

# DragonForce Malaysia – #OpsBedil

Renewed Hactivism in the Middle East Persists  
With New Digital Attacks

JULY 13, 2021

During the month of May, increasing tensions in the Middle East resulted in renewed hactivist operations throughout the region. The digital attacks in May presented a certain level of risk for unprotected sites as threat actors targeted organizations in the telecommunications, financial sectors and government agencies. At the moment, physical actions have deescalated in the region since the last incursion, but digital attacks have persisted into June. Cyber events in the Middle East have become reactionary over the past year; cases of hactivism in the region typically follow physical or political confrontations.

## #OpsBedil

#OpsBedil is a hactivist operation currently targeting several verticals and government agencies in the Middle East. It is the latest digital campaign to target the region and is being conducted by threat actors in Southeast Asia, specifically Malaysia and Indonesia. Attacks performed under #OpsBedil are considered a political response to the Israeli ambassador to Singapore stating in June that Israel is ready to work towards establishing ties with Southeast Asia's Muslim-majority nations. Malaysia, which is over 60% Muslim and supports Palestine, has a significant presence of hactivist and Palestinian militants. As a result of this call to establish ties, hactivists in the region began targeting Israeli assets in June with a series of DoS attacks, data leaks and defacement campaigns. The group condemns the proposal to establish ties and reiterates their ongoing support of Palestine with digital attacks.

## DragonForce Malaysia

The driving force behind #OpsBedil is DragonForce Malaysia (DFM), a pro-Palestinian hactivist group located in Malaysia. DFM has also been observed working in collaboration with several other hactivist groups, including T3S and SBC x PANOC. DFM has a website and a forum where threat actors conduct most of their operational discussions. DFM also has a Telegram channel, but most of the content is repeated throughout the forum and other social media outlets. In addition to leaking content in their Telegram channel, the group has also posted details on Pastebin, AnonFiles and Google Drive.

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists  
With New Digital Attacks

JULY 13, 2021



Figure 1: OpsBedil campaign flyer

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists With New Digital Attacks

JULY 13, 2021

## Forum

The threat actors behind DragonForce Malaysia created the domain DragonForce.io on June 11, 2021. The forum claims to already have over 10,000 members and 3,000 discussion threads (at the time of publication). This forum has been the central communication hub for the recent operation, #OpsBedil, but also contains discussion about anonymity, hacking, general technology and education.

Over the last few months, the criminal underground has been experiencing difficulties dealing with the brazen ransomware operators and affiliates who openly conduct business on public forums. Administrators of these forums have been banning those who openly engage in ransomware activity out of fear of losing their servers to law enforcement seizures. Because of this, operators and affiliates are now altering their tone while discussing operational details about ransomware on public forums. They are withdrawing from the public eye, self-governing and running their own platforms. In the DFM forum, there are no rules about conducting malicious activity or moderators that ban users and the only threat to losing their platform is de-hosting.

