Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TVAI (Threat, Vulnerabilities, Attack, and Impact) Spectrum Report on Dragon Force Ransomware

ST, PT and OTRB ISACs

August 2024

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Purpose

The Public Transportation (PT), Over-the-Road Bus (OTRB), and Surface Transportation (ST) Information Sharing and Analysis Centers (ISACs) are providing this Situational Awareness Bulletin (SAB) for your general security awareness.

Utilization of any standards or guidance discussed herein is strictly voluntary. The practices implemented by rail, transit, and OTRB systems may be more or less restrictive than any recommended practices or guidance in this document. Federal or state regulations sometimes govern portions of public transit systems' operations. In those cases, government regulations should take precedence over the information or guidance provided herein. Organizations should consult their policies and guidance before acting based on the information presented in these documents.

This document supplements guidance and analysis already provided in daily reports produced by the ST, PT, and OTRB ISACs. Of note, the last page of this report lists references for additional information.

FAIR USE: The ST, PT, and OTRB ISACs are providing this report to ISAC members and partners. Recipients may share this report with members of their organization who may benefit from the information; however, public dissemination is not authorized without prior author approval.

To contact ST analysts, please call 866-784-7221 or email st-isac@surfacetransportationisac.org.

To contact PT and OTRB analysts, please call 877-847-5510 or email mcanalyst@motorcoachisac.org.

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Overview

DragonForce (DF) Ransomware first emerged in December of 2023. In less than a year, the group has claimed attacks on dozens of organizations within the healthcare, education, information technology (IT), communications, and transportation sectors. Most of their known victims are from the United States and the United Kingdom. In part to the ransomware's novelty, little is known about the group's origins, members, and possible motives. DF shares a name with the hacktivist group DragonForce Malaysia; however, both groups deny involvement with each other (See Appendix A). DF Malaysia claims its victims on Telegram, whereas DF Ransomware claims its victims via the Onion leak site DragonLeaks.

Figure 1

DragonLeaks homepage (Cyble, 2024).

DF Malaysia maintains that its goal is to "oppose oppression" and targets victims based on its pro-Palestinian ideology. According to the group, they do not engage in extortion for personal gain, which is believed to be the motive for DF ransomware (See Appendix B). However, many cyber experts believe the two groups are linked. WatchGuard's recently published threat profile on DF Ransomware noted that "In 2023… DragonForce Malaysia claimed they were in the process of creating a ransomware operation… Let's not forget that one of the primary goals of ransomware groups is to avoid attribution, and they are prolific liars." Despite the allegations, until confirmed, the ST, PT, and OTRB ISACs consider them separate entities. Furthermore, this paper will only report on the research, tactics, and victims that are solely associated with DragonLeaks.

