Radware Cybersecurity Advisory
DragonForce Malaysia: OpsPetir

April 12, 2023

DragonForce Malaysia, a pro-Palestinian hacktivist group located in Malaysia, returns for a third year with rebranded operations targeting Israel.

Figure 1: DragonForce Malaysia OpsPetir

OpsPetir

This year, DragonForce Malaysia returns for the third year in a row with operations targeting Israel. OpsPetir, an official replacement for OpsBedil, is a rebranded campaign from DragonForce Malaysia. The operation, announced on the morning of April 11th, is scheduled to begin on the evening of April 12th.

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 11th, the threat group posted a press release to their forum calling for all Muslim cyber warriors, human rights activists, journalists, and Malaysians alike to join their operation targeting Israel. OpsPetir will officially begin on April 12th at 9.30 pm (MYT), 2.30pm Israel time, and is projected to last until April 20th.

DragonForce Malaysia

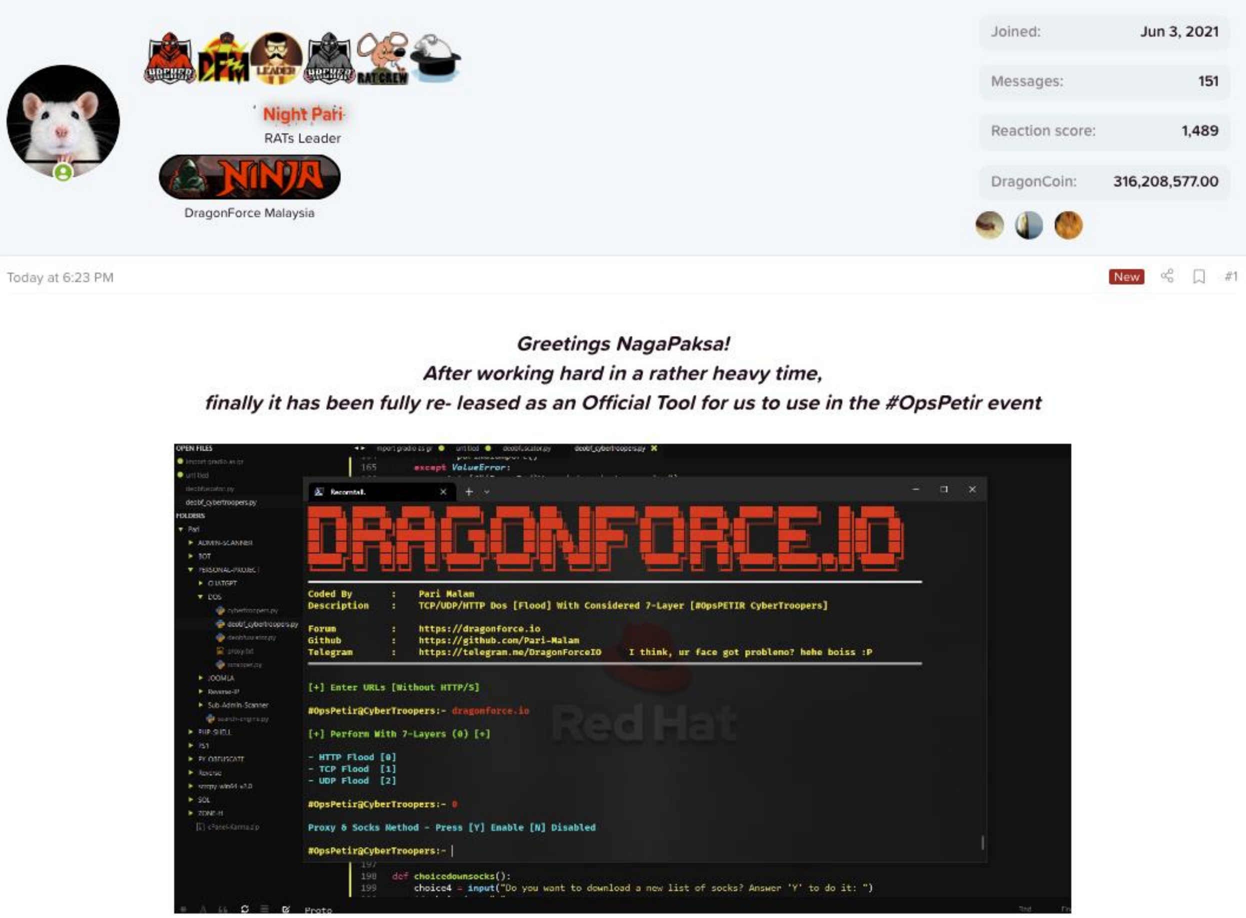
The driving force behind OpsPetir is DragonForce Malaysia, a pro-Palestinian hacktivist group in Malaysia. The group has been observed working with several threat groups over the years, including the T3 dimension Team, Reliks Crew, and AnonGhost. In addition, DragonForce Malaysia has an active forum where threat actors post campaign announcements and discuss varying tactics, techniques, and procedures. The group also has a Telegram channel, but most of their content is replicated throughout the forum and other social media platforms, including Discord, this year. 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.

