

# Radware Threat Advisory

## OpsBedil Reloaded 2022 by DragonForce Malaysia

April 19, 2022

Last year's renewed hacktivist operations throughout the Middle East have returned, presenting a certain level of risk for unprotected assets as threat actors begin to target organizations and citizens across Israel.



Figure 1: OpsBedil reloaded 2022 campaign flyer

## OpsBedil

OpsBedil is a relatively new campaign targeting Israel. It first appeared in 2021 and has since seen four official operations under its battle tag. The operations are mainly reactionary and following physical or political confrontations. Operations tend to have a more substantial presence in the months April to July.

OpsBedil is replacing the now-defunct Anonymous operations known as OplIsrael. The new operations are conducted by DragonForce Malaysia and its affiliates throughout Southeast Asia, specifically Malaysia and Indonesia. The current operation, OpsBedilReloaded, is a political response to events that occurred in Israel on April 11, 2022.

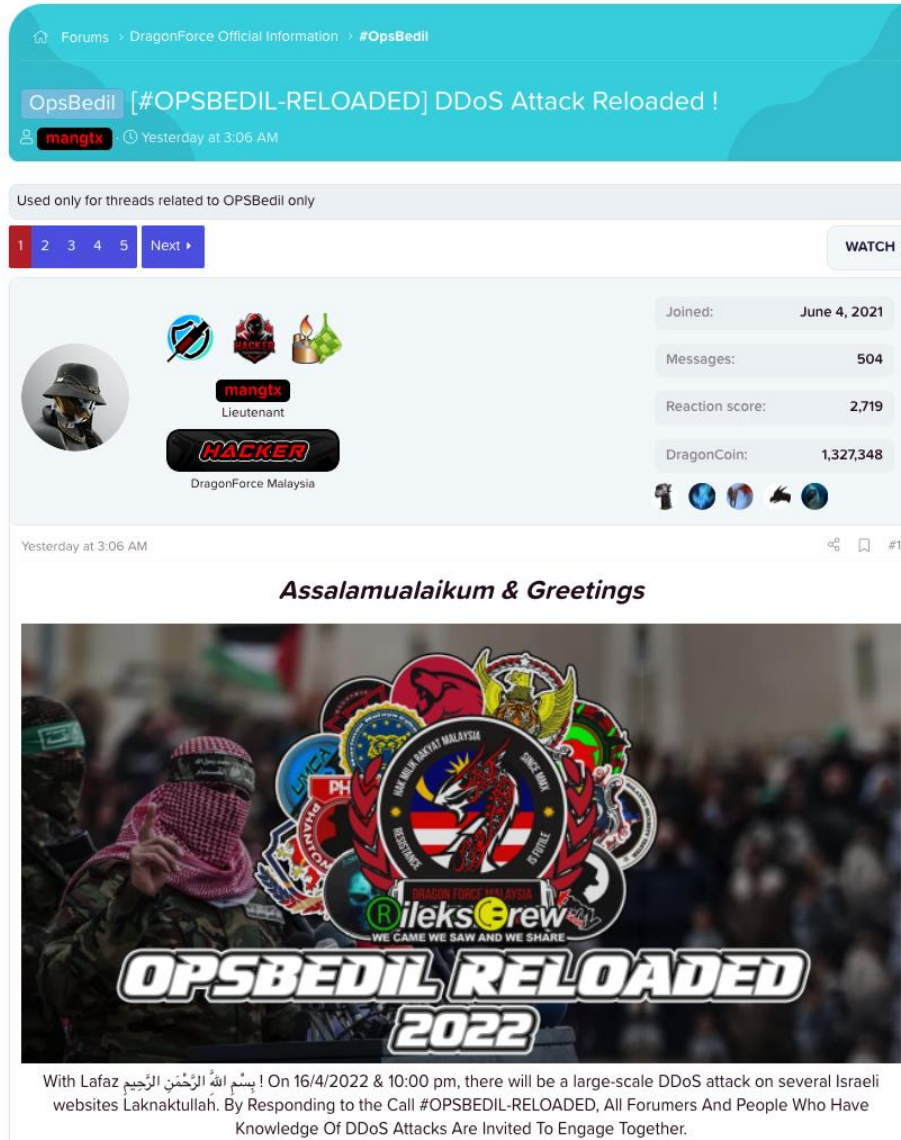
## DragonForce Malaysia

The driving force behind #OpsBedilReloaded is DragonForce Malaysia, a pro-Palestinian hacktivist group located in Malaysia. DragonForce Malaysia has also been observed working with several other hacktivist groups, including the T3 Dimension Team and RileksCrews. DragonForce Malaysia has a website and a forum where threat actors conduct most of their announcements and discussions. The group also has a Telegram channel, but most content is replicated throughout the forum and other social media platforms.