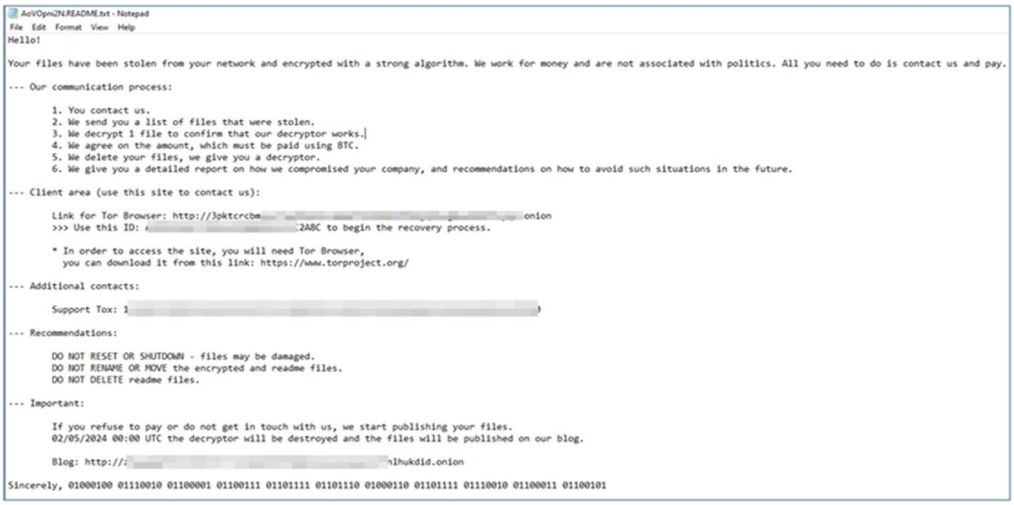
MITRE ATT&CK Alignment

The methodology and tactics of DF ransomware actors align closely with the MITRE ATT&CK framework. The group most commonly gains initial access through phishing attacks, particularly spearphishing with malicious attachments (T1566.001) such as Word documents, Excel files, or ZIP archives containing JavaScript files, to trick users into executing malware. The group is also known to gain access by exploiting vulnerabilities in Remote Desktop Protocols (RDP) and Virtual Private Network (VPN) solutions (T1133) (SOCRadar, 2024). Once inside a victim's network, DF employs User Execution (T1204.002) by tricking users into opening malicious files. The ransomware then impairs defenses by disabling or modifying security tools (T1562.001), specifically targeting Windows Defender. The malware is programmed to delete itself after execution (T1070.004) to erase remnants of the group's activity on the network.

The group utilizes File and Directory Discovery (T1083) to enumerate folders for file encryption and deletion. The primary impact technique is Data Encrypted for Impact (T1486), as the ransomware encrypts victim data for extortion purposes. DF employs a double extortion strategy, exfiltrating sensitive data before encrypting files on the victim's system, indicating using Data from Local System (T1005) or Automated Collection (T1119) techniques. This tactic pressures victims to pay the ransom, as the group threatens to leak the stolen data if their demands are unmet. To facilitate this strategy, DragonForce operates dedicated leak sites on the dark web, where they publish information about their victims and samples of stolen data.

Two such Onion Router (Tor) addresses have been identified:

1. Z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion
2. 3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion.



AoVOpni2NLREADME.txt - Notepad
File Edit Format View Help
Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are not associated with politics. All you need to do is contact us and pay.

--- Our communication process:

1. You contact us.
2. We send you a list of files that were stolen.
3. We decrypt 1 file to confirm that our decryptor works.
4. We agree on the amount, which must be paid using BTC.
5. We delete your files, we give you a decryptor.
6. We give you a detailed report on how we compromised your company, and recommendations on how to avoid such situations in the future.

--- Client area (use this site to contact us):

Link for Tor Browser: http://3pktcrcbm onion
>>> Use this ID: 2ABC to begin the recovery process.

* In order to access the site, you will need Tor Browser,
you can download it from this link: https://www.torproject.org/

--- Additional contacts:

Support Tox: 1

--- Recommendations:

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.

--- Important:

If you refuse to pay or do not get in touch with us, we start publishing your files.
02/05/2024 00:00 UTC the decryptor will be destroyed and the files will be published on our blog.

Blog: http:// nlhukdid.onion

Sincerely, 01000100 01110010 01100001 01100111 01101111 01101110 01000110 01101111 01110010 01100011 01100101

Figure 2

A ransom note from DragonForce (Cyble, 2024).

Malware and Variants Employed

DF utilizes a sophisticated combination of tools and malware in its attacks. The primary malware used by the group is their custom ransomware payload, which is based on the LockBit Black (LockBit 3.0) strain. This ransomware is generated using a leaked builder from the LockBit ransomware group, allowing for extensive customization of payload features. These customizable options include encryption mode, filename encryption, and the ability to exclude specific files or folders from encryption, providing the threat actors with significant flexibility in their attacks.

The ransomware encrypts files on the victim's system, appending the extension ".AoVOpni2N" to encrypted files. The malware terminates specific processes and services to optimize its encryption process and evade detection. This includes stopping antivirus services like Sophos and terminating applications that might lock files, such as database services, email clients, and office software. The list of terminated processes is extensive, including oracle, tbirdconfig, powerpnt, ocssd, mydesktopqos, steam, dbsnmp, ocomm, thebat, synctime, dbeng50, thunderbird, and many others. After encryption, the malware drops a ransom note named "AoVOpni2N.README.txt" (see Figure 2) in each directory it encrypts. This note typically contains instructions for contacting the attackers and making ransom payments, often directing victims to a Tor-based website for further communication.

Indicators of Compromise

Indicators of Compromise (IOCs) are pieces of forensic data that help identify potentially malicious activity on a network or system. For DF, these indicators include file signatures(hashes) that act like digital fingerprints for the malware's code. Each hash type (MD5, SHA1, SHA256) represents a different algorithm used to create these fingerprints, with SHA256 being the most robust and detailed. The IOCs most commonly attributed to the threat actor can be seen in the figures below.

