CYFIRMA

DECODING THREATS

Caught in the Crossfire

How International Relationships Generate Cyber Threats

EXECUTIVE SUMMARY

In times of conflict, there are consequences of being an ally or an enemy of warring nations, either geopolitically, or in the cyber realm. Analyzing the Russia-Ukraine war and the Israel-Gaza conflict, it's evident that hacktivists now play a significant role, launching attacks using custom-made DDoS tools, defacing websites, and mentoring others in how to disrupt organizations. This behavior arguably goes beyond the attacks themselves, involving a quasi-recruitment process, akin to a sleeper cell, where individuals are trained to act when needed. This dual strategy of cyber and ideological warfare poses huge challenges for governments and private organizations during times of escalating global tension.

INTRODUCTION

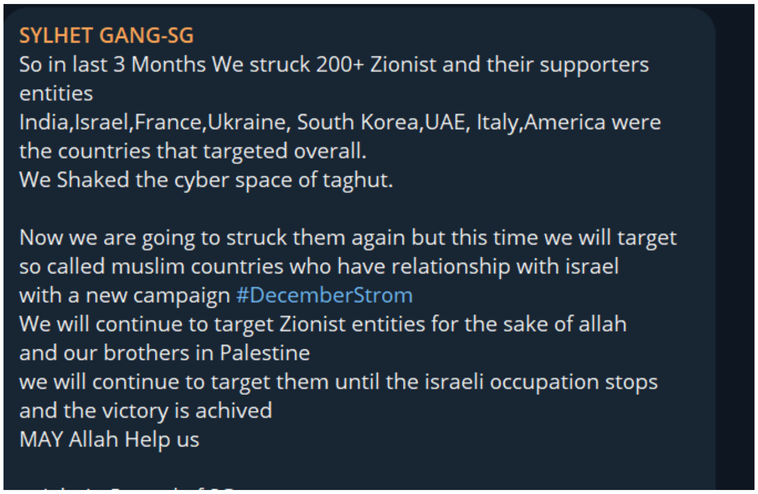
The surge in DDoS attacks and other hacking activities extends beyond the Israel-Gaza war. In the past, hacktivists from Russia (such as NoName057(16) and Killnet) and ransomware gangs supporting pro-Russian causes have engaged in damaging actions against countries opposing their stance.

In the ongoing Israel-Palestine conflict, much is happening in the physical world and online. Previous reports have focused on the geopolitical and cyber aspects of the conflict, whereas this report explores the cybercriminal community in greater depth, including advanced persistent threats, hacktivists, and 'script kiddies' who are destroying servers, leaking sensitive information, defacing websites, and launching DDOS attacks. We've identified many in-house tools created by hackers and shared on platforms like Telegram and GitHub, and tutorials on how to launch cyber-attacks to contribute to the ongoing war.

ASSESSMENT

Hackers Supporting Palestine

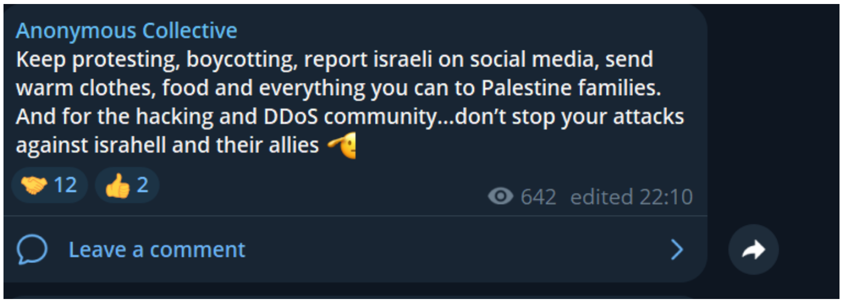
Hackers from Pakistan, Palestine, Turkey, Bangladesh, Iran, and Yemen target nations who are not only directly involved, but their supporters, too.



SYLHET GANG-SG
So in last 3 Months We struck 200+ Zionist and their supporters entities
India,Israel,France,Ukraine, South Korea,UAE, Italy,America were the countries that targeted overall.
We Shaked the cyber space of taghut.

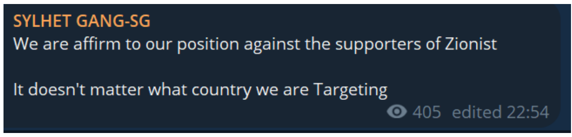
Now we are going to struck them again but this time we will target so called muslim countries who have relationship with israel with a new campaign #DecemberStrom
We will continue to target Zionist entities for the sake of allah and our brothers in Palestine
we will continue to target them until the israeli occupation stops and the victory is achived
MAY Allah Help us

This Anonymous Collective message from Telegram calls for continued attacks against Israel and its supporters.



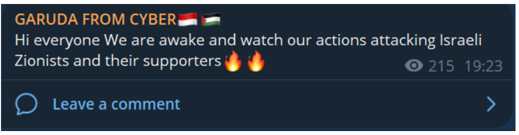
Anonymous Collective
Keep protesting, boycotting, report israeli on social media, send warm clothes, food and everything you can to Palestine families.
And for the hacking and DDoS community...don't stop your attacks against israhell and their allies 🫡

Whilst there are a large number of hacktivist groups supporting Palestine, there appears to be far fewer groups opposing Palestine.



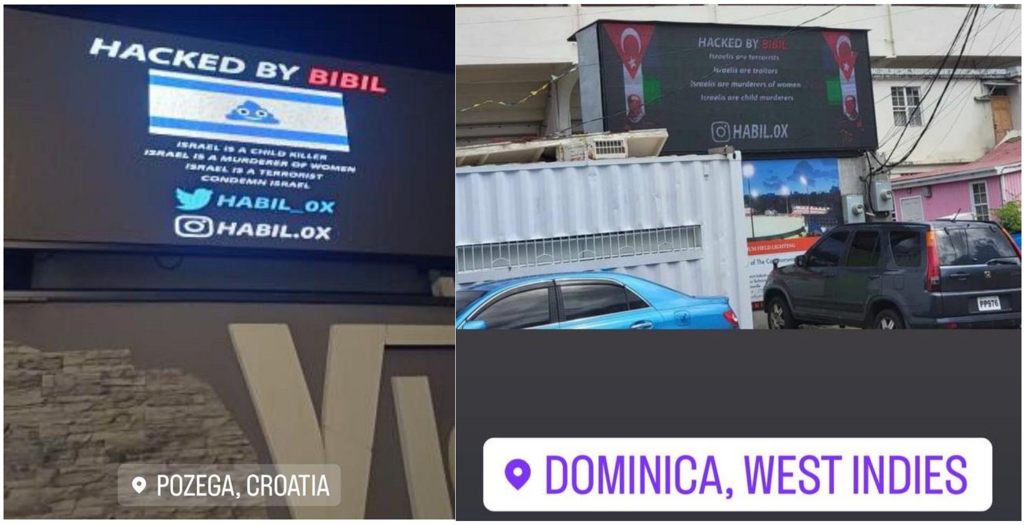
SYLHET GANG-SG
We are affirm to our position against the supporters of Zionist