Attack Method

DragonForce Malaysia is not considered an advanced or persistent group. Where they lack sophistication, they make up for it with their organizational skills and ability to quickly disseminate information. After years of growth, their forum contains dozens of tutorials and guides on how to install tools and launch various attacks. The group also uses well-designed advertisements that list target information to entice followers to join the operations. It is typical for the group to announce a campaign less than 24 hours in advance.

CYBERTROOPERS

User Pari Malam, aka Night Pari, has released a denial-of-service tool called CyberTroopers for OpsPetir. The obfuscated Python program 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 randomize the origin of the attacks and increase the complexity of detection and mitigation for L7 application attacks. Cyber Troopers will be used by dozens of members of DragonForce Malaysia on April 12th to target multiple government institutions and organizations across Israel over the coming week. 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.



Joined:	Jun 3, 2021
Messages:	151
Reaction score:	1,489
DragonCoin:	316,208,577.00

Today at 6:23 PM

Greetings NagaPaksa!
After working hard in a rather heavy time,
finally it has been fully re- leased as an Official Tool for us to use in the #OpsPetir event

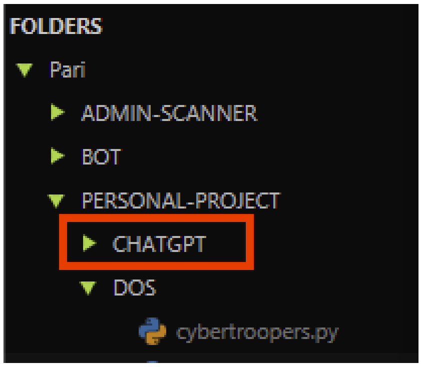
```
165        except ValueError:
```

```
Coded By       :    Pari Malam
Description    :    TCP/UDP/HTTP Dos [Flood] With Considered 7-Layer [#OpsPETIR CyberTroopers]

Forum          :    https://dragonforce.io
Github         :    https://github.com/Pari-Malam
Telegram       :    https://telegram.me/DragonForceIO     I think, ur face got probleno? hehe boiss :P

[+] Enter URLs [Without HTTP/S]

#OpsPetir@CyberTroopers:- dragonforce.io

[+] Perform With 7-Layers (0) [+]

- HTTP Flood [0]
- TCP Flood  [1]
- UDP Flood  [2]

#OpsPetir@CyberTroopers:- 0

Proxy & Socks Method - Press [Y] Enable [N] Disabled

#OpsPetir@CyberTroopers:- |
```

```
198   def choicedownsocks():
199       choice4 = input("Do you want to download a new list of socks? Answer 'Y' to do it: ")
```