TYPE	VALUE
MD5	d54bae930b038950c2947f5397c13f84
SHA1	e164bbaf848fa5d46fa42f62402a1c55330ef562
SHA256	1250ba6f25fd60077f698a2617c15f89d58c1867339bfd9ee8ab19ce9943304b

Figure 3

IOCs associated with DragonForce Ransomware (Hive Pro, 2024).

Adaptive-based

- ACM.Ps-RgPst!g1
- ACM.Ps-SvcReg!g1
- ACM.Untrst-RLsass!g1

Behavior-based

- AGR.Terminate!g2
- SONAR.Ransom!gen82
- SONAR.TCP!gen1
- SONAR.UACBypass!gen30

File-based

- Ransom.Lockbit!g6
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.2
- WS.SecurityRisk.4

Machine Learning-based

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

Figure 4

Antivirus detection names associated with DragonForce Ransomware (BroadCom, 2024).

In addition to file hashes, IOCs for DragonForce include specific detection names used by antivirus software. For example, Symantec's security products identify this threat using various detection names across different categories. These include adaptive-based detections like "ACM.Ps-RgPst!g1" and "ACM.Untrst-RLsass!g1", which adapt to new threats based on observed patterns in real-time. Behavior-based detections such as "SONAR.Ransom!gen82" and "SONAR.UACBypass!gen30" flag suspicious system activities, including attempts to encrypt files or bypass User Account Control. File-based detections like "Ransom.Lockbit!g6" and "Trojan.Gen.MBT" identify known malware files associated with DragonForce and its LockBit-based components. Machine learning-based detections (e.g.,

"Heur.AdvML.B!100" and "Heur.AdvML.A!300") use AI algorithms to recognize potential threats based on learned patterns from vast malware datasets. Network-based indicators, such as "System Infected: Bad Reputation Application Network Activity," detect suspicious network communications. Web-based detections cover observed domains and IPs associated with DragonForce operations.

Threat to Transportation

DF has targeted a significant number of organizations within the transportation sector. Most notably, the ransomware group claimed Oahu Transit Serv-ices (OTS) as a victim in late June 2024. OTS is a contractor that manages the Honolulu, Hawaii, bus and paratransit system. OTS is the primary bus service on the island of Oahu, managing over 100 routes that connect customers to significant destinations such as Honolulu, Waikiki, Kapolei, and Pearl Harbor (Halycon, 2024). The initial access point has not yet been officially confirmed by OTS or the Federal Bureau of Investigation (FBI), which was investigating the cyber breach. The attack impacted the organization's phone systems and left its websites offline for four days. Additionally, DF listed OTS on its leak site, claiming to have stolen 800,000 records containing customers' sensitive personal information. The attack did not impact bus routes and the ability of OTS to dispatch buses on time; however, the attack did affect customer-facing systems.

Since December 2023, DF has claimed over a dozen transportation organizations on its leak site, many of which provide logistics services. DF is likely targeting the transportation sector, especially logistics, to increase the chance of payment, as a ransomware attack could shut down critical operation systems. Moreover, cybersecurity experts have seen a sharp increase in cyberattacks in the sector since 2017 (Truck News, 2023).

Another claimed victim of DF is Seafrigo, an international freight and logistics company specializing in food transportation. The threat actor added them to their leak site on 12 June 2024 and claimed to have exfiltrated 43.01 GB of data. The ransom deadline was set for the same day. A company representative has not officially confirmed the attack on Seafrigo, nor can the ST, PT, and OTRB ISAC confirm DF leaking the allegedly stolen information. However, another similar DF victim, confirmed through various news outlets, is Ward Trucking & Logistics. The company was attacked on 3 March 2024, and 574.14 GB of data was stolen. The attack severely impacted multiple layers of Ward's network, forcing the company to run "limited operations to handle freight already in their system." Ward Trucking & Logistics fully resolved the breach. However, DF's activity highlights cybercriminal groups continued targeting of the sector.