It doesn't matter what country we are Targeting



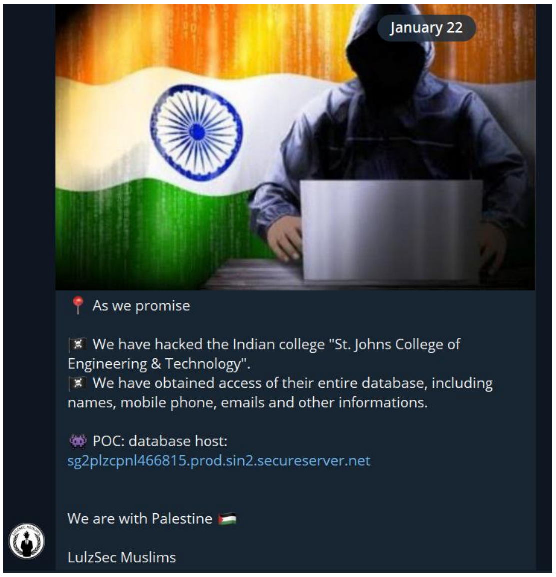
GARUDA FROM CYBER🇮🇩🇵🇸
Hi everyone We are awake and watch our actions attacking Israeli Zionists and their supporters🔥🔥

Pro-Palestinian hacktivist groups have hacked billboards and displayed messages against Israel in Croatia and the West Indies.



Against India

Groups like LulzSec Muslim and SystemadminBD are carrying out significant cyber-attacks against India as part of a wider pro-Palestine campaign. Recently, LulzSec Muslim gained access to the database and server of an Indian engineering college:



📍 As we promise

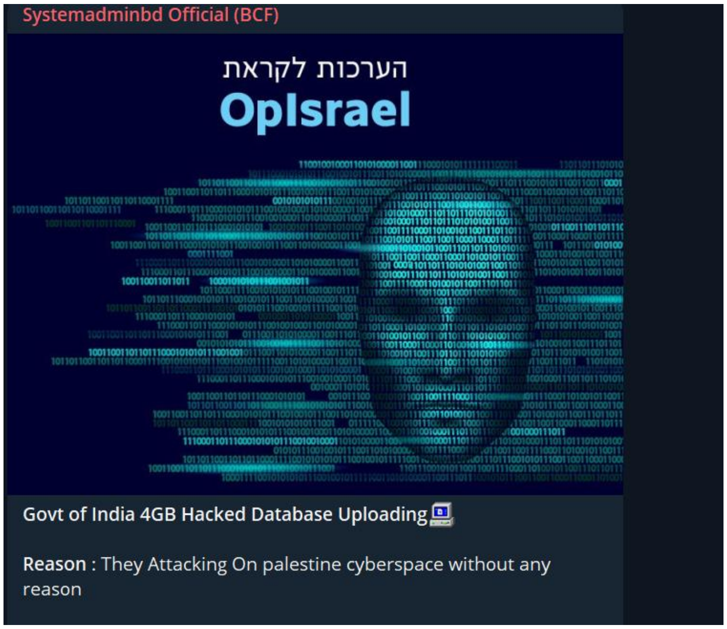
✖ We have hacked the Indian college "St. Johns College of Engineering & Technology".
✖ We have obtained access of their entire database, including names, mobile phone, emails and other informations.

👾 POC: database host:
sg2plzcpnl466815.prod.sin2.secureserver.net

We are with Palestine 🇵🇸

LulzSec Muslims

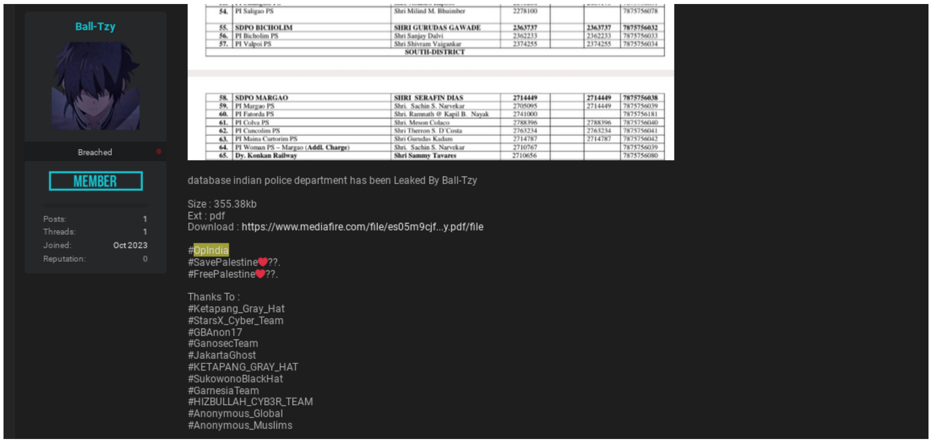
SystemadminBD, a group based in Bangladesh with a history of targeting Indian organizations, has recently attacked the Indian government by claiming to leak a database, stating that their actions were in retaliation to cyber-attacks from Indian hacktivists against the cyberspace of Palestine.


Systemadminbd Official (BCF)

Govt of India 4GB Hacked Database Uploading 💻

Reason : They Attacking On palestine cyberspace without any reason

Additionally, we've observed instances of misinformation being spread by users in underground forums and Telegram groups, claiming to have breached or leaked data, but ultimately their claims didn't stand up to scrutiny: for example, the assertion below, which our investigation debunked by revealing that the data in question had already been officially uploaded on the Goa government's official website some time ago.


