

Radware Advisory

DragonForce Malaysia OpsPatuk / OpsIndia

June 14, 2022

On June 10th, 2022, DragonForce Malaysia launched a series of cyberattacks against the government of India and numerous organizations across the country.

OpsPatuk

OpsPatuk is a new campaign from DragonForce Malaysia. Like all operations this hacktivist group runs, this one is reactionary and in response to the controversial Bharatiya Janata Party (BJP) spokesperson [Nupur Sharma condemning the Prophet Muhammad, SAW](#)¹. As a result, DragonForce Malaysia, with the assistance of several other threat groups, has begun indiscriminately scanning, defacing and launching denial-of-service attacks against numerous websites in India. More advanced threat actors were observed leveraging current exploits, breaching networks and leaking data.



Figure 1: DragonForce Malaysia announcing OpsPatuk on social media

DragonForce Malaysia

The driving force behind #OpsPatuk is a hacktivist group known as [DragonForce Malaysia](#). The group is a known pro-Palestinian hacktivist group located in Malaysia and has been observed working with several threat groups in the past, including the T3 Dimension Team and ReliksCrew. 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, including TikTok.

¹ Muslims follow the name of Muhammad by the Arabic benediction sallallahu 'alayhi wa sallam, meaning Peace be upon him, abbreviated as "SAW" or "PBUH".

Radware Advisory

DragonForce Malaysia OpsPatuk / OpsIndia

June 14, 2022

Before #OpsPatuk, DragonForce Malaysia targeted organizations and citizens across Israel with [#OpsBedil](#), [#OpsBedilReloaded](#) and #OpsRWM (Raids Without Mercy).

Recent Attacks

Members of DragonForce Malaysia, along with other threat groups, began targeting numerous organizations and government resources in India with defacements, denial-of-service attacks and data leaks on June 10, 2022, as part of OpsPatuk. The operation is still ongoing at the time of publication.

DDOS ATTACKS

As seen in previous operations, DragonForce Malaysia again uses well-designed advertisements that list information about targets to entice followers to join the operation. The events are announced in the DragonForce Malaysia forums and shared through social platforms. Denial-of-service campaigns from the threat group are typically announced less than 24 hours in advance. In addition to the official attacks, unannounced denial-of-service attacks are to be expected by “lone-wolfs” as the operation progresses.



Figure 2: OpsPatuk attack flyer

DragonForce Malaysia is not considered an advanced or a persistent threat group, nor are they currently considered to be sophisticated. But where they lack sophistication, they make up for it with their organizational skills and ability to quickly disseminate information to other members. Threat actors launching denial-of-service attacks during #OpsPatuk have been leveraging DragonForce Malaysia’s standard toolset, including but not limited to, Slowloris, DDoSTool, DDoS-Ripper, Hammer, and several other scripts generally found in open source repositories such as GitHub. To this date, the threat group has not been seen leveraging IoT botnets.

Radware Advisory

DragonForce Malaysia OpsPatuk / OpsIndia

June 14, 2022

DEFACEMENTS

Radware has observed and confirmed numerous defacements across India by DragonForce Malaysia and its associates since the start of the campaign on June 10. The defacements claim that India's BJP spokesperson, Nupur Sharm, insulted the Prophet Muhammad and that the country abuses its Muslim population. DragonForce Malaysia claims, in the defacements, it will be victorious over India in the end, but does not truly define its overall objective.