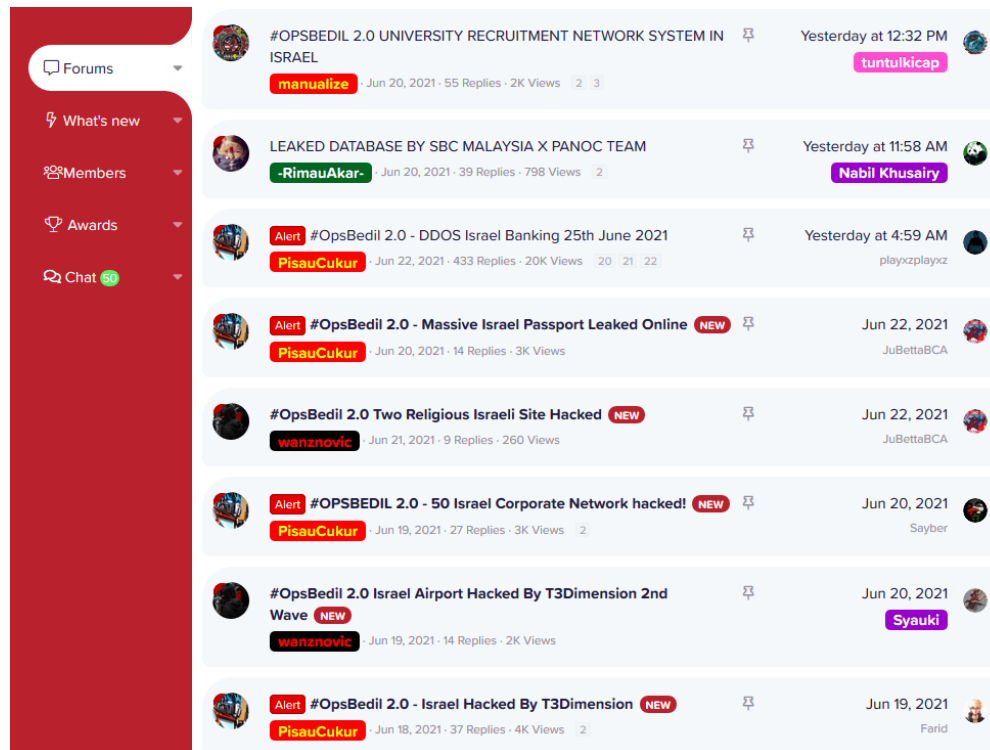


Figure 2: The DragonForce Forum

## Recent Attacks

Hacktivism of DragonForce Malaysia, along with other threat actors in the month of June, targeted a number of organizations in Israel as part of #OpsBedil. The attacks ranged from simple defacement campaigns to data leaks and were documented in detail on DFM's forum and Telegram channel. The content and

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists With New Digital Attacks

JULY 13, 2021



information related to recent attacks conducted by the threat actors on DFM's forum is covered in the sections below.

## UNIVERSITY RECRUITMENT NETWORK SYSTEM

In one of the more publicized [1] events, DFM leaked information on hundreds of thousands of Israeli students. This information included usernames, passwords, names, addresses, phone numbers, dates of birth and other school-related data. The defacement of the AcadeME website [2] references #OpsBedil and "Operation Israel" while calling hackers, activists and human rights organizations to unite and campaign against Israel.

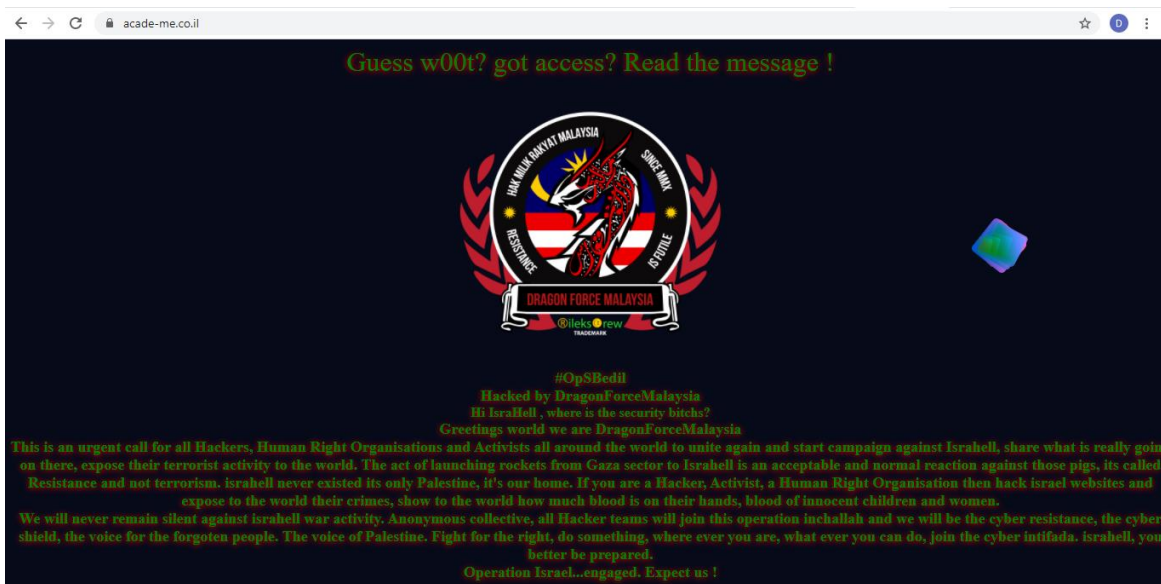


Figure 3: Defaced AcadeME website

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists With New Digital Attacks

JULY 13, 2021



Shared with me > ISRA3L > DB Wanted.co.il

Name ↑	Owner	Last modified
academe_tau_type_user.sql	darkforcemy official	Jun 19, 2021
g_academe_biu_type_user.sql	darkforcemy official	Jun 19, 2021
g_academe_braude_type_user.sql	darkforcemy official	Jun 19, 2021
g_academe_haifa_type_user.sql	darkforcemy official	Jun 19, 2021
g_academe_hit_type_user.sql	darkforcemy official	Jun 19, 2021
g_academe_iem_tec_type_user.sql	darkforcemy official	Jun 19, 2021
g_academe_into_type_user.sql	darkforcemy official	Jun 19, 2021
g_academe_ruppin_type_user.sql	darkforcemy official	Jun 19, 2021

Figure 4: AcadeME leaked data on Google Drive

## LEAKED DATABASE BY SBC MALAYSIA X PANOC TEAM

In this event, forum leader RimauAkar posted [3] several links to pastes containing leaked information, including usernames and passwords, from organizations in both Israel and India. These data leaks are claimed by Syntax Brute Code (SBC) Malaysia and PANOC.