Ball-Tzy

Breached

MEMBER

Posts: 1
Threads: 1
Joined: Oct 2023
Reputation: 0

54.	PI Saligao PS	Shri Milind M. Bhuimber	2278100			7875756078
55.	**SDPO BICHOLIM**	**SHRI GURUDAS GAWADE**	**2363737**		**2363737**	**7875756032**
56.	PI Bicholim PS	Shri Sanjay Dalvi	2362233		2362233	7875756033
57.	PI Valpoi PS	Shri Shivram Vaigankar	2374255		2374255	7875756034
		SOUTH-DISTRICT				

58.	**SDPO MARGAO**	**SHRI SERAFIN DIAS**	**2714449**		**2714449**	**7875756038**
59.	PI Margao PS	Shri. Sachin S. Narvekar	2705095		2714449	7875756039
60.	PI Fatorda PS	Shri. Ramnath @ Kapil B. Nayak	2741000			7875756181
61.	PI Colva PS	Shri. Meson Colaco	2788396		2788396	7875756040
62.	PI Cuncolim PS	Shri Therron S. D'Costa	2763234		2763234	7875756041
63.	PI Maina Curtorim PS	Shri Gurudas Kadam	2714787		2714787	7875756042
64.	PI Woman PS – Margao (**Addl. Charge**)	Shri. Sachin S. Narvekar	2710767			7875756039
65.	**Dy. Konkan Railway**	**Shri Sammy Tavares**	2710656			7875756080

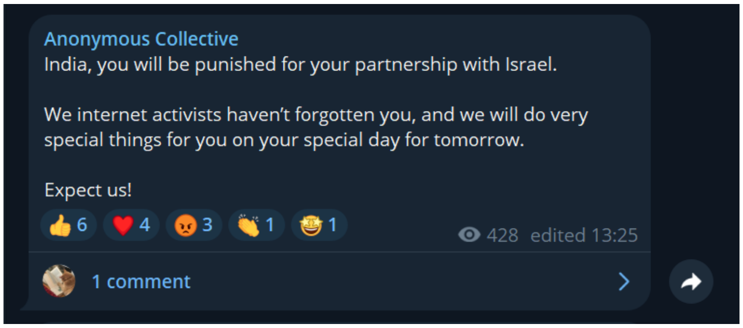
database indian police department has been Leaked By Ball-Tzy

Size : 355.38kb
Ext : pdf
Download : https://www.mediafire.com/file/es05m9cjf...y.pdf/file

#OpIndia
#SavePalestine❤️??.
#FreePalestine❤️??.

Thanks To :
#Ketapang_Gray_Hat
#StarsX_Cyber_Team
#GBAnon17
#GanosecTeam
#JakartaGhost
#KETAPANG_GRAY_HAT
#SukowonoBlackHat
#GarnesiaTeam
#HIZBULLAH_CYB3R_TEAM
#Anonymous_Global
#Anonymous_Muslims

The Anonymous Collective initiated an attack on the Indian Post website, rending it inaccessible for four consecutive days and causing difficulties for many users.

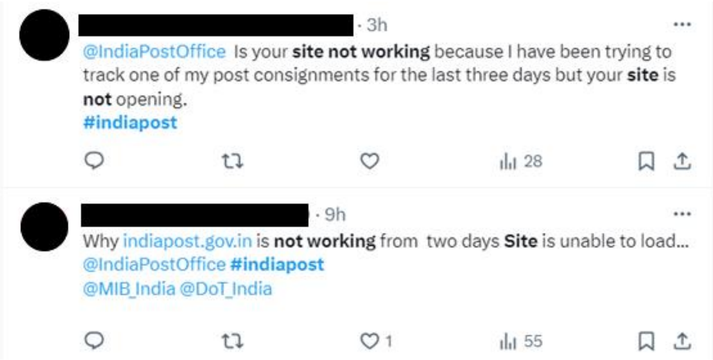


Anonymous Collective

India, you will be punished for your partnership with Israel.

We internet activists haven't forgotten you, and we will do very special things for you on your special day for tomorrow.

Expect us!

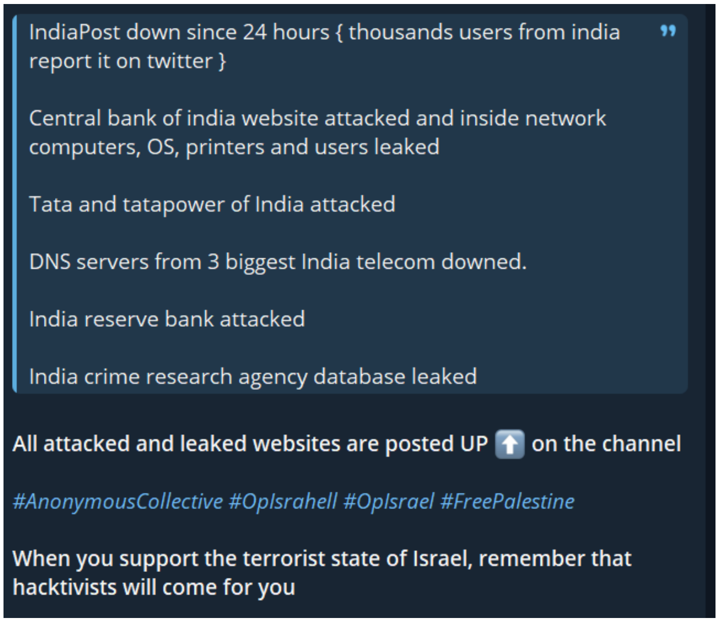


[redacted] · 3h

@IndiaPostOffice Is your **site not working** because I have been trying to track one of my post consignments for the last three days but your **site** is **not** opening.
#indiapost

[redacted] · 9h

Why indiapost.gov.in is **not working** from two days **Site** is unable to load...
@IndiaPostOffice **#indiapost**
@MIB_India @DoT_India



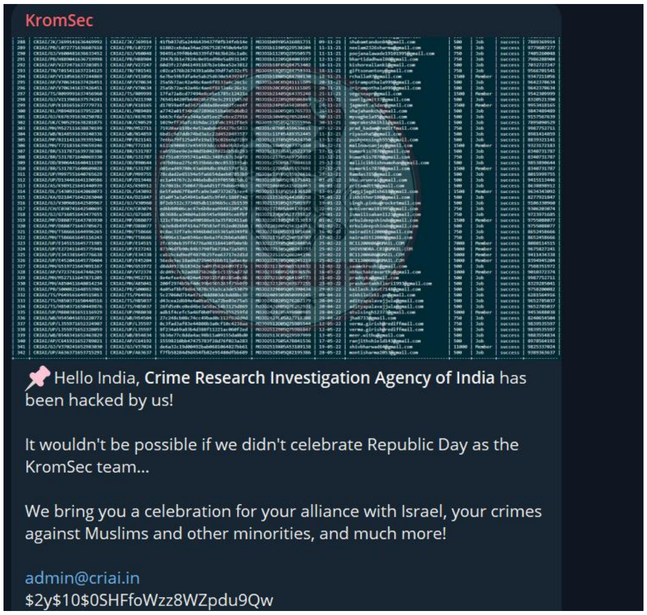
> IndiaPost down since 24 hours { thousands users from india report it on twitter }
>
> Central bank of india website attacked and inside network computers, OS, printers and users leaked
>
> Tata and tatapower of India attacked
>
> DNS servers from 3 biggest India telecom downed.
>
> India reserve bank attacked
>
> India crime research agency database leaked

All attacked and leaked websites are posted UP ⬆️ on the channel

#AnonymousCollective #OpIsrahell #OpIsrael #FreePalestine

When you support the terrorist state of Israel, remember that hacktivists will come for you

The Kromsec hacker group conducted a DDoS (Distributed Denial of Service) attack, and leaked data from the Central Bank of India and the India Crime Research Agency:



KromSec

📌 Hello India, **Crime Research Investigation Agency of India** has been hacked by us!