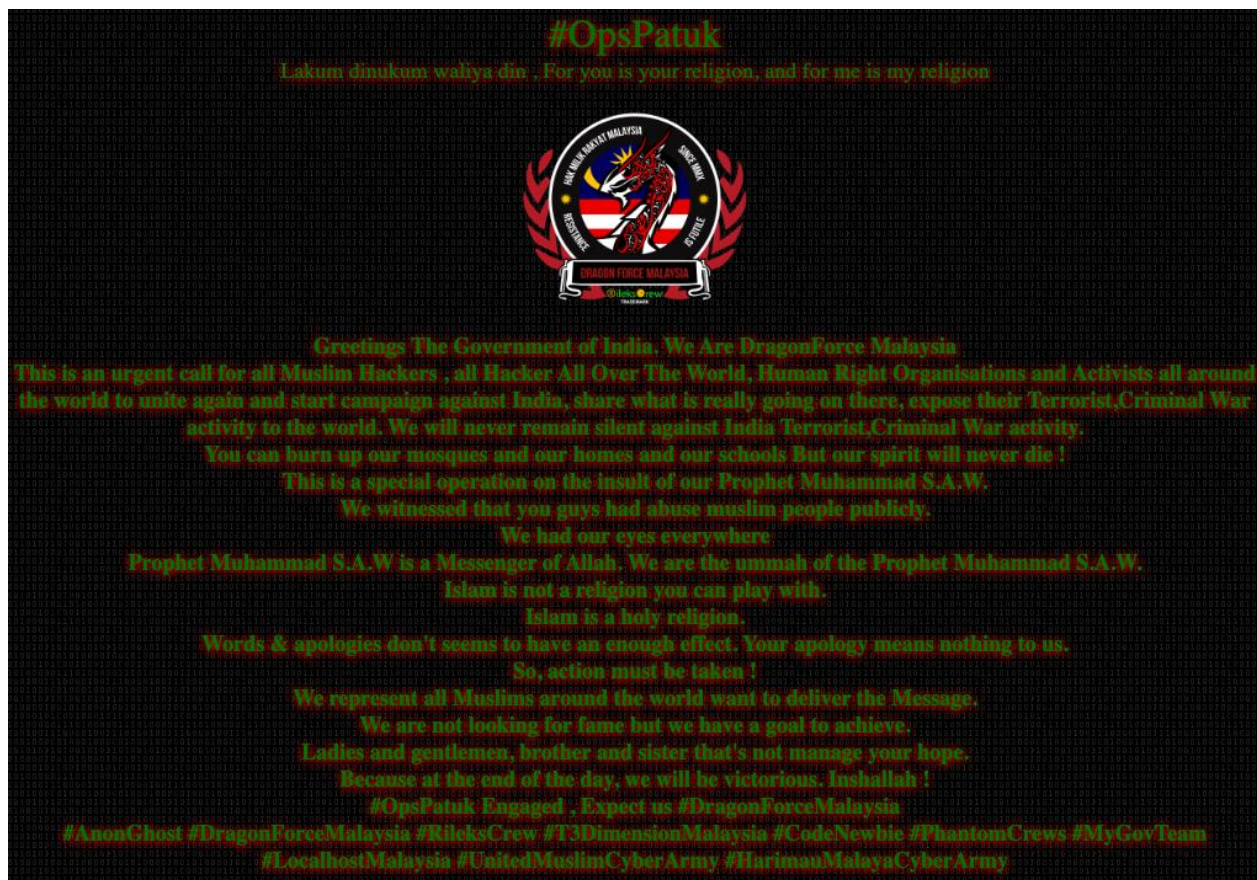


Figure 3: OpsPatuk defacement message by DragonForce Malaysia members

In addition to numerous defacements by DragonForce Malaysia, several other hacktivists, including 'Localhost', 'M4NGTX', '1887', and 'RzkyO', have been seen defacing multiple websites across India in the name of their religion.

Radware Advisory

DragonForce Malaysia OpsPatuk / OpsIndia

June 14, 2022



Figure 4: OpsPatuk defacement message by Localhost

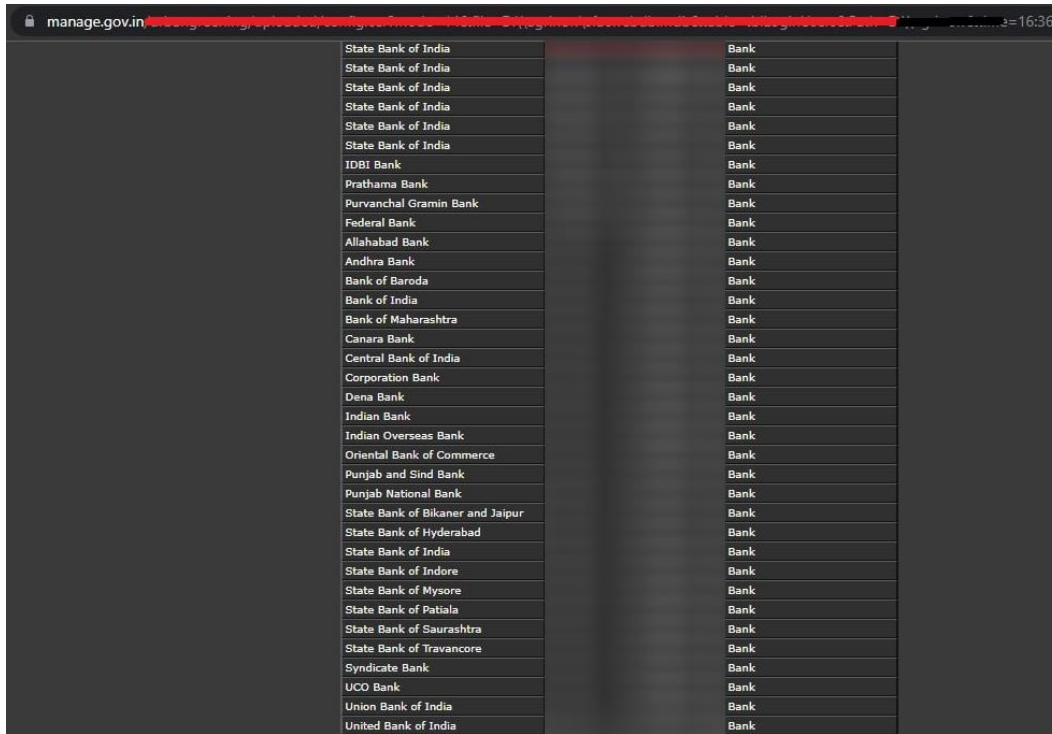
DATA LEAKS

DragonForce Malaysia has claimed several data leaks since the beginning of the campaign. Data leaks are often difficult to validate and their origins verified. At this time, the threat group has claimed to have breached and leaked data from various government agencies, financial institutions, universities, service providers, and several other Indian databases.