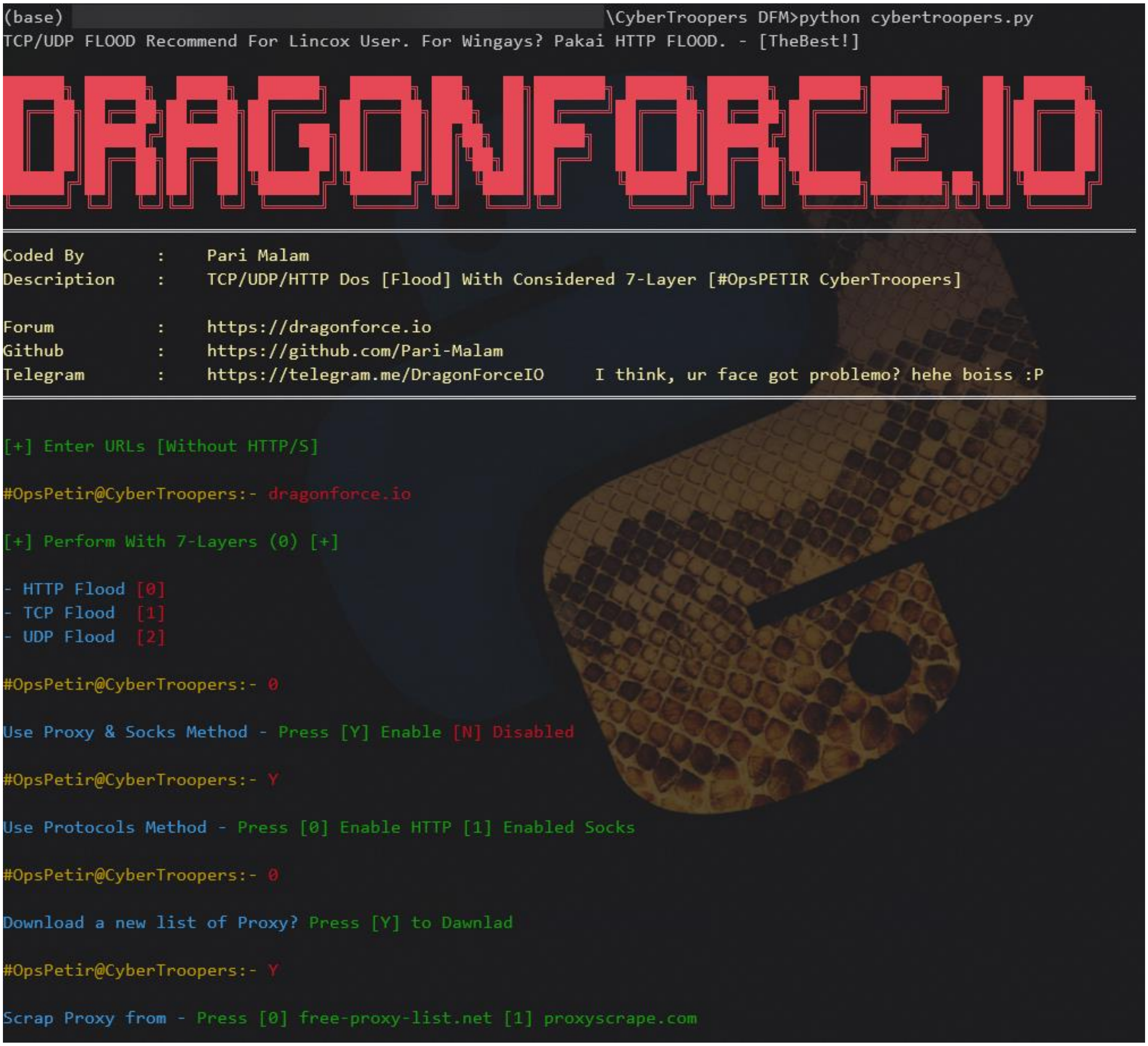
Figure 2: #OpsPETIR CyberTroopers Tool release announcement (source: dragonforce.io)

In an image of the attack tool posted by the creator to the DragonForce Malaysia forum, there is a folder named ChatGPT, indicating that this threat actor may be using OpenAI to aid in the creation and/or modification of the attack script.



```
FOLDERS
▼ Pari
  ▶ ADMIN-SCANNER
  ▶ BOT
  ▼ PERSONAL-PROJECT
    ▶ CHATGPT
    ▼ DOS
        cybertroopers.py
```