It wouldn't be possible if we didn't celebrate Republic Day as the KromSec team...

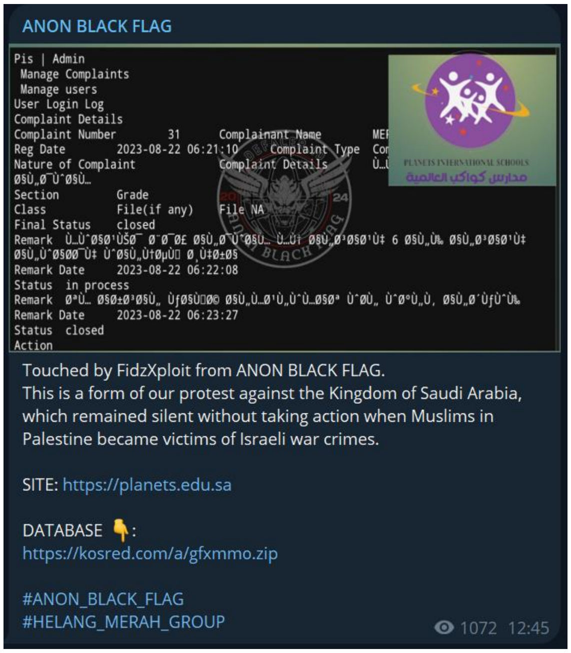
We bring you a celebration for your alliance with Israel, your crimes against Muslims and other minorities, and much more!

admin@criai.in
$2y$10$0SHFfoWzz8WZpdu9Qw

Upon investigating the data leaked by KromSec on ICRA, we ascertained that none of the data was confidential in nature, simply containing data from their web server to host the website. This is another example of how hacktivists tend to overemphasize their impact on the cyber threat landscape globally.

Against Saudi Arabia

Several hacktivist groups are targeting multiple sectors within Saudi Arabia, for example, ‘Anon Black Flag’ which were found targeting education websites.



ANON BLACK FLAG

```
Pis | Admin
 Manage Complaints
 Manage users
User Login Log
Complaint Details
Complaint Number        31      Complainant Name       MEF
Reg Date        2023-08-22 06:21:10     Complaint Type  Cor
Nature of Complaint             Complaint Details      Ù…Ù
Ø§Ù„Ø¯Ù ØªØ§Ù…
Section         Grade
Class           File(if any)    File NA
Final Status    closed
Remark  Ù…Ù ØªØ§Ø¹ÙŠØ¯ Ø¨Ø¯Ø£ Ø§Ù„Ø¯Ù ØªØ§Ù… Ù…Ù† Ø§Ù„Ø³Ø§Ø¹Ù‡ 6 Ø§Ù„Ù‰ Ø§Ù„Ø³Ø§Ø¹Ù‡
Ø§Ù„Ù Ø§Ø¯Ø¯Ù‡ Ù Ø§Ù„Ù†ØµÙ Ø¸Ù‡Ø±Ø§
Remark Date     2023-08-22 06:22:08
Status  in process
Remark  ØªÙ… Ø§Ø±Ø³Ø§Ù„ ÙƒØ§Ù ØŒ Ø§Ù„Ù…Ø¹Ù„Ù Ù…Ø§Øª Ù ØÙ„ Ù Ø°Ù„Ù, Ø§Ù„Ø´ÙƒÙ Ù‰
Remark Date     2023-08-22 06:23:27
Status  closed
Action
```

Touched by FidzXploit from ANON BLACK FLAG.
This is a form of our protest against the Kingdom of Saudi Arabia, which remained silent without taking action when Muslims in Palestine became victims of Israeli war crimes.

SITE: https://planets.edu.sa

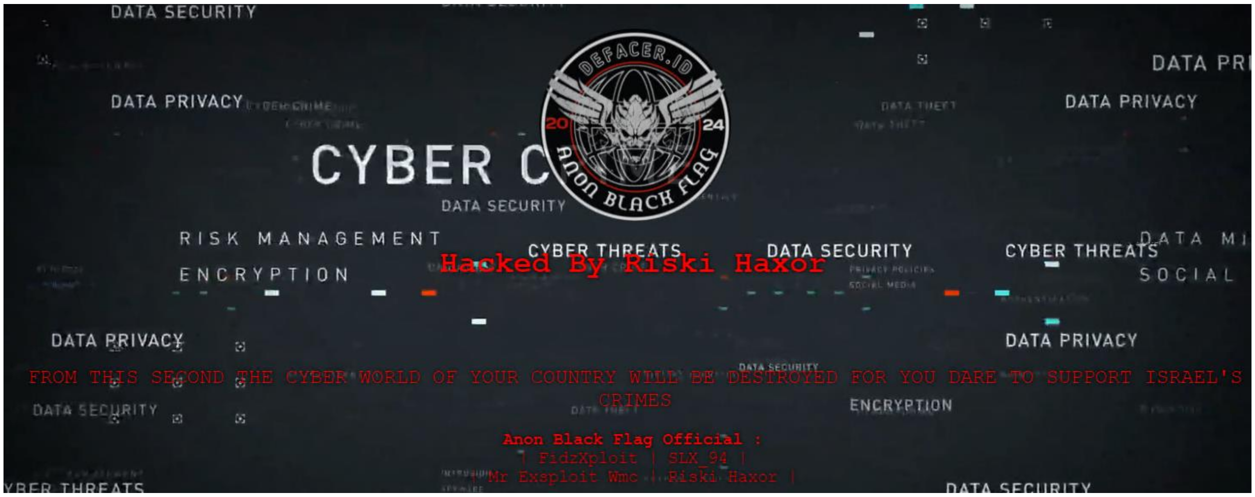
DATABASE 👇:
https://kosred.com/a/gfxmmo.zip

#ANON_BLACK_FLAG
#HELANG_MERAH_GROUP

👁 1072 12:45

Against USA

The USA is a prominent target, with multiple websites defaced in response to the nation's support of Israel.