Mitigations/Recommendations

DragonForce Ransomware is a sophisticated threat actor designed to extract the highest ransom possible from its victim. At-risk sectors should follow the preventative measures below:

- Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- Secure accounts by separating user and privileged accounts, enforcing the principle of least privilege, auditing all user, admin, and service accounts, and implementing multi-factor authentication (MFA) to mitigate the risk of compromised valid accounts.
- Conduct regular backup practices and keep those backups offline or in a separate network.
- Update all software regularly.
- Secure credentials by requiring passwords for all password-protected assets to be at least 15 characters, disabling the storage of clear text passwords in LSASS (Local Security Authority Subsystem Service) memory, and ensuring that edge devices (an endpoint on a network) do not contain accounts that could provide domain admin access.
- Secure remote access services by limiting remote desktop services. If RDP is necessary, apply best practices, including auditing the network for systems using RDP, closing unused RDP ports, and logging RDP login attempts.
- Implement cyber safety training to inform staff about the risks and methods used by threat actors to launch attacks and steal data.

References

ATT&CK Matrix for Enterprise; MITRE, 2024
https://attack.mitre.org/#

Dark Web Profile: DragonForce Ransomware; SOCRadar, 6/20/2024
https://socradar.io/dark-web-profile-dragonforce-ransomware/

Dragonforce Ransomware Breach Compromises Oahu Transit Services Data; Halcyon, 6/15/2024
https://ransomwareattacks.halcyon.ai/attacks/dragonforce-ransomware-breach-compromises-oahu-transit-services-data

DragonForce Unleashes Chaos with Leaked Lockbit Builder; Hive Pro, 6/25/2024
https://www.hivepro.com/wp-content/uploads/2024/06/TA2024243.pdf

LOCKBIT Black's Legacy: Unraveling the DragonForce Ransomware Connection; Cyble, 4/24/2024
https://cyble.com/blog/lockbit-blacks-legacy-unraveling-the-dragonforce-ransomware-connection/

New DragonForce Ransomware Variant; Broadcom, 4/26/2024
https://www.broadcom.com/support/security-center/protection-bulletin/new-dragonforce-ransomware-variant

Ransomware – DragonForce; WatchGuard, 2024
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/dragonforce

Rider Data Apparently Compromised in Alleged Ransomware Attack on TheBus, Handi-Van; Hawaii News Now, 6/18/2024
https://www.hawaiinewsnow.com/2024/06/19/ots-cyber-breach-allegedly-includes-800000-pieces-data/

Seafrigo Group Hit by DragonForce Ransomware, 43 GB Data Exfiltrated; Halcyon, 6/12/2024
https://ransomwareattacks.halcyon.ai/attacks/seafrigo-group-hit-by-dragonforce-ransomware-43-gb-data-exfiltrated

Under Attack: Trucking Industry Increasingly At Risk Of Cyberattacks; Truck News, 11/10/2023
https://www.trucknews.com/features/under-attack-trucking-industry-increasingly-at-risk-of-cyberattacks/

Ward Trucking Is the Latest Carrier Under Cyber Attack; Translogistics Inc, 3/4/2024
https://www.translogisticsinc.com/blog/ward-transport-and-logistics-latest-carrier-with-cyberattack

Appendix A

The below image is a screenshot taken from DragonForce Malaysia's Telegram channel, dragonforceio. The hacktivist group posted images from an article that claimed DragonForce Malaysia and DragonForce Ransomware are the same entity.