	User	user	Password	password	Usertype	usertype
17.						
18.						
19.						
20.					Admin	Admin
21.					Admin	Admin
22.					Admin	Admin
23.					Admin	Admin
24.					Admin	Admin
25.					Admin	Admin
26.					Admin	Admin
27.					Admin	Admin
28.					Admin	Admin
29.					Admin	Admin
30.					Admin	Admin
31.					Admin	Admin
32.					Admin	Admin

Figure 5: SBC Malaysia x PANOC leaked data

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists  
With New Digital Attacks

JULY 13, 2021

## #OPSBEDIL 2.0 - DDOS ISRAEL BANKING

Another headline-grabbing event [4] was a coordinated DoS attack targeting the financial industry in Israel on June 25, 2021. This event was organized by threat actors in the DFM forum [5] and shared through the Telegram channels. Operational details were spread across several social media outlets, including Facebook [6], using well-designed advertisements listing the targets and their IP addresses. This attack came on the same day the student data from AcadeME was leaked.

The advertisement is a digital poster with a dark, textured background and a yellow border. At the top, a red banner with white text reads "ATTENTION!". Below this is a circular logo featuring a dragon and the Malaysian flag. The main title "#OPSBEDIL 2.0" is in large, bold, yellow letters, with "DDOS ATTACK" in white on a red background below it. The date and time "25<sup>TH</sup> JUNE 2021 | FRIDAY | 9.00PM" are in yellow. A "TARGET LIST:" section follows, with four red buttons containing the following URLs: bankhapoalim.com, www.leumi.co.il, www.mizrahi-tefahot.co.il, and www.fibi.co.il. At the bottom, a red banner with white text reads "MARK THE DATE, WE NEED YOU!".

Figure 6: Advertisement on social media for #OpsBedil 2.0 DDoS attack on Israeli banks [6]

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists With New Digital Attacks

JULY 13, 2021



## #OPSBEDIL 2.0 - MASSIVE ISRAEL PASSPORT LEAKED ONLINE

The administrator for the DFM forum, PisauCukur, posted [7] a MEGA<sup>1</sup> link containing several dozen Israeli passports. This attack was allegedly perpetrated by the T3 Dimension Team [8] in alliance with #OpsBedil and condemned the proposal for Israel to establish relations with Malaysia and neighboring counties.

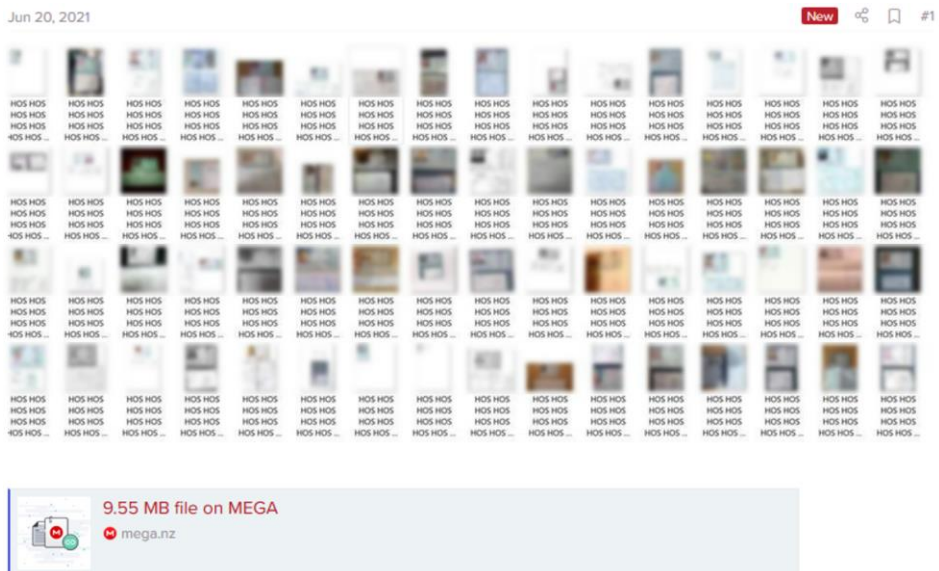


Figure 7: Leaked Israeli passport data on MEGA

## #OPSBEDIL 2.0 - TWO RELIGIOUS ISRAELI SITES HACKED

In another event [9], T3 Dimension Team, in collaboration with DFM, defaced two Israeli religious sites: Limudmeshutaf[.]com and Limoudyakhad[.]com. They claimed the defacement had nothing to do with religion and that their actions were related to #OpsBedil to send a message to Israel.