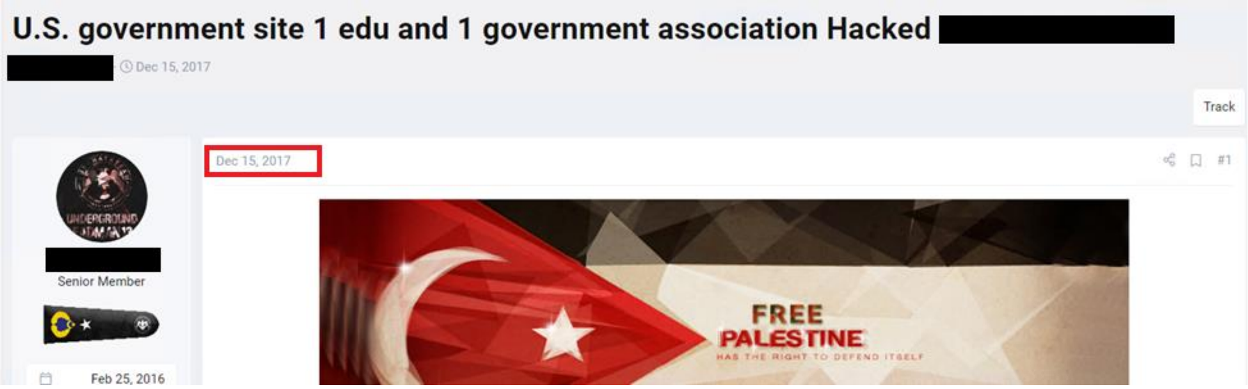
Hacked By Riski Haxor

FROM THIS SECOND THE CYBER WORLD OF YOUR COUNTRY WILL BE DESTROYED FOR YOU DARE TO SUPPORT ISRAEL'S CRIMES

Anon Black Flag Official :
| FidzXploit | SLX_94 |
| Mr Exsploit Wmc | Riski Haxor |

Website defacements are not a new occurrence, as this post from 2017 can attest. In this case, the Turkish-based group; 'Turkhackteam', targeted Mossad and websites associated with the USA, as part of a Free Palestine campaign.

Turkhackteam was established in 2002 by Arsenik and is one of the oldest hacking forums in Turkey, first gaining recognition by hacking a Microsoft MSN web portal subdomain and engaging in other high-profile activities.



U.S. government site 1 edu and 1 government association Hacked [redacted]

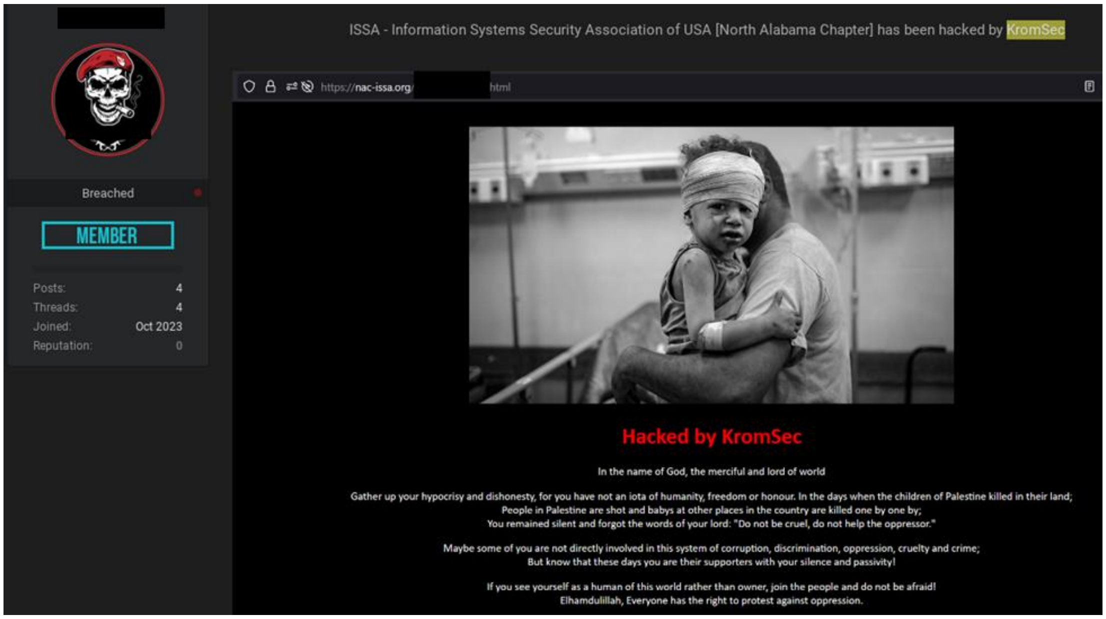
[redacted] Dec 15, 2017

Dec 15, 2017

[redacted]
Senior Member

Feb 25, 2016

Kromsec successfully hacked and breached the data of AC-ISSA (Information Systems Security Association) North Alabama Chapter, claiming the attack on Beach forum. The compromised information includes email addresses, names, phone numbers, locations, and other related data.


[redacted]

Breached

MEMBER

Posts:	4
Threads:	4
Joined:	Oct 2023
Reputation:	0

ISSA - Information Systems Security Association of USA [North Alabama Chapter] has been hacked by KromSec

https://nac-issa.org/[redacted]html

Hacked by KromSec

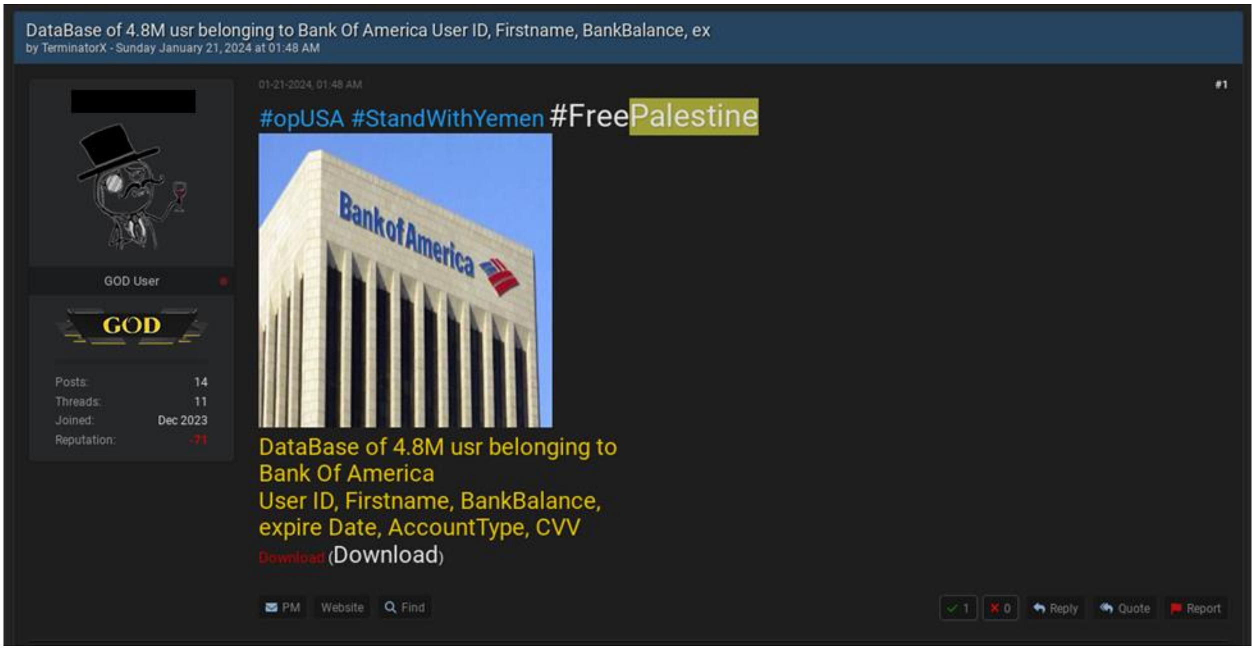
In the name of God, the merciful and lord of world

