UTC

After being absent from this year's OpIsrael campaign, the pro-Palestinian hacktivist group DragonForce Malaysia has returned for a third year with an operation targeting Israel. The group's rebranded campaign, OpsPetir, replaced OpsBedil and currently overlaps with OpIsrael. As a result, those who directly or indirectly support the country of Israel could become a target of OpsPetir, which is anticipated to run between April 12 and Al Quds Day on April 21. This is according to a new Radware cybersecurity advisory.

Some of OpsPetir's first attacks on Israel were reported against universities and financial institutions. During the coming days, Radware expects campaign targets to include religious and healthcare organisations, service providers, transportation, and government agencies. Attacks will likely range from scanning and exploiting to data dumps, denial-of-service attacks, and website defacements.

According to Daniel Smith, head of research for Radware's threat intelligence division, "To draw attention to its political statement, DragonForce Malaysia aims to disrupt and temporarily disable online services and websites for multiple organisations and government institutions."

"We expect dozens of members of DragonForce Malaysia will use a new denial-of-service tool, called CyberTroopers, which was released by a member of the OpsPetir group. It's interesting to note in a screenshot shared by the CyberTroopers creator that it appears the threat actor is using ChatGPT for personal projects," he adds.

CyberTroopers is an obfuscated Python program, which includes functionality to download lists of free and open proxy and SOCKS services on the internet from free-proxy-list[.]net and proxyscrape[.]com. The collected proxy and SOCKS services are leveraged to spoof and randomise the origin of the attacks and increase the complexity of detection and mitigation for L7 application attacks. Furthermore, by exploiting the tool's TCP, UDP and HTTP flooding capabilities, the group will aim to disrupt and temporarily disable online services and websites to draw attention to their political statement.

In June of 2021, DragonForce Malaysia launched OpsBedil in response to an Israeli ambassador to Singapore stating that Israel was ready to begin working towards establishing ties with Southeast Asia's Muslim-majority nations. The following year, in April, the group launched OpsBedil Reloaded in reaction to political confrontation in Israel.

After being absent during the return of OpIsrael 2023 on April 11, the threat group posted a statement in their forum stating that an operation targeting Israel, OpsPetir, will officially begin on April 12 at 9.30 pm Malaysia Time, or 2.30 pm Israel time, and is projected to last until April 20.

The group has been observed working with several threat groups over the years, including the T3 dimension Team, Reliks Crew, and AnonGhost. In addition, DragonForce Malaysia has an active forum where threat actors

post-campaign announcements and discuss varying tactics, techniques, and procedures. The group also has a Telegram channel, but this year, most of its content is replicated throughout the forum and other social media platforms, including Discord. Before OpsPetir, DragonForce Malaysia targeted India with OpsPatuk, a reactionary operation related to a political figure's controversial statements in India about the Prophet Muhammad.