<sup>1</sup> Secure cloud storage and private communications platform (mega.io)

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists With New Digital Attacks

JULY 13, 2021

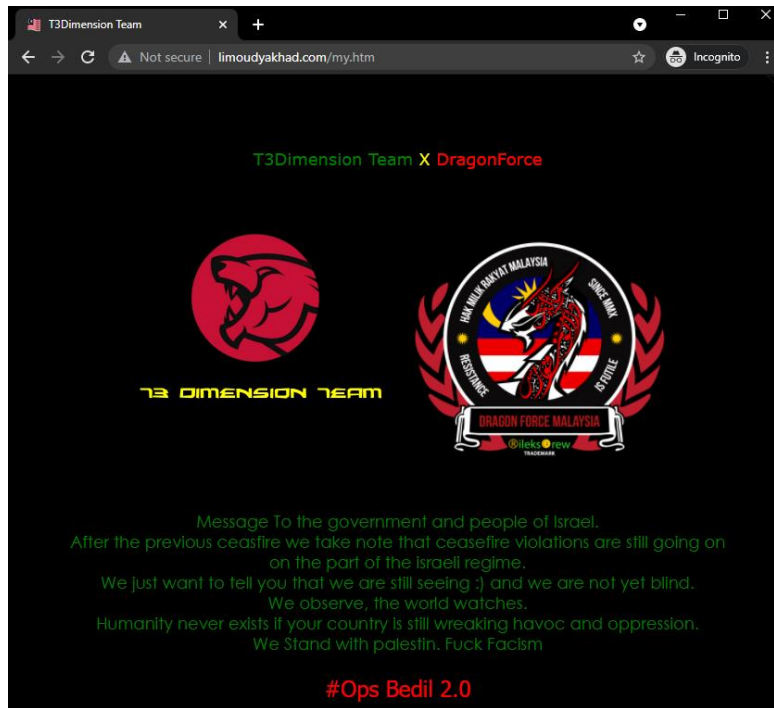


Figure 8: Defaced page of limoudyakhad.com

## #OPSBEDIL 2.0 - 50 ISRAEL CORPORATE NETWORKS HACKED

In yet another post [10] on the DFM forum, PisauCukur shared a link to a file on AnonFiles, an anonymous file sharing service, containing credentials for 50 corporate SSLVPN gateways giving access to the networks of Israeli organizations. This event was related to OpSbedil and claimed by DFM.

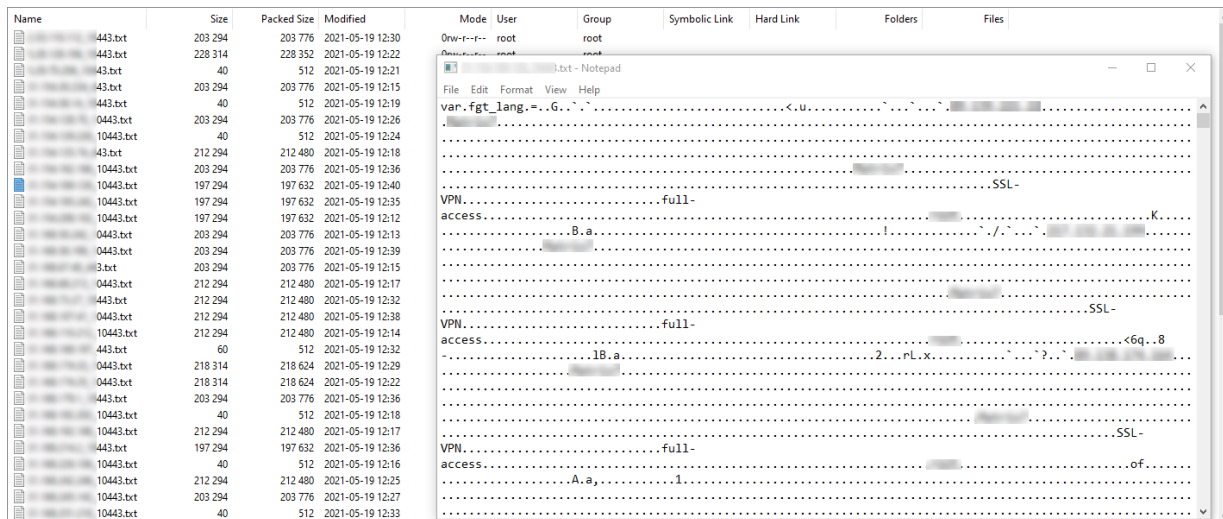


Figure 9: Leaked credentials of 50 corporate SSLVPN gateways owned by Israeli organizations



# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists  
With New Digital Attacks

JULY 13, 2021

## #OPSBEDIL 2.0 - ISRAEL AIRPORT HACKED BY T3DDIMENSION 2ND WAVE

T3 Dimension Team (T3D) and DFM targeted the Ramon Airport and other airline-related organizations in a second attack. The hacktivists claim they are acting in solidarity with their brothers in Palestine. The digital attacks were performed as a reaction to Israeli reports that Ramon Airport had not been bombed by the Palestinian extremist group, Hamas [11].