Gather up your hypocrisy and dishonesty, for you have not an iota of humanity, freedom or honour. In the days when the children of Palestine killed in their land;
People in Palestine are shot and babys at other places in the country are killed one by one by;
You remained silent and forgot the words of your lord: "Do not be cruel, do not help the oppressor."

Maybe some of you are not directly involved in this system of corruption, discrimination, oppression, cruelty and crime;
But know that these days you are their supporters with your silence and passivity!

If you see yourself as a human of this world rather than owner, join the people and do not be afraid!
Elhamdulillah, Everyone has the right to protest against oppression.

Since mid-October, there have been over 100 cyber-attacks on the United States. US defense officials report that more than 100 drones and missiles have been launched against vessels, targeting Israeli interests. In contrast to these kinetic events, a user on a Breach Forum leaked a database associated with Bank of America, purportedly as a response to the American stance on the Red Sea conflict.


DataBase of 4.8M usr belonging to Bank Of America User ID, Firstname, BankBalance, ex
by TerminatorX - Sunday January 21, 2024 at 01:48 AM

[redacted]

GOD User

GOD

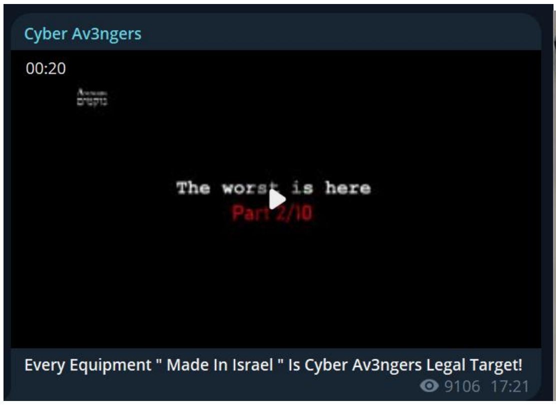
Posts:	14
Threads:	11
Joined:	Dec 2023
Reputation:	-71

01-21-2024, 01:48 AM #1

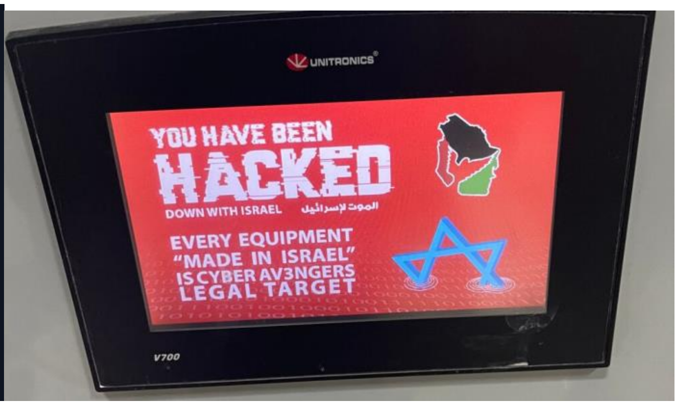
#opUSA #StandWithYemen #FreePalestine

DataBase of 4.8M usr belonging to
Bank Of America
User ID, Firstname, BankBalance,
expire Date, AccountType, CVV
Download (Download)

Cyber Av3ngers affiliated to Iran's Islamic Revolutionary Guard Corps (IRGC) announced their intention to target any equipment made in Israel, and have attacked water systems in the United States, made by Unitronics, headquartered in Israel.

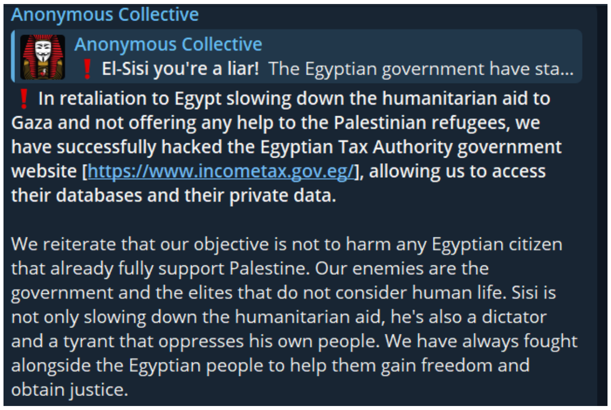


Every Equipment " Made In Israel " Is Cyber Av3ngers Legal Target!



Against Egypt

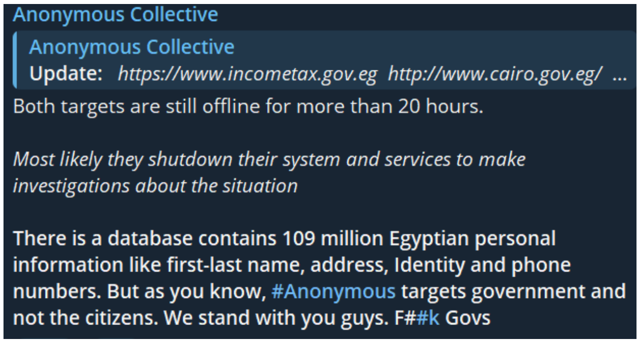
Hacktivists have turned their attention to the Egyptian government for slowing down humanitarian aid to Palestinian refugees. In retaliation, the Anonymous Collective group executed a DDoS attack against the Cairo official website and the government income tax department, collecting a database of 109 million records containing sensitive data.