# Radware Threat Advisory

## OpsBedil Reloaded 2022 by DragonForce Malaysia

April 19, 2022



The screenshot shows a forum post on the DragonForce Official Information forum. The post is titled "OpsBedil Reloaded 2022" and is by user "mangtx", a Lieutenant in DragonForce Malaysia. The post content includes the greeting "Assalamualaikum & Greetings" and a large graphic for "OPSBEDIL RELOADED 2022". The graphic features the DragonForce Malaysia logo, the RileksGrew logo with the slogan "WE CAME WE SAW AND WE SHARE", and the text "DRAGON FORCE MALAYSIA". Below the graphic, the post text reads: "With Lafaz بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ ! On 16/4/2022 & 10:00 pm, there will be a large-scale DDoS attack on several Israeli websites Laknaktullah. By Responding to the Call #OPSBEDIL-RELOADED, All Forumers And People Who Have Knowledge Of DDoS Attacks Are Invited To Engage Together."

Figure 2: OpsBedil Reloaded 2022 forum post

The threat actors behind DragonForce Malaysia created the domain DragonForce.io in 2021 during their [original campaign](#). The forum today has grown to 13,000 members and 11,000 discussion threads. Since its creation, this forum has been the central communication hub for the group. Discussions in the forum include OpsBedil, but also threads about anonymity, hacking, general technology and education.

# Radware Threat Advisory

## OpsBedil Reloaded 2022 by DragonForce Malaysia

April 19, 2022



### Recent Attacks

The hackers of DragonForce Malaysia, along with other threat actors, began targeting several organizations in Israel with defacements, denial-of-service attacks and data leaks on April 11, 2022 as part of the OpsBedilReloaded campaign. Recent OpsBedilReloaded attacks are illustrated below, but the operation is still ongoing at the time of publication.

#### DEFAACEMENT

Radware has observed and confirmed several defacements by DragonForce Malaysia and members of T3 Dimension Team since the start of OpsBedilReloaded on April 11. The defacements cite the escalating tension in the Middle East during Ramadan as their justification for cyberattacks and call hackers and activists to unite and campaign against Israel. The defacements in the current campaign are very similar to the campaign of last year, only updated with new content.

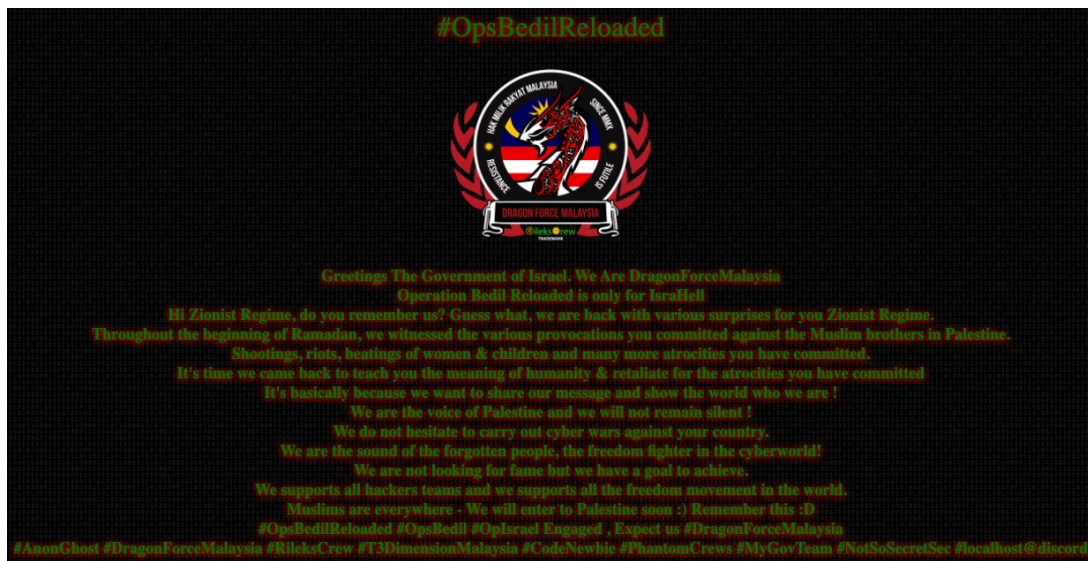


Figure 3: OpsBedil Reloaded defacement message

#### SCANNING & EXPLOITING

Since the beginning of the operation, Radware has seen and confirmed several scanning and exploitation attempts by members of DragonForce Malaysia. Threat actors have been exchanging information about