Figure 3: ChatGPT folder under the author's working directory



```
(base) [redacted]\CyberTroopers DFM>python cybertroopers.py
TCP/UDP FLOOD Recommend For Lincox User. For Wingays? Pakai HTTP FLOOD. - [TheBest!]

DRAGONFORCE.IO

===========================================================================================
Coded By        :    Pari Malam
Description     :    TCP/UDP/HTTP Dos [Flood] With Considered 7-Layer [#OpsPETIR CyberTroopers]

Forum           :    https://dragonforce.io
Github          :    https://github.com/Pari-Malam
Telegram        :    https://telegram.me/DragonForceIO     I think, ur face got problemo? hehe boiss :P
===========================================================================================

[+] Enter URLs [Without HTTP/S]

#OpsPetir@CyberTroopers:- dragonforce.io

[+] Perform With 7-Layers (0) [+]

- HTTP Flood [0]
- TCP Flood  [1]
- UDP Flood  [2]

#OpsPetir@CyberTroopers:- 0

Use Proxy & Socks Method - Press [Y] Enable [N] Disabled

#OpsPetir@CyberTroopers:- Y

Use Protocols Method - Press [0] Enable HTTP [1] Enabled Socks

#OpsPetir@CyberTroopers:- 0

Download a new list of Proxy? Press [Y] to Dawnlad

#OpsPetir@CyberTroopers:- Y

Scrap Proxy from - Press [0] free-proxy-list.net [1] proxyscrape.com
```

Figure 4: CyberTroopers Attack vectors and proxy scraper feature (source: Radware)

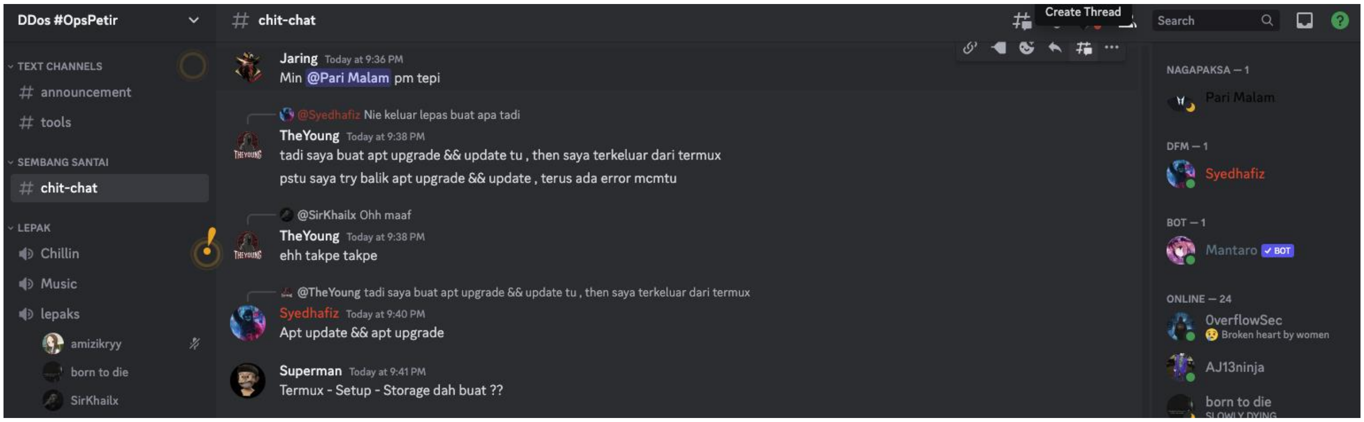
Radware Cybersecurity Advisory

DragonForce Malaysia: OpsPetir

April 12, 2023

Operational Details

This year, DragonForce Malaysia decided to host operational details in an open chat on Discord. In the Discord channel, leaders of the group have shared the CyberTroopers tool and currently are providing support to users who experience issues or limitations while installing the attack tool. As the start of the operation approaches, it is expected that the admins of DragonForce Malaysia will begin posting target lists inside the chat for supporting members.



Jaring Today at 9:36 PM
Min @Pari Malam pm tepi

@Syedhafiz Nie keluar lepas buat apa tadi
TheYoung Today at 9:38 PM
tadi saya buat apt upgrade && update tu , then saya terkeluar dari termux
pstu saya try balik apt upgrade && update , terus ada error mcmtu

@SirKhailx Ohh maaf
TheYoung Today at 9:38 PM
ehh takpe takpe

@TheYoung tadi saya buat apt upgrade && update tu , then saya terkeluar dari termux
Syedhafiz Today at 9:40 PM
Apt update && apt upgrade

Superman Today at 9:41 PM
Termux - Setup - Storage dah buat ??