❗ **El-Sisi you're a liar!** The Egyptian government have sta...

❗ **In retaliation to Egypt slowing down the humanitarian aid to Gaza and not offering any help to the Palestinian refugees, we have successfully hacked the Egyptian Tax Authority government website [https://www.incometax.gov.eg/], allowing us to access their databases and their private data.**

We reiterate that our objective is not to harm any Egyptian citizen that already fully support Palestine. Our enemies are the government and the elites that do not consider human life. Sisi is not only slowing down the humanitarian aid, he's also a dictator and a tyrant that oppresses his own people. We have always fought alongside the Egyptian people to help them gain freedom and obtain justice.



Update: *https://www.incometax.gov.eg http://www.cairo.gov.eg/* ...

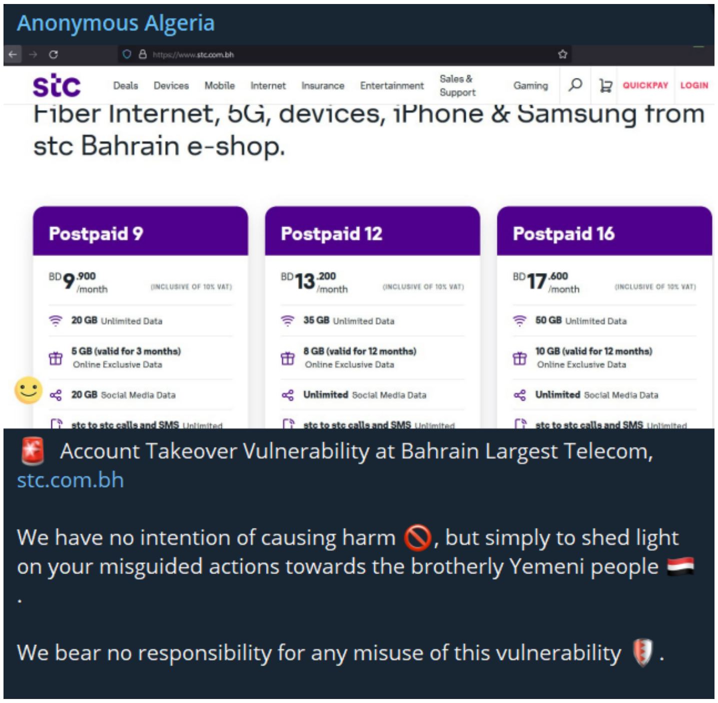
Both targets are still offline for more than 20 hours.

Most likely they shutdown their system and services to make investigations about the situation

There is a database contains 109 million Egyptian personal information like first-last name, address, Identity and phone numbers. But as you know, #Anonymous targets government and not the citizens. We stand with you guys. F##k Govs

Against Bahrain

The US and the UK, along with other countries, conducted joint strikes on Houthi targets in Yemen. The strikes aimed to weaken the Iran-backed militia that has been targeting international ships in the Red Sea in response to the Israel-Hamas conflict. Bahrain's silence on the matter has irked hacktivists.



Anonymous Algeria

Fiber Internet, 5G, devices, iPhone & Samsung from stc Bahrain e-shop.

Postpaid 9	Postpaid 12	Postpaid 16
BD 9.900 /month (INCLUSIVE OF 10% VAT)	BD 13.200 /month (INCLUSIVE OF 10% VAT)	BD 17.600 /month (INCLUSIVE OF 10% VAT)
20 GB Unlimited Data	35 GB Unlimited Data	50 GB Unlimited Data
5 GB (valid for 3 months) Online Exclusive Data	8 GB (valid for 12 months) Online Exclusive Data	10 GB (valid for 12 months) Online Exclusive Data
20 GB Social Media Data	Unlimited Social Media Data	Unlimited Social Media Data
stc to stc calls and SMS Unlimited	stc to stc calls and SMS Unlimited	stc to stc calls and SMS Unlimited

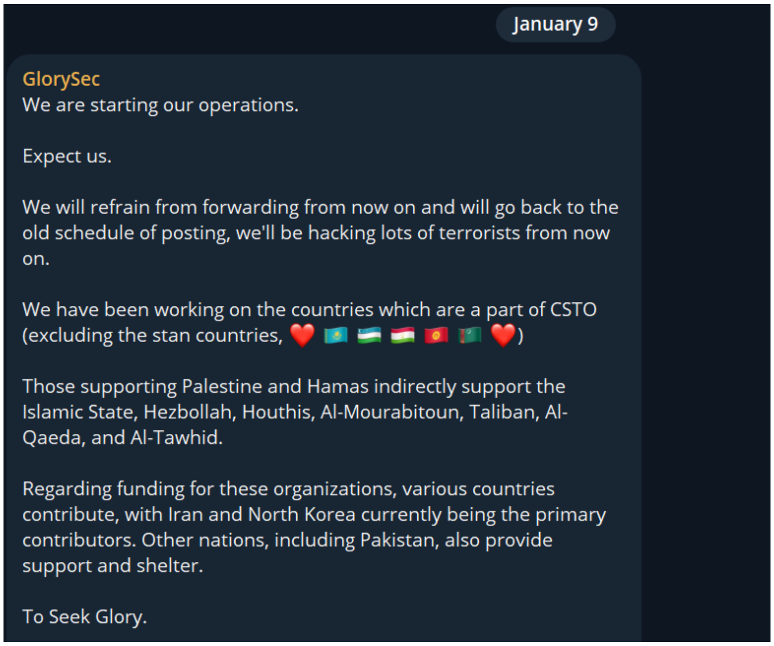
🚨 Account Takeover Vulnerability at Bahrain Largest Telecom, stc.com.bh

We have no intention of causing harm 🚫, but simply to shed light on your misguided actions towards the brotherly Yemeni people 🇾🇪 .

We bear no responsibility for any misuse of this vulnerability 🛡️.

Hackers Supporting Israel

The hacktivist group Glorysec issued a warning, indirectly stating that countries supporting Hamas and other terrorist groups in Palestine will be heavily targeted.



January 9

GlorySec
We are starting our operations.

Expect us.

We will refrain from forwarding from now on and will go back to the old schedule of posting, we'll be hacking lots of terrorists from now on.