# Radware Threat Advisory

## OpsBedil Reloaded 2022 by DragonForce Malaysia

April 19, 2022



compromised and leaked sensitive information through a Google Dork<sup>1</sup> query 'inurl:objDoc.asp?PID הרשמה'. Forum post to members joining the OpsBedilReloaded campaign provide several tools from scanner used to discover vulnerable servers that can be exploited for defacement to scripts for performing denial-of-service attacks.

```
C:\Windows\System32\cmd.exe
DRAGONFORCE.IO

Priv0 POC Israhell Made By Manualize and Eagle Eye
Func reverse ip lookup scan exploitable server
https://dragonforce.io
Telegram: dragonforceio
Get Started With (pip install -r requirements.txt)

error while connecting site -> amonrama.co.il
error while connecting site -> amonrama.com
successfully uploaded -> http://bzb.co.uk/
error while connecting site -> bzbbooks.com
error while connecting site -> bzcftp.com
not vulnerable -> bitoprint.net (Maybe vuln from authentication)
not vulnerable -> by-print.co.il (Maybe vuln from authentication)
not vulnerable -> canmedico.il (Maybe vuln from authentication)
successfully uploaded! -> http://www.clickprint.co.il/
error while connecting site -> coffee-print.co.il
successfully uploaded -> http://www.coffee-print.co.il/
error while connecting site -> coronaprint.co.il
successfully uploaded -> http://www.digital.co.il/
error while connecting site -> dfosewer.co.il
not vulnerable -> dilon.co.il (Maybe vuln from authentication)
not vulnerable -> dlovcic.co.il (Maybe vuln from authentication)
error while connecting site -> docuprint.co.il
not vulnerable -> flash-lcd.co.il (Maybe vuln from authentication)
error while connecting site -> ftp.org.il
error while connecting site -> galdigital.co.il
error while connecting site -> galdigital-ftp.org.il
error while connecting site -> grafi.co.il
successfully uploaded! -> http://www.grafiprint.co.il/
not vulnerable -> graphicprint.co.il (Maybe vuln from authentication)
not vulnerable -> graphoprint.co.il (Maybe vuln from authentication)
successfully uploaded -> http://www.hadwin.co.il
error while connecting site -> hisigraf.co.il
not vulnerable -> imagine-ep.co.il (Maybe vuln from authentication)
not vulnerable -> infooptouch.co.il (Maybe vuln from authentication)
error while connecting site -> kolprint.co.il
not vulnerable -> lemox.com (Maybe vuln from authentication)
not vulnerable -> mail.unigrafi.com (Maybe vuln from authentication)
not vulnerable -> mail.bzcprint.co.il (Maybe vuln from authentication)
not vulnerable -> mail.bzcprint.com (Maybe vuln from authentication)
```

Figure 4: DragonForce.io tool to scan for vulnerable servers

### DATA LEAKS

As with most hacktivist-related operations, DragonForce Malaysia has claimed several data leaks since the beginning of the campaign. Data leaks are often difficult to validate and their origins verified. However, lists of emails and phone numbers are easy to come by and can be leveraged for phishing and spam campaigns. In the past, hacktivist campaigns targeting Israel have leveraged this kind of data dumps to send unwanted and antisemitic messages to Israelis.