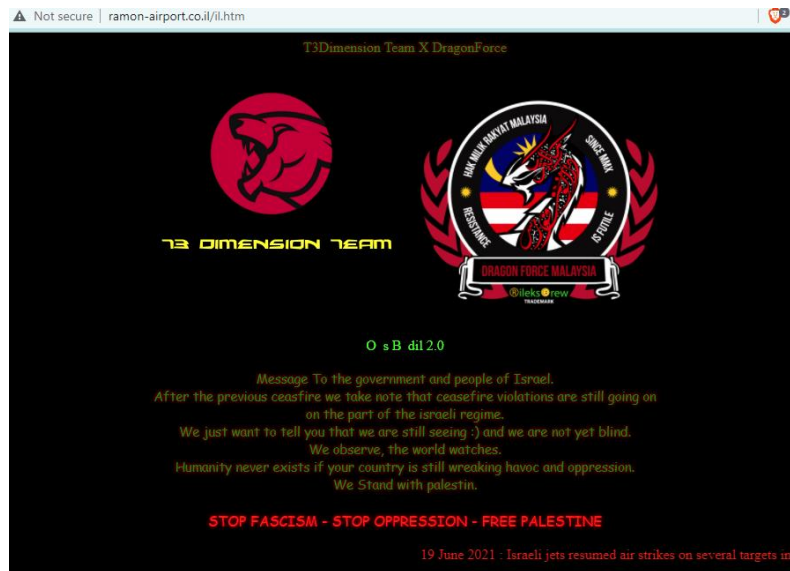


Figure 10: Defaced webpage of Ramon Airport

Websites targeted and allegedly defaced during this attack included ramon-airport[.]co.il, skylink[.]co.il, skytrip[.]co.il, tao[.]org.il, kockonwood[.]co.il and villa-brenner[.]com.

## Attack Methods

Judging by posts from the threat actors in the DFM forum, it appears the group is not very sophisticated. Members are having trouble installing and using basic and widely available tools. It also appears that those with some level of competence use mobile devices or Kali Linux as their primary attack platform. While the organizers seem to lack the skill and ability to conduct sophisticated and largescale DDoS attacks, the DoS tools they suggest still have their place in the DoS threat landscape. While well-known and rudimentary, these tools still are very effective when leveraged against unprotected assets.

### DOS TOOLS

- LOIC
- HOIC
- HULK
- DDoSIM
- PyLoris
- OWASP HTTP Post
- RUDY
- Torshammer
- Davoset
- GoldenEye
- Garuda

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists With New Digital Attacks

JULY 13, 2021



## TORSHAMMER

Torshammer is a slow-rate, Layer 7, HTTP POST DoS tool created by phiral[.]net and similar to the R.U.D.Y. (R-U-Dead-Yet) tool. The first public occurrence of this tool dates back to early 2011. Torshammer executes a DoS attack by using a classic slow POST attack, where HTML POST fields are transmitted in slow rates under the same session. The rates are randomly chosen within the limit of 0.5-3 seconds.

A slow POST attack causes web server's request handling threads to wait for the end of a boundless post before processing the request. This causes exhaustion of web server resources and a denial-of-service state with the inability to process legitimate traffic.

In newer releases of Torshammer, a traffic anonymity feature allows DoS attacks to be carried out through the Tor Network using the native SOCKS proxy integrated in Tor clients. This allows attackers to launch attacks from random source IP addresses making detection of the attack and tracking of the perpetrator almost impossible.