Figure 5: OpsPetir DDoS channel on Discord

Attack Channel invitation link

- https://discord.com/invite/6sTB9SEp

Hashtag

- #OpsPetir

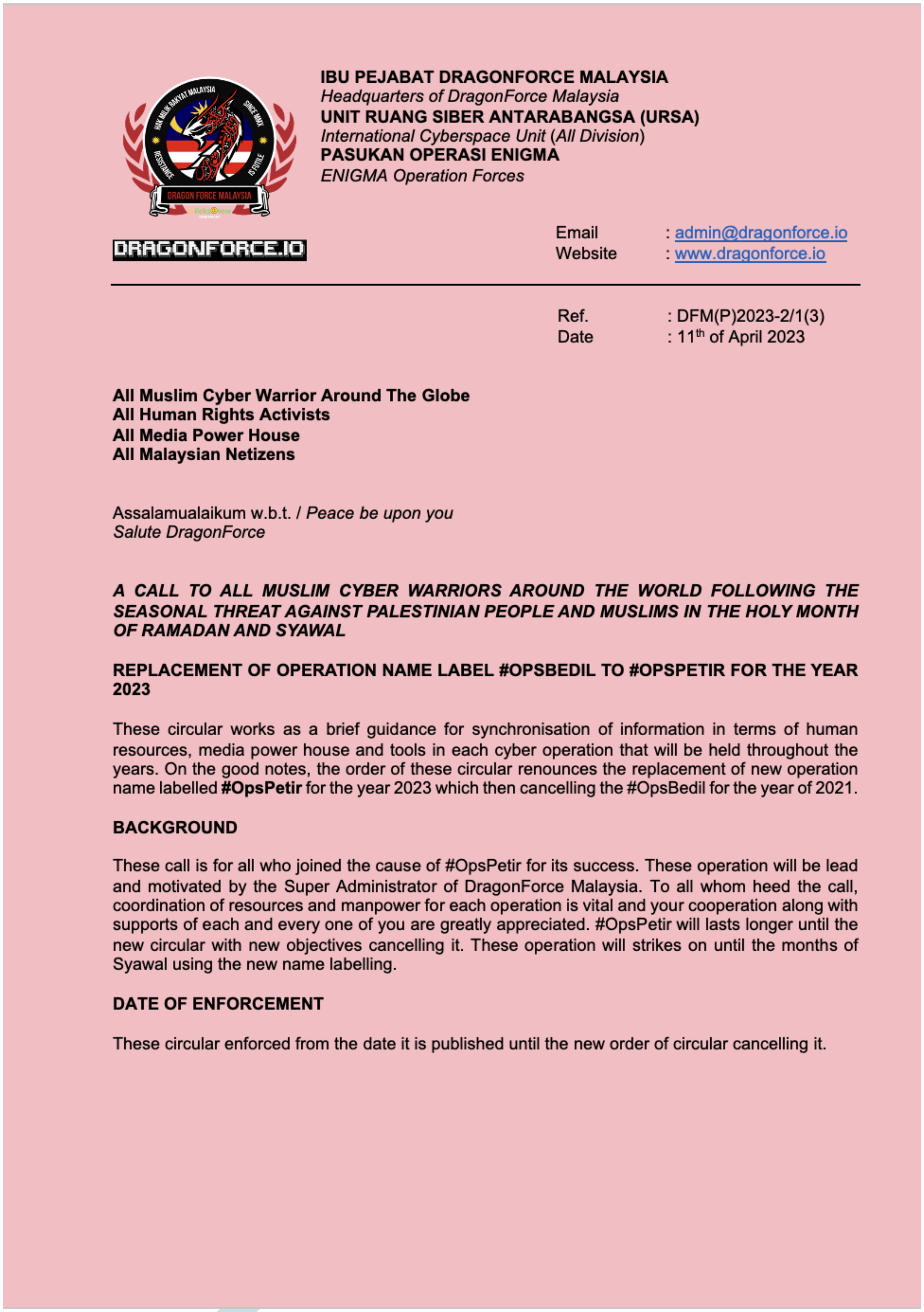
Expected Targets

- Religion
- Financial
- Healthcare
- Service Provider
- Transportation
- Education
- Government

Reasons for Concern

Over the last three years, DragonForce Malaysia and its associates have launched several successful campaigns targeting government agencies and organizations across the Middle East and Asia. While at their core, the group's primary focus is denial-of-service and defacement attacks; they have in the past demonstrated their ability to leverage recently disclosed exploits.