<sup>1</sup> A Google dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find information that is not readily available on a website. Google dorking, also known as Google hacking, can return information that is difficult to locate through simple search queries. That description includes information that is not intended for public viewing but that has not been adequately protected. ([TechTarget](#))

# Radware Threat Advisory

## OpsBedil Reloaded 2022 by DragonForce Malaysia

April 19, 2022



select type_credits_trans__temp	<input type="checkbox"/> edit	NULL
select type_document	<input type="checkbox"/> edit	NULL
select type_document__paragraphs	<input type="checkbox"/> edit	NULL
select type_element	<input type="checkbox"/> edit	NULL
select type_exam	<input type="checkbox"/> edit	NULL
select type_exam__answers_multip	<input type="checkbox"/> edit	NULL
select type_exam__pages	<input type="checkbox"/> edit	NULL
select type_exam__participants	<input type="checkbox"/> edit	NULL
select type_exam__participants_an	<input type="checkbox"/> edit	NULL
select type_exam__questions	<input type="checkbox"/> edit	NULL
select type_group	<input type="checkbox"/> edit	NULL
select type_group__associated_doc	<input type="checkbox"/> edit	NULL
select type_group__paragraphs	<input type="checkbox"/> edit	NULL
select type_license	<input type="checkbox"/> edit	NULL
select type_license__images	<input type="checkbox"/> edit	NULL
select type_license__links	<input type="checkbox"/> edit	NULL
select type_license__user_variables	<input type="checkbox"/> edit	NULL
select type_license__variables	<input type="checkbox"/> edit	NULL
select type_memberzone	<input type="checkbox"/> edit	NULL
select type_memberzone__products	<input type="checkbox"/> edit	NULL
select type_memberzone__users	<input type="checkbox"/> edit	NULL
select type_newsletter	<input type="checkbox"/> edit	NULL
select type_newsletter__links	<input type="checkbox"/> edit	NULL
select type_newsletter__links_recip	<input type="checkbox"/> edit	NULL
select type_newsletter__recipients	<input type="checkbox"/> edit	NULL
select type_object	<input type="checkbox"/> edit	NULL
select type_order	<input type="checkbox"/> edit	NULL
select type_order__products	<input type="checkbox"/> edit	NULL
select type_order__products_attri	<input type="checkbox"/> edit	NULL
select type_order__sub_carts	<input type="checkbox"/> edit	NULL
select type_order__temp	<input type="checkbox"/> edit	NULL
select type_poll	<input type="checkbox"/> edit	NULL

Figure 5: Claimed data leak (DragonForce.io forum)

### DDOS ATTACKS

This year again, DragonForce Malaysia is using well-designed advertisements that lists target information to entice followers to join in the operation. The events are announced in the DragonForce Malaysia forum and shared through social platforms. Denial-of-service campaigns were typically announced less than 24 hours in advance and started on April 16, 2022. In addition to the official attacks, several unannounced denial-of-service attacks were launched under the battle tag OpsBedilReloaded between April 11 and April 16, 2022.



Figure 6: Attack flyer 1



Figure 7: Attack flyer 2

# Radware Threat Advisory

OpsBedil Reloaded 2022  
by DragonForce Malaysia

April 19, 2022



Figure 8: Attack flyer 3

## DDoS Attack Methods

DragonForce Malaysia is not considered an advanced or a persistent group, nor are they sophisticated. But where they lack sophistication, they make up for it with their organizational skills and ability to quickly disseminate information.

This year, followers do not appear to have trouble installing attack tools provided through the forum. The tools, however, are still based on widely available and basic attack scripts. Threat actors with basic levels of competence appear to be using mobile devices and virtual machines loaded with Kali or Parrot Linux as their primary attack platform. While the organizers still seem to lack the skills or ability to conduct largescale distributed denial-of-service attacks, the simple denial-of-service tools they are leveraging are effective against unprotected assets and still have a place in the 2022 threat landscape.



Figure 9: DDoS attack advertisement in DragonForce.io forum

## SLOW LORIS

**Slowloris** is a denial-of-service tool developed by the grey hat hacker "RSnake." The tool causes a denial-of-service by using a very slow HTTP request. By sending HTTP headers to the target site in tiny chunks, as slowly as possible, waiting to send the next chunk until just before the server would time out the request, the server is forced to wait for headers to arrive. If enough slow connections are opened to the server, resources will become constrained and the server will be unable to handle new legitimate requests.



# Radware Threat Advisory

## OpsBedil Reloaded 2022 by DragonForce Malaysia

April 19, 2022

### DDOS-RIPPER

Another tool seen heavily leveraged by DragonForce Malaysia is DDoS-Ripper by [Palahsu](#). DDoS Ripper is an obfuscated Python script designed to perform direct and indirect path application-level attacks on web servers.