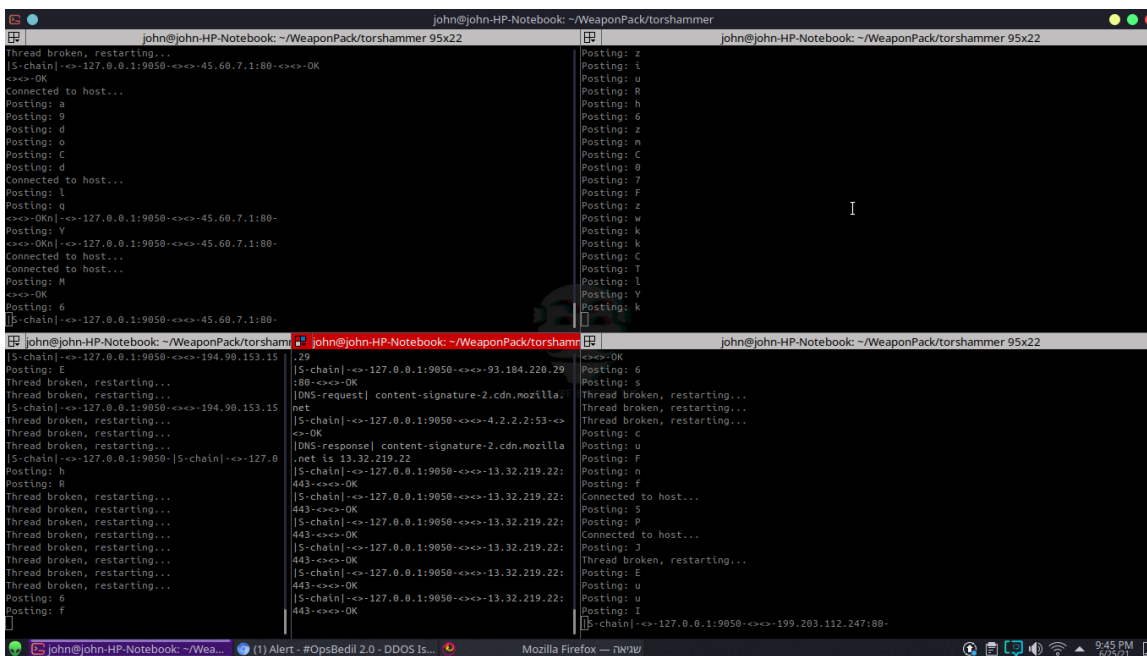


Figure 11: Torshammer in action on a DFM member's notebook during the #OpsBedil 2.0 DDoS operation

## HOIC

The High Orbit Ion Cannon (HOIC) is a network stress tool closely related to the Low Orbit Ion Cannon (LOIC) tool. Both tools were popularized in recent years for launching DDoS attacks by the hacktivist group Anonymous. Unlike its "low-orbiting" cousin, HOIC is able to cause denial-of-service through the use of HTTP floods. HOIC has a built-in scripting system that accepts '.hoic' files called "boosters," allowing the implementation of anti-DDoS counter measures such as randomization and provides the ability to increase the magnitude of the attack.

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists With New Digital Attacks

JULY 13, 2021

While HOIC and LOIC have no significant obfuscation or anonymization capabilities that protect the attacker, the use of '.hoic' booster scripts allows the attacker to specify a list of rotating target URLs, referrers, user-agents and headers in order to make the attack more effective through attacking multiple pages on the same site as well as make it seem like attacks are coming from different users.

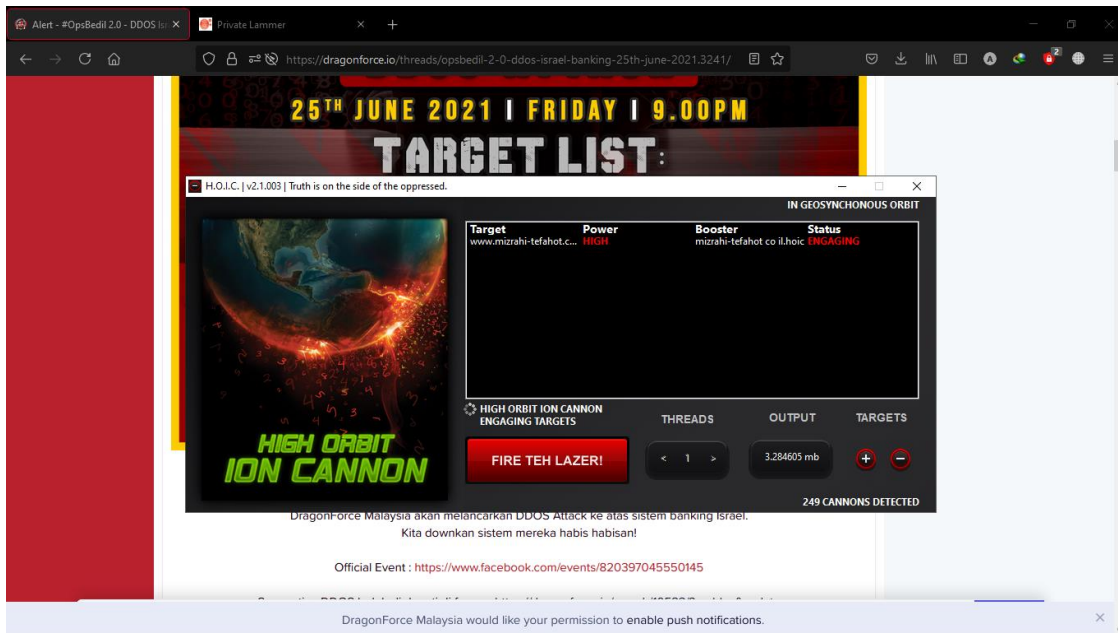


Figure 12: Screenshot of a member of DFM performing HOIC attacks relating to the #OpsBedil 2.0 DDoS operation

## MOBILE DOS TOOLS

Throughout the DFM forum there are images of threat actors using mobile devices to conduct DoS attacks. One user in the forum suggested that other members download an Android APK<sup>2</sup> and install Garuda, a mobile DoS tool, to use during the attacks.

<sup>2</sup> An Android Package Kit (APK for short) is the package file format used by the Android operating system for distribution and installation of mobile apps.

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists With New Digital Attacks

JULY 13, 2021



The screenshot shows a forum profile for a user named **-RimauAkar-**, who is a **Technology Leader** and **Forum Leader**. The profile includes a circular profile picture, a **DFM** logo, a **LEADER** badge, and a **LEADER** badge. The user's statistics are: **Joined: May 29, 2021**, **Messages: 452**, and **Reaction score: 741**.