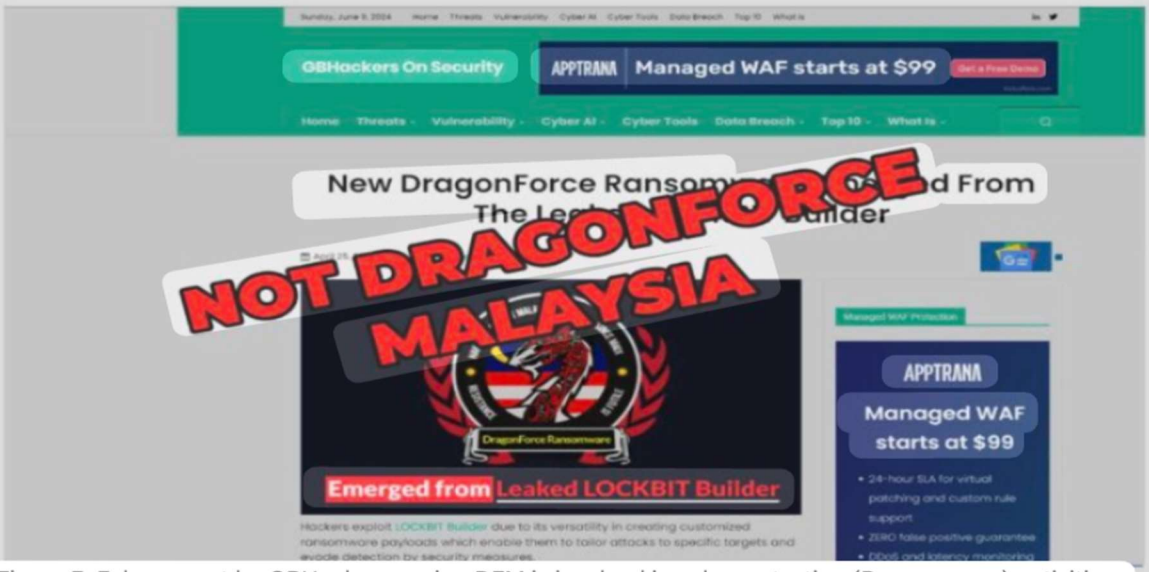


Figure 7: False report by GBHackers saying DFM is involved in cyber extortion (Ransomware) activities.
Source link - GBHackers False Report | DFM

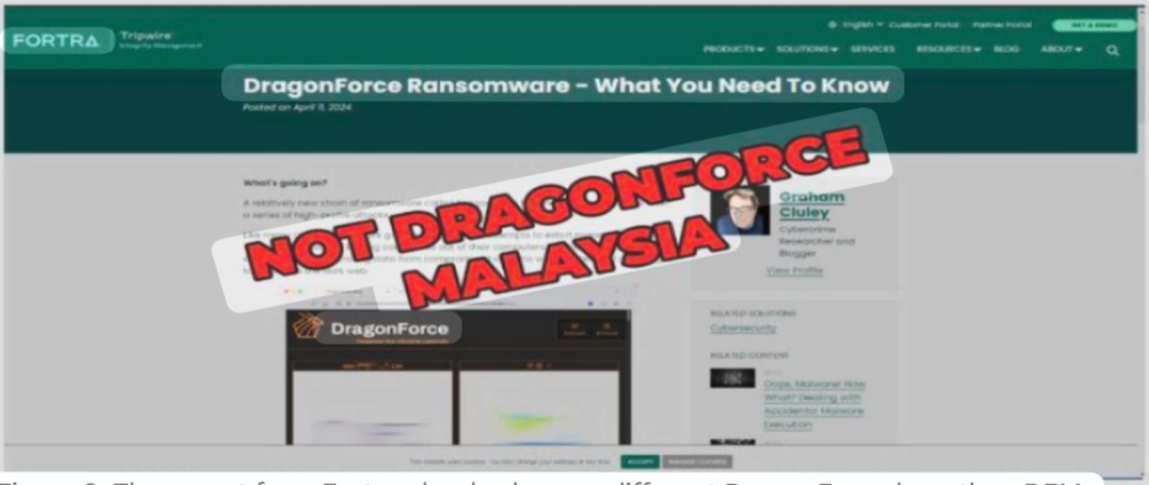


Figure 8: The report from Fortra clearly shows a different DragonForce logo than DFM.
Source link - Fortra | Tripwire Researcher Report

Appendix B

The below images were taken from DragonForce Malaysia's Telegram channel. It is the threat actors formal "motives and modus operandi." The document is available on the group's website, https://dragonforce.io, and Telegram channel. It appears to have been published as a "media release" regarding many articles conflating their tactics, techniques, and procedures with DragonForce Ransomware's.

DFM(SS)2024-1/2(1)

DRAGONFORCE.IO
DRAGONFORCE MALAYSIA

ABOUT DRAGONFORCE MALAYSIA, MOTIVES AND MODES OF OPERATION

All concerned,

PURPOSE

This identification is to ensure the identity of DragonForce Malaysia remains preserved, ensure the uniformity of information delivery, according to the correct procedures and ethics in the movement of assets and resources and guidance to any entity that requires an inquiry.