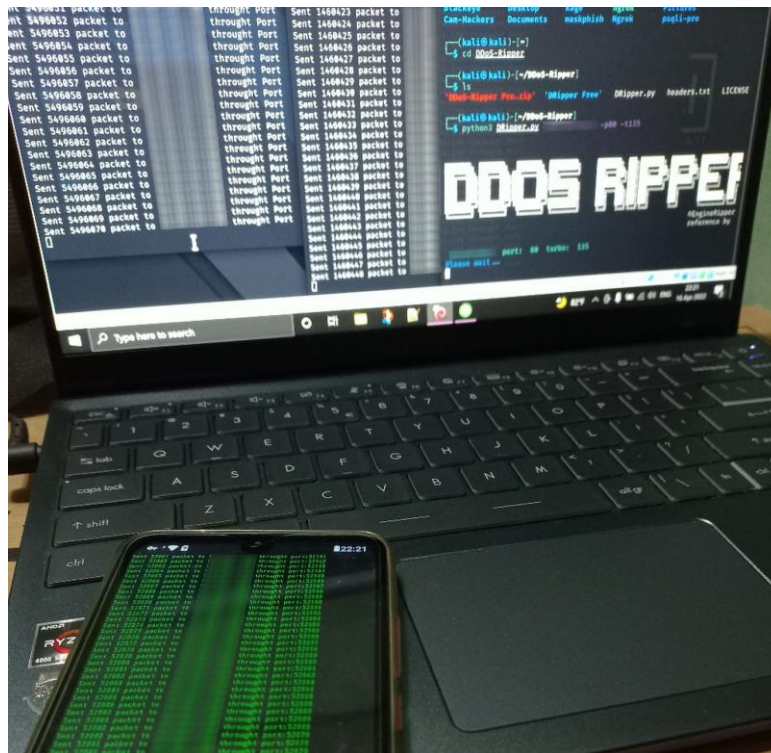


Figure 12: Picture of DDoS-Ripper used by a member of the DragonForce Malaysia social army

The script is designed to run two simultaneous attack vectors, each consisting of 135 independent threads that will load the target server with HTTP requests.

The first attack vector is a direct path HTTP GET request to the target IP leveraging a random user-agent header chosen from a predefined list and a static set of headers imported from a text file named 'headers.txt'.

```
uagent.append("Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0) Opera 12.14")
uagent.append("Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:26.0) Gecko/20100101 Firefox/26.0")
uagent.append("Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913 Firefox/3.5.3")
uagent.append("Mozilla/5.0 (Windows; U; Windows NT 6.1; en; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)")
uagent.append("Mozilla/5.0 (Windows NT 6.2) AppleWebKit/535.7 (KHTML, like Gecko) Comodo_Dragon/16.1.1.0 Chrome/16.0.912.63 Safari/535.7")
uagent.append("Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)")
uagent.append("Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1")
uagent.append("Mozilla / 5.0(X11;Linux i686; rv:81.0) Gecko / 20100101 Firefox / 81.0")
uagent.append("Mozilla / 5.0(Linuxx86_64;rv:81.0) Gecko / 20100101Firefox / 81.0")
uagent.append("Mozilla / 5.0(X11;Ubuntu;Linux i686;rv:81.0) Gecko / 20100101Firefox / 81.0")
uagent.append("Mozilla / 5.0(X11;Ubuntu;Linuxx86_64;rv:81.0) Gecko / 20100101Firefox / 81.0")
uagent.append("Mozilla / 5.0(X11;Fedora;Linuxx86_64;rv:81.0) Gecko / 20100101Firefox / 81.0")
```