The post, dated **Jun 7, 2021**, contains the following text:

Cara senang ddos hanya guna apk  
Tak payah sakit kepala 😊

Senang nanti klau nk join ddos ramai2  
Kata nk serang israhell kan

Download file kat sini

Three file download links are provided, each for **Garuda DDOS BETA . apk** (1.97 MB):

- Download Garuda DDOS BETA .apk diupload Nailon pada 14 May 2019 di folder APK 1.97 MB. [sfile.mobi](#)
- Download Garuda DDOS BETA .apk diupload Nailon pada 14 May 2019 di folder APK 1.97 MB. [sfile.mobi](#)
- Download Garuda DDOS BETA .apk diupload Nailon pada 14 May 2019 di folder APK 1.97 MB. [sfile.mobi](#)

Figure 13: DFM Forum user suggesting other members to use Garuda

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists With New Digital Attacks

JULY 13, 2021

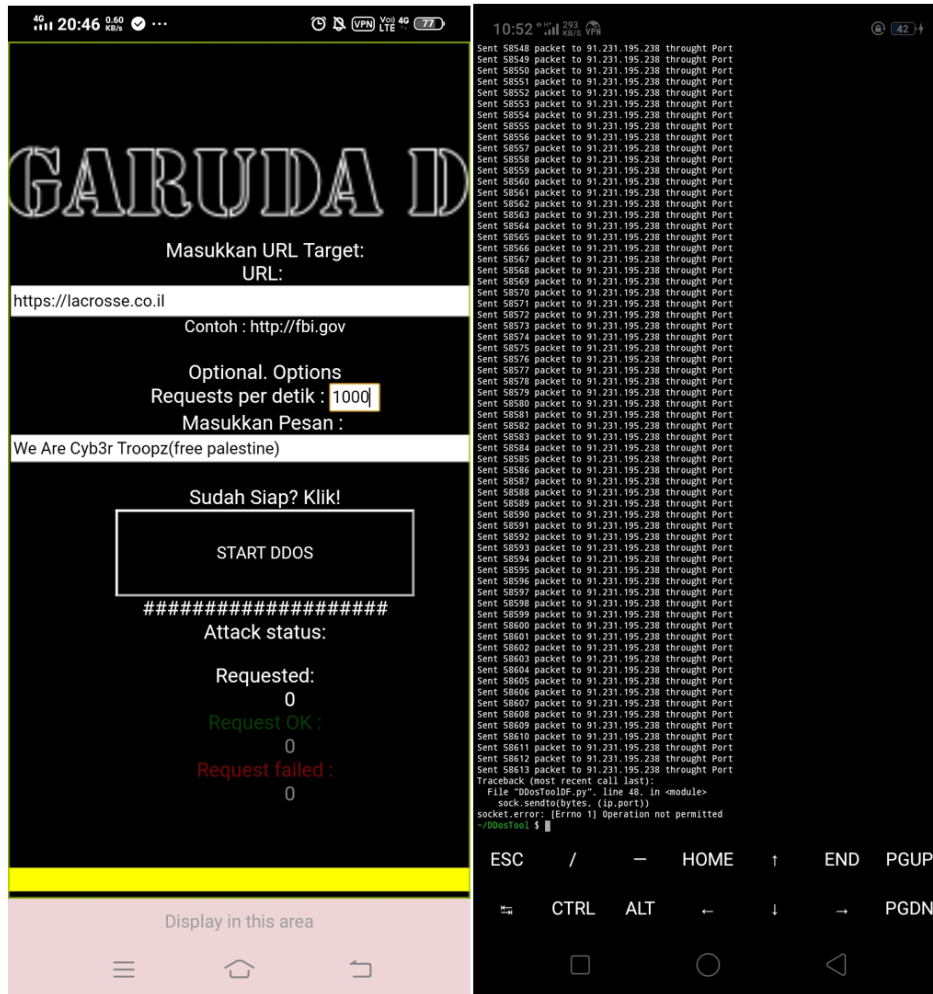


Figure 14: Garuda used by a member of DFM during the #OpsBedil 2.0 DDoS attacks

## Operation Details

### TARGETED VERTICALS

- Religion
- Financial
- Transportation
- Education

### HASHTAGS

- #OpsBedil
- #OpIsrael
- #FreePalestine
- #GroupTempurSiberMalaysia
- #HakMilikRakyatMalaysia
- #DragonForceMalaysia

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists  
With New Digital Attacks

JULY 13, 2021



- #GateKeeper
- #AlamSebalikMata
- #IsraelKoyak

## OFFICIAL DRAGONFORCE MALAYSIA ACCOUNTS

- Facebook: <https://fb.me/Dragonforce.io>
- Telegram: <https://t.me/dragonforceio>
- Twitter: <https://twitter.com/dragonforceio>
- Instagram: <https://instagram.com/dragonforceio> (Down)
- Forum: <https://dragonforce.io>