DragonForce Malaysia is expected to be active between April 12th and Al Quds Day, April 21st, with extended operations lasting through April. Attacks will include scanning and exploiting, data dumps, denial-of-service attacks, and website defacements. Those who directly or indirectly support the country of Israel could become a target of DragonForce Malaysia during this period.



IBU PEJABAT DRAGONFORCE MALAYSIA
Headquarters of DragonForce Malaysia
UNIT RUANG SIBER ANTARABANGSA (URSA)
International Cyberspace Unit (All Division)
PASUKAN OPERASI ENIGMA
ENIGMA Operation Forces

DRAGONFORCE.IO

Email	: admin@dragonforce.io
Website	: www.dragonforce.io

Ref.	: DFM(P)2023-2/1(3)
Date	: 11th of April 2023

All Muslim Cyber Warrior Around The Globe
All Human Rights Activists
All Media Power House
All Malaysian Netizens

Assalamualaikum w.b.t. / *Peace be upon you*
Salute DragonForce

A CALL TO ALL MUSLIM CYBER WARRIORS AROUND THE WORLD FOLLOWING THE SEASONAL THREAT AGAINST PALESTINIAN PEOPLE AND MUSLIMS IN THE HOLY MONTH OF RAMADAN AND SYAWAL

REPLACEMENT OF OPERATION NAME LABEL #OPSBEDIL TO #OPSPETIR FOR THE YEAR 2023

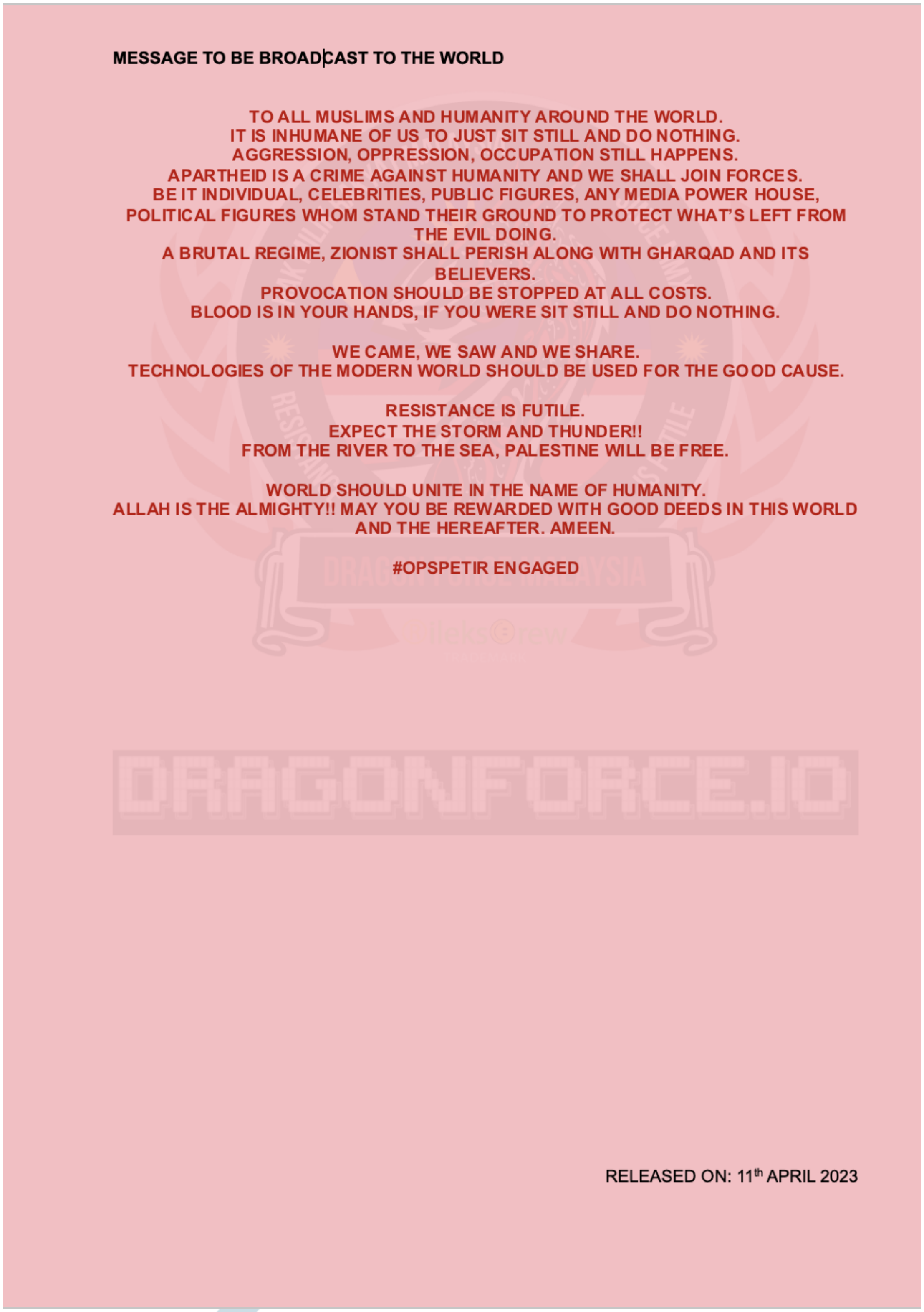
These circular works as a brief guidance for synchronisation of information in terms of human resources, media power house and tools in each cyber operation that will be held throughout the years. On the good notes, the order of these circular renounces the replacement of new operation name labelled **#OpsPetir** for the year 2023 which then cancelling the #OpsBedil for the year of 2021.