BACKGROUND

2. DragonForce Malaysia (DFM) is an organization established in 2012, bringing together the community of IT and ethical hacking experts. Dedicated to cyber security and technological innovation, especially to our beloved motherland Malaysia. We foster a collaborative environment for enthusiasts as well as IT lovers and professionals, ensuring a safe and progressive digital community. Created a forum website known as dragonforce.io, now (previously dragonforce.my: domain migration for external reach expansion) for IT activists and enthusiasts from home and abroad to interact in discussions and exchange ideas and establish social relationships.

3. DFM administrators are made up of various backgrounds and it is our confidentiality and ethics not to expose each other to the general public. It became a rumor and public inquiry to get to know the DFM administrator closely. However, on the basis of privacy and humility, we use a persona that can be seen virtually and interacted with in the capacity of IT lovers. In general, we are just IT lovers who use knowledge and skills and wisdom in achieving the same goal in an independent organization managed by ourselves the administrators.

4. As an independent organization (stand-alone), DFM does not focus on the profit and insistence of any party either politically or for personal purposes. DFM is a non-profit organization that takes financial resources from the public or solicits donations. In fact, various free classes and courses are offered to the public to gain knowledge. DFM only promotes affordable paid classes and seminars conducted by experts and recognized professionals in the field of cyber security to the general public. This is to guarantee the quality of education and knowledge on par with the proper qualifications.

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

10. The following is a list of official social media and affiliates that patronize and collaborate under the responsibility of DFM:

OFFICIAL DFM

- Official Forum: https://dragonforce.io
- Official Radio: https://radio.dragonforce.io
- **Facebook:** https://fb.me/dragonforcedotio
- **Telegram:** https://t.me/dragonforceio
- **Twitter:** https://twitter.com/dragonforceIO_
- **Instagram:** https://instagram.com/dragonforceio
- **YouTube:** https://www.youtube.com/@dragonforceio

DFM AFFILIATES

- **TikTok:** https://www.tiktok.com/@komando16_dfm
- **TikTok:** http://www.tiktok.com/@dragonforcemalaysia
- **Discord: DragonForce E-Sports**
- **Telegram:** https://t.me/nusantaraMYID

11. DFM always moves under the name of DragonForce Malaysia (DFM) and delivers special messages to the world. DFM does not engage in cyber activities for fame and fortune. Measure ten times, cut once. Too many entities have sprung up like mushrooms after the rain, using the name and logo and identity of the DFM admin persona. However, only jewelers know manikam. Times change, seasons change. Operations carried out by DFM are covered by foreign and domestic media. Therefore, behavior and speech should reflect oneself. It's like talking to each other during the day, talking to each other at night. This enlightenment is done so that no entity associates the name of DragonForce Malaysia in irresponsible activities and beyond our knowledge. Like some swelling, others pus. Therefore, once again DFM affirms our stance in any cyber operation as hacktivist and denies the involvement of motivated attacks

financial extortion ransomware for personal purposes.

12. Here are some links in the DragonForce Malaysia tag search that can be referred to:

i) https://mazebolt.com/tag/dragonforce-malaysia/
ii) https://www.radware.com/security/threat-advisories-and-attack-reports/dragonforce-malaysia-opspetir/
iii) https://www.brighttalk.com/webcast/12695/547944
iv) https://www.radware.com/security/ddos-knowledge-center/ddospedia/opsbedil-and-opsbedilreloaded/
v) https://securitybrief.asia/story/resurgence-of-opsbedil-is-hacktivism-now-on-tiktok
i) https://cybernews.com/news/tensions-in-the-middle-east-trigger-a-wave-of-cyberattacks-against-israel/
vii) https://www.radware.com/blog/dragonforce-malaysia-opsbedil-reloaded-campaign-flyerjpg-2/?lang=zh-hans
viii) https://www.firstpost.com/tag/dragonforce-malaysia/
ix) https://www.freepressjournal.in/india/opspatuk-to-be-theme-for-malaysia-based-hacker-group-dragonforces-anniversary-celebrations
x) https://cxotoday.com/interviews/radware-on-fighting-the-fight-against-ddos-attacks-and-why-its-much-needed-today/
xi) https://securitybrief.asia/story/dragonforce-malaysia-attacks-israeli-institutions-radware
xii) https://securityboulevard.com/2022/06/q1-2022-ddos-and-application-attack-activity-an-overview/
xiii) https://cloudsek.com/threatintelligence/hacktivist-group-dragonforce-malaysia-releases-windows-lpe-exploit-discloses-plans-to-evolve-into-a-ransomware-group