## T3DIMENSION ACCOUNTS

- Facebook: <https://www.facebook.com/T3DimensionTeam>
- Telegram: <https://t.me/T3DimensionTeam>

## UNOFFICIAL DRAGONFORCE MALAYSIA ACCOUNTS

dragonforce.my is not under the umbrella of dragonforce.io

- Facebook: <https://facebook.com/dragonforce.my>
- Telegram: <https://t.me/dragonforcemy>
- Forum: <https://dragonforce.my>

## OPSBEDIL ACCOUNTS

- Twitter: <https://twitter.com/opsbedil>

## References

- [1] S. Winer, "Pro-Palestinian hackers steal info on hundreds of thousands of Israeli students," 27 June 2021. [Online]. Available: <https://www.timesofisrael.com/pro-palestinian-hackers-steal-info-on-hundreds-of-thousands-of-israeli-students/>.
- [2] manualize, "#OPSBEDIL 2.0 UNIVERSITY RECRUITMENT NETWORK SYSTEM IN ISRAEL," DFM Forum, 20 June 2021. [Online]. Available: <https://dragonforce.io/threads/opsbedil-2-0-university-recruitment-network-system-in-israel.3127/>. [Accessed 6 July 2021].
- [3] RimauAkar, "LEAKED DATABASE BY SBC MALAYSIA X PANOC TEAM," DFM Forum, 20 June 2021. [Online]. Available: <https://dragonforce.io/threads/leaked-database-by-sbc-malaysia-x-panoc-team.3158/>. [Accessed 6 July 2021].
- [4] T. Shahaf, "אתרי הבנקים הותקפו בסוף השבוע," ynet, 27 June 21. [Online]. Available: <https://www.ynet.co.il/digital/technews/article/rkBWvx82u>.
- [5] PisauCukur, "#OpsBedil 2.0 - DDOS Israel Banking 25th June 2021," DFM Forum, 22 June 2021. [Online]. Available: <https://dragonforce.io/threads/opsbedil-2-0-ddos-israel-banking-25th-june-2021.3241/>. [Accessed 6 July 2021].
- [6] DragonForce Malaysia, "#OPSBEDIL 2.0 DDOS ATTACK," Facebook, 22 June 2021. [Online]. Available: <https://www.facebook.com/events/820397045550145>.

# DragonForce Malaysia – #OpsBedil






Renewed Hacktivism in the Middle East Persists  
With New Digital Attacks

JULY 13, 2021





- [7] PisauCukur, "#OpsBedil 2.0 - Massive Israel Passport Leaked Online," DFM Forum, 20 June 2021. [Online]. Available: <https://dragonforce.io/threads/opsbedil-2-0-massive-israel-passport-leaked-online.3163/>. [Accessed 6 July 2021].
- [8] T3 Dimension, "Facebook page," [Online]. Available: <https://www.facebook.com/T3DimensionTeam/>. [Accessed 9 July 2021].
- [9] wanznovic, "#OpsBedil 2.0 Two Religious Israeli Site Hacked," DFM Forum, 21 June 2021. [Online]. Available: <https://dragonforce.io/threads/opsbedil-2-0-two-religious-israeli-site-hacked.3198/>. [Accessed 6 July 2021].
- [10] PisauCukur, "#OPSBEDIL 2.0 - 50 Israel Corporate Network hacked!," DFM Forum, 20 June 2021. [Online]. Available: <https://dragonforce.io/threads/opsbedil-2-0-50-israel-corporate-network-hacked.3120/>. [Accessed 6 July 2021].
- [11] Reuters, Jerusalem, "Israel denies Hamas targeted Ramon Airport with rocket," Alarabiya News, 13 May 2021. [Online]. Available: <https://english.alarabiya.net/News/middle-east/2021/05/13/Israel-denies-Hamas-targeted-Ramon-Airport-with-rocket->.

## EFFECTIVE DDoS PROTECTION ESSENTIALS

-  **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
-  **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
-  **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
-  **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
-  **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed data for preemptive protection against currently active known attackers.

For further [network and application protection](#) measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

## EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

-  **Full OWASP Top-10** coverage against defacements, injections, etc.
-  **Low false positive rate** using negative and positive security models for maximum accuracy

# DragonForce Malaysia – #OpsBedil

Renewed Hacktivism in the Middle East Persists With New Digital Attacks

JULY 13, 2021



effort

**Auto-policy generation** capabilities for the widest coverage with the lowest operational



**Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking



**Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources



**Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

## LEARN MORE AT THE SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit [Radware's Security Research Center](#). It is the ultimate resource for everything security professionals need to know about DDoS attacks and cybersecurity.

## ABOUT RADWARE

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit [www.radware.com](http://www.radware.com).

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our Security Research Center that provides a comprehensive analysis of DDoS attack tools, trends and threats. This document is provided for information purposes only.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.

© 2021 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this report are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see <https://www.radware.com/LegalNotice/>. All other trademarks and names are the property of their respective owners.