BACKGROUND

These call is for all who joined the cause of #OpsPetir for its success. These operation will be lead and motivated by the Super Administrator of DragonForce Malaysia. To all whom heed the call, coordination of resources and manpower for each operation is vital and your cooperation along with supports of each and every one of you are greatly appreciated. #OpsPetir will lasts longer until the new circular with new objectives cancelling it. These operation will strikes on until the months of Syawal using the new name labelling.

DATE OF ENFORCEMENT

These circular enforced from the date it is published until the new order of circular cancelling it.



MESSAGE TO BE BROADCAST TO THE WORLD

TO ALL MUSLIMS AND HUMANITY AROUND THE WORLD.
IT IS INHUMANE OF US TO JUST SIT STILL AND DO NOTHING.
AGGRESSION, OPPRESSION, OCCUPATION STILL HAPPENS.
APARTHEID IS A CRIME AGAINST HUMANITY AND WE SHALL JOIN FORCES.
BE IT INDIVIDUAL, CELEBRITIES, PUBLIC FIGURES, ANY MEDIA POWER HOUSE,
POLITICAL FIGURES WHOM STAND THEIR GROUND TO PROTECT WHAT'S LEFT FROM THE EVIL DOING.
A BRUTAL REGIME, ZIONIST SHALL PERISH ALONG WITH GHARQAD AND ITS BELIEVERS.
PROVOCATION SHOULD BE STOPPED AT ALL COSTS.
BLOOD IS IN YOUR HANDS, IF YOU WERE SIT STILL AND DO NOTHING.

WE CAME, WE SAW AND WE SHARE.
TECHNOLOGIES OF THE MODERN WORLD SHOULD BE USED FOR THE GOOD CAUSE.

RESISTANCE IS FUTILE.
EXPECT THE STORM AND THUNDER!!
FROM THE RIVER TO THE SEA, PALESTINE WILL BE FREE.

WORLD SHOULD UNITE IN THE NAME OF HUMANITY.
ALLAH IS THE ALMIGHTY!! MAY YOU BE REWARDED WITH GOOD DEEDS IN THIS WORLD AND THE HEREAFTER. AMEEN.

#OPSPETIR ENGAGED

RELEASED ON: 11th APRIL 2023

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use 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 against unknown threats and zero-day attacks

A Cyber-Security 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 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 achieve improved bot detection and blocking

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

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

LEARN MORE AT RADWARE'S 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. Additionally, visit Radware's Quarterly DDoS & Application Threat Analysis Center for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.