Figure 13: Predefined list of user-agent headers leveraged by DDoS-Ripper



# Radware Threat Advisory

## OpsBedil Reloaded 2022 by DragonForce Malaysia

April 19, 2022

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
```

Figure 14: HTTP request headers used by DDoS-Ripper (as defined in headers.txt)

The second attack vector is an indirect path attack that leverages the Facebook crawler and w3.org markup validation web services as bots to generate load on the target server. The 135 threads of the second attack vector results in requests randomly chosen between the following two predefined URI:

`https://validator.w3.org/check?uri=<target server>` [1]

`https://www.facebook.com/sharer/sharer.php?u=<target server>` [2]

The w3.org markup validation website queried by URI [1] will create a new web request originating from w3.org to the target server to validate the markup of the target URI. The Facebook sharer URI [2] initiates a new feed or story and will result in the Facebook crawler to request the Open Graph tags from the target website and inspect metadata for the website, including description and a potential image defined by the target's meta properties.



Figure 15: Example Facebook sharer request for 'radware.com'



# Radware Threat Advisory

## OpsBedil Reloaded 2022 by DragonForce Malaysia

April 19, 2022

### OTHER ATTACK SCRIPTS

The threat actors behind DragonForce Malaysia may not be sophisticated bot herders, but they seem to have a stockpile of simple denial-of-service attack scripts to choose from. For example, the group has been seen leveraging [IkzCx's collection](#) of attack scripts. Some of the more popular scripts include SadAttack, Saphyra and m60. All aforementioned scripts perform direct path HTTP requests to a target server leveraging random user agents and referers, and randomly generated query parameters to invalidate potential CDN caching by the target. SadAttack, Saphyra and m60 are almost identical Python scripts, the main difference between them are the predefined lists of user agents and referers, of which Saphyra has the most extensive ones.

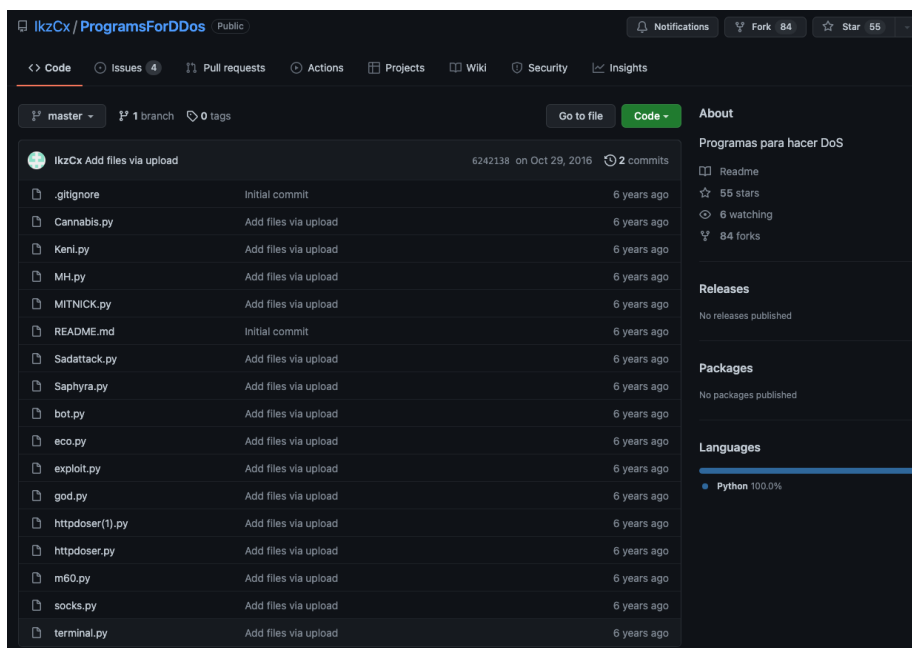


Figure 17: Collection of publicly available attack scripts on Github

## Operation Details

### TARGETED VERTICALS

- Religion
- Financial
- Transportation
- Education
- Government
- Small and Medium Enterprises

### THREAT GROUPS

- DragonForce Malaysia
- RileksCrew
- T3 Dimension Team

# Radware Threat Advisory

## OpsBedil Reloaded 2022 by DragonForce Malaysia

April 19, 2022

### HASHTAGS

- #OpsBedil
- #OpsBedilReloaded
- #OpsIsrael
- #Opsrahell
- #AIAqsa
- #AIAqsaUnderAttack
- #GazaUnderAttack
- #FreePalesine