Radware Advisory

DragonForce Malaysia OpsPatuk / OpsIndia

June 14, 2022



The screenshot shows a web browser window with the address bar displaying 'manage.gov.in'. The main content area contains a table with two columns. The left column lists various Indian banks, and the right column lists the word 'Bank' for each entry. The banks listed include State Bank of India, IDBI Bank, Prathama Bank, Purvanchal Gramin Bank, Federal Bank, Allahabad Bank, Andhra Bank, Bank of Baroda, Bank of India, Bank of Maharashtra, Canara Bank, Central Bank of India, Corporation Bank, Dena Bank, Indian Bank, Indian Overseas Bank, Oriental Bank of Commerce, Punjab and Sind Bank, Punjab National Bank, State Bank of Bikaner and Jaipur, State Bank of Hyderabad, State Bank of India, State Bank of Indore, State Bank of Mysore, State Bank of Patiala, State Bank of Saurashtra, State Bank of Travancore, Syndicate Bank, UCO Bank, Union Bank of India, and United Bank of India.

State Bank of India	Bank
State Bank of India	Bank
State Bank of India	Bank
State Bank of India	Bank
State Bank of India	Bank
State Bank of India	Bank
IDBI Bank	Bank
Prathama Bank	Bank
Purvanchal Gramin Bank	Bank
Federal Bank	Bank
Allahabad Bank	Bank
Andhra Bank	Bank
Bank of Baroda	Bank
Bank of India	Bank
Bank of Maharashtra	Bank
Canara Bank	Bank
Central Bank of India	Bank
Corporation Bank	Bank
Dena Bank	Bank
Indian Bank	Bank
Indian Overseas Bank	Bank
Oriental Bank of Commerce	Bank
Punjab and Sind Bank	Bank
Punjab National Bank	Bank
State Bank of Bikaner and Jaipur	Bank
State Bank of Hyderabad	Bank
State Bank of India	Bank
State Bank of Indore	Bank
State Bank of Mysore	Bank
State Bank of Patiala	Bank
State Bank of Saurashtra	Bank
State Bank of Travancore	Bank
Syndicate Bank	Bank
UCO Bank	Bank
Union Bank of India	Bank
United Bank of India	Bank

Figure 5: Alleged leak by DragonForce Malayse

DragonForce Forum

The threat actors behind DragonForce Malaysia created their forum a year ago, on June 11, 2021. Today, the forum has tens of thousands of users and threads ranging from running an eSports team to launching cyberattacks. Users in the forum gain social credit and DragonCoins based on the information and knowledge they share with the broader community.

CVE-2022-26134 ATLISSIAN CONFLUENCE (RCE)

On June 3, 2022, Atlassian [published](#) a security advisory regarding a zero-day vulnerability affecting versions of Confluence Server and Data Center. The Remote Code Execution (RCE) vulnerability would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The vulnerability, [CVE-2022-26134](#), was observed being actively exploited in the wild before Atlassian was made aware of it.

Radware Advisory

DragonForce Malaysia OpsPatuk / OpsIndia

June 14, 2022

TAMINGSARI'S THREAD

On June 10, 2022, seven days after Atlassian published their security advisory, a DragonForce Malaysia user, going by the handle of 'TamingSari', posted an educational piece in the DragonForce Malaysia forum and on [YouTube](#) on how to leverage CVE-2022-26134 proof-of-concept code to breach websites for OpsPatuk.

Shodan Dorks for CVE-2022-26134

```
http.component:"atlassian confluence"  
http.favicon.hash:-305179312 country:"IN"  
http.title:"Log In - Confluence" 200  
http.component:"atlassian confluence" http.title:"Log In - Confluence" 200  
http.favicon.hash:-305179312 200
```

LIVE TARGET #OPSPATUK

RISK TARGET

```
https://14.99.30.4/login.action?os_destination=%2Findex.action&permissionViolation=true  
30.99.14-tataidc.co.in
```

MY PROOF OF CONCEPT



Figure 6: Educational post in DragonForce Malaysia forum on how to leverage CVE-2022-26134 to breach websites

Radware Advisory

DragonForce Malaysia OpsPatuk / OpsIndia

June 14, 2022

EDUCATIONAL RESOURCE

The members of the DragonForce Malaysia forum, over the last year, have demonstrated the ability and desire to evolve into a highly sophisticated threat group. Forum members constantly share information and educational resources that help other hackers evolve. More recently, during both #OpsBedilReloaded and #OpsPatuk, users have shared information relating to scanning and discovery, specifically Google Dorking² for vulnerable targets, how to download and set up basic denial-of-service scripts, and more recently, how to leverage exploits to target their victims.