### TIKTOK PRESENCE

As the threat landscape evolves, hackers have migrated away from Twitter and Facebook. They have begun moving to TikTok and Telegram as alternative platforms to post and share information related to their operations. Komando16\_, a member of DragonForce Malaysia, has been active on TikTok during OpsBedilReloaded, posting videos about the campaign and attacks they are conducting. In several of Komando16\_'s videos, you can see the threat actors' battle station and a denial-of-service script called Saphyra.

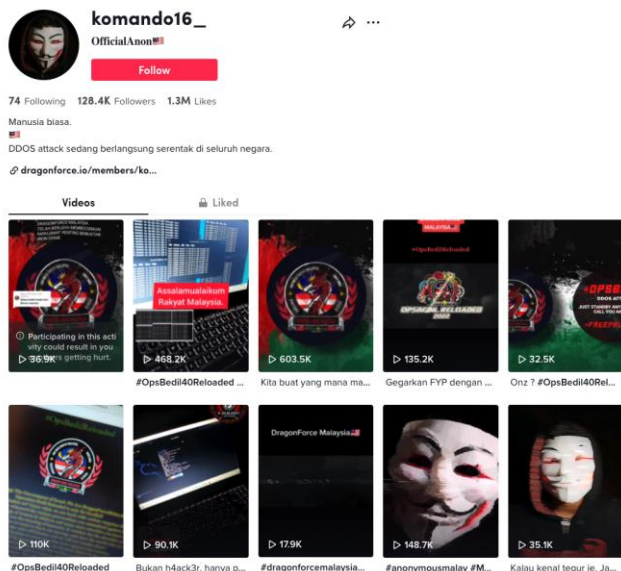


Figure 18: Komando16\_'s TikTok account

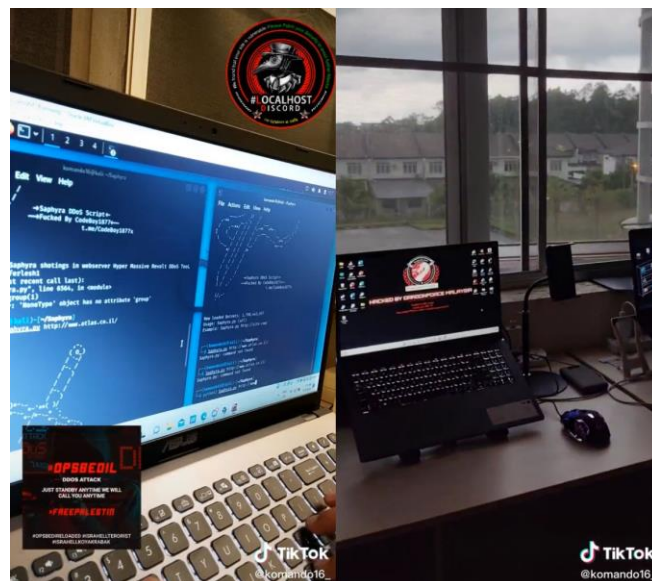


Figure 19: Komando16\_ TikTok posts

### OTHER MEDIA PLATFORMS

- dragonforce.io
- facebook.com/dragonforce.io
- t.me/dragonforce.io
- twitter.com/dragonforceio
- instagram.com/dragonforceio

# Radware Threat Advisory

## OpsBedil Reloaded 2022 by DragonForce Malaysia

April 19, 2022



## Reason For Concern

### SHIFTING LANDSCAPE

Oplsrail, as well as Anonymous, over the years, has dissolved into a benign threat. Today the moniker has transformed from a yearly operation on Holocaust Remembrance Day into a battle tag leveraged by opportunist hackers in response to escalating violence in the Middle East.

This transition is mainly due to the escalation of hybrid warfare in the region, Israel successfully discouraging cyber aggression, and a shift from hacker to organized and nation-state related groups. As a result of this escalation in hybrid warfare, hackers typically no longer target Israel in mass.

### RENEWED THREAT

Hacker campaigns like OpsBedil, while nowhere close to as notorious as Oplsrail once was, present a renewed level of risk for the region. Unlike Anonymous, which has very little remaining bandwidth to target Israel, DragonForce Malaysia and its affiliates have the time, resources and motivation to present a new moderate level of risk for the country of Israel.

It is expected that DragonForce Malaysia will be most active between Al Quds day and Jerusalem day, with extended operations lasting thru July. Attacks will include scanning and exploiting, data dumps, denial-of-service attacks, and website defacements. Attacks may also include unwanted emails containing malicious files or antisemitic SMS/WhatsApp messages directed at Israeli citizens. Those who directly or indirectly support the country of Israel could become a target of DragonForce Malaysia during this period.

### 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.

# Radware Threat Advisory

OpsBedil Reloaded 2022  
by DragonForce Malaysia

April 19, 2022



For further [network and application protection](#) measures, Radware urges companies to inspect and patch their network 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
- /// **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- /// **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 DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit [DDoSWarriors.com](https://DDoSWarriors.com). Created by Radware's [Emergency Response Team \(ERT\)](#), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.