Operational Details

TARGETED VERTICALS

- Government
- Education
- Financial
- Healthcare
- Service Providers
- Agriculture
- Enterprise
- Small Business

ADDITIONAL THREAT GROUPS

- AnonGhost
- Team 1877
- Rileks Crew
- T3 Dimension
- Phantom Crews
- MyGovTeam
- Localhost Malaysia
- Code Newbie
- RzkyO
- United Muslim Cyber Army
- Harimau Malya Cyber Army

HASHTAGS

- #OpsPatuk
- #OpsIndia

SHELL IOCS

- LinkFiles/shell.php
- iqacupload/shell.php
- announceupload/shell.php
- /(S(hxk3e4gjorv5wqxtuzexhacb))/

² Google dorking is a technique that leverages Google Search and other Google applications to discover targets or vulnerable hosts. Example: 'inurl:adminpanel site:gov.*' (source: [exploit-db](#))

Radware Advisory

DragonForce Malaysia OpsPatuk / OpsIndia

June 14, 2022

CONTACTS

- **Forum** – dragonforce.io
- **Facebook** – fb.me/dragonforcedotio
- **Telegram** – t.me/dragonforceio
- **Twitter** – twitter.com/dragonforceio
- **Instagram** – Instagram.com/dragonforceio

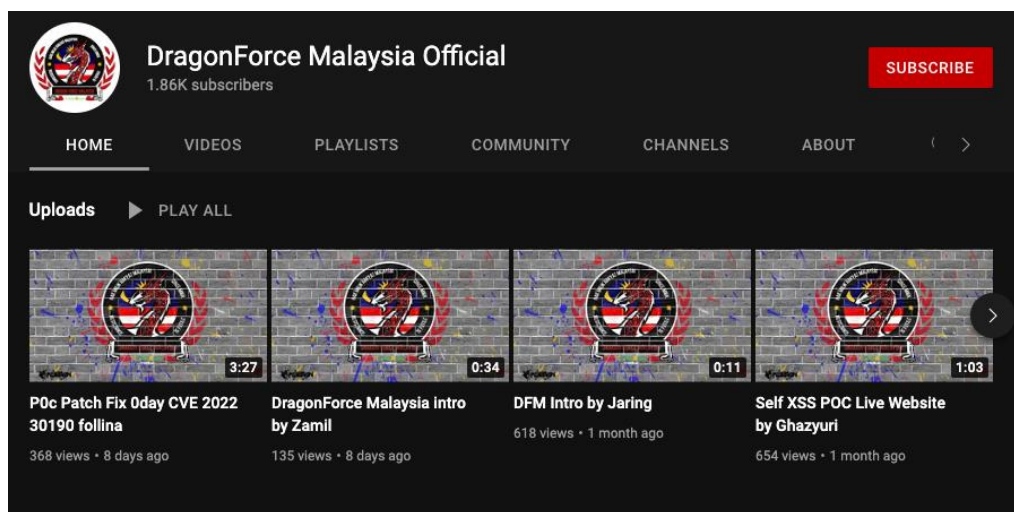


Figure 7: DragonForce Malaysia's Official YouTube Channel

Reasons For Concern

Over the last year, DragonForce Malaysia and its associates have launched several campaigns targeting government agencies and organizations across the Middle East and Asia. The threat groups, in combination, have successfully filled the void left by Anonymous while remaining independent during the resurgence of hacktivists relating to the Russian/Ukrainian war.

EVOLVING THREAT

DragonForce Malaysia and its associates have proven their ability to adapt and evolve with the threat landscape in the last year. While at its core, the group's primary focus is denial-of-service attacks and defacement, they have recently demonstrated their ability to leverage recently disclosed exploits quickly.

Radware expects DragonForce Malaysia to continue launching new reactionary campaigns based on their social, political, and religious affiliations in the foreseeable future.

Radware Advisory

DragonForce Malaysia OpsPatuk / OpsIndia

June 14, 2022

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
- /// **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 THE RADWARE 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 maintained by our Threat Intelligence team for everything security professionals need to know about DDoS attacks and cyber security. Also visit our quarterly updated [DDoS & Application Threat Analysis Hub](#) for up to date statistics and analytics on all threats relating to denial-of-service and online application attacks.