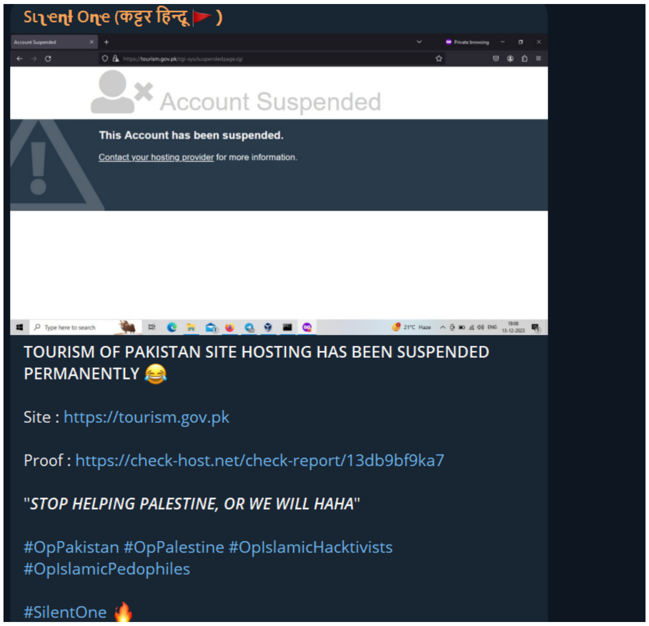
We have been working on the countries which are a part of CSTO (excluding the stan countries, ❤️🇰🇿🇺🇿🇹🇯🇰🇬🇹🇲❤️)

Those supporting Palestine and Hamas indirectly support the Islamic State, Hezbollah, Houthis, Al-Mourabitoun, Taliban, Al-Qaeda, and Al-Tawhid.

Regarding funding for these organizations, various countries contribute, with Iran and North Korea currently being the primary contributors. Other nations, including Pakistan, also provide support and shelter.

To Seek Glory.

Hackers from India have also joined the fray, engaging in DDoS attacks and defacing websites of countries supporting Palestine in the conflict. Below is an image depicting an Indian group attacking a Pakistani website for backing Palestine.



Sılent One (कट्टर हिन्दू🚩)

Account Suspended

This Account has been suspended.

Contact your hosting provider for more information.

TOURISM OF PAKISTAN SITE HOSTING HAS BEEN SUSPENDED PERMANENTLY 😂

Site : https://tourism.gov.pk

Proof : https://check-host.net/check-report/13db9bf9ka7

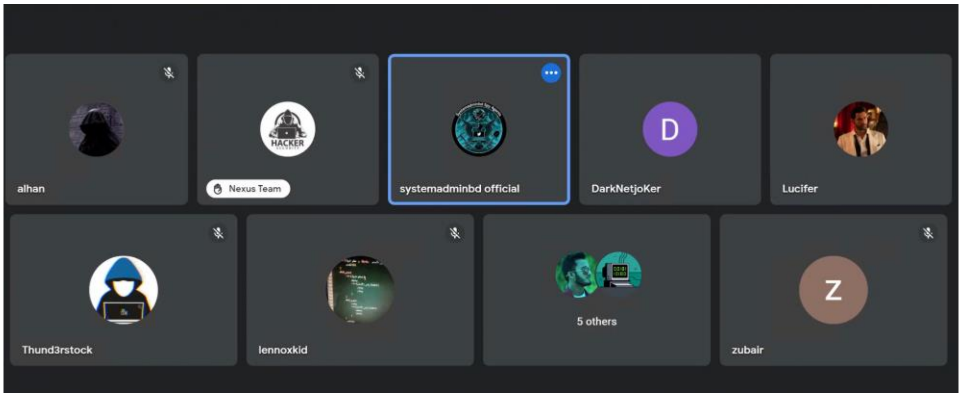
"*STOP HELPING PALESTINE, OR WE WILL HAHA*"

#OpPakistan #OpPalestine #OpIslamicHacktivists #OpIslamicPedophiles

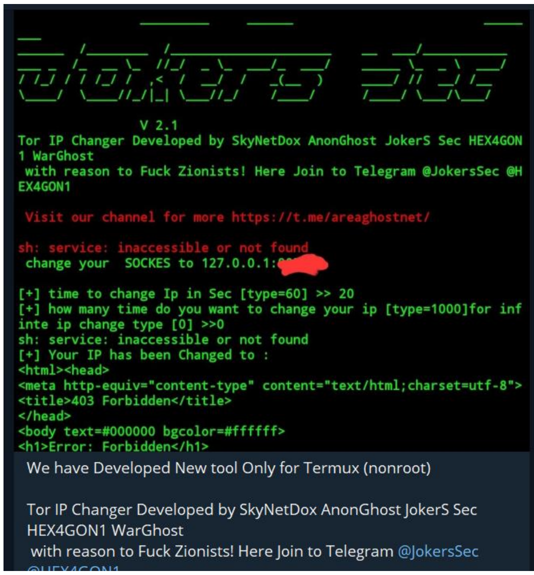
#SilentOne 🔥

Training and Tool Sharing

CYFIRMA researchers obtained covert access to a meeting organized by hacktivist group; SystemadminBD, addressing queries from its users, such as how to search for and exploit vulnerabilities.



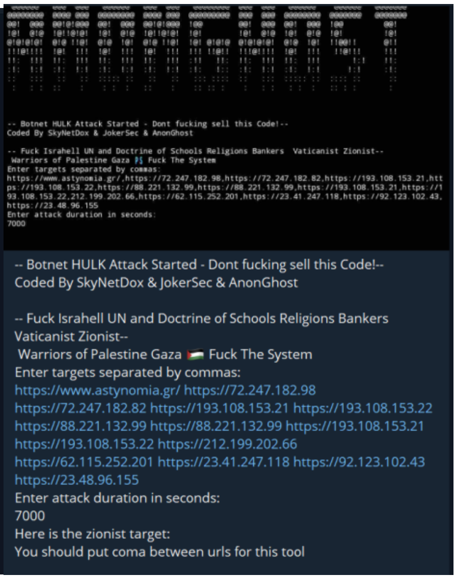
The team has also observed numerous in-house tools and DDoS software (both free and paid) created by hacktivists. These tools are shared on platforms like Telegram and GitHub, and they come in both command-line versions and versions compatible with Termux on Android devices. Since Termux is easily installable on any Android phone, and with step-by-step instructions provided, it enables users to participate in disruptive activities, causing slowdowns or disruptions to organizations.



```
                  V 2.1
Tor IP Changer Developed by SkyNetDox AnonGhost JokerS Sec HEX4GON
1 WarGhost
 with reason to Fuck Zionists! Here Join to Telegram @JokersSec @H
EX4GON1

 Visit our channel for more https://t.me/areaghostnet/

sh: service: inaccessible or not found
 change your  SOCKES to 127.0.0.1:[redacted]

[+] time to change Ip in Sec [type=60] >> 20
[+] how many time do you want to change your ip [type=1000]for inf
inte ip change type [0] >>0
sh: service: inaccessible or not found
[+] Your IP has been Changed to :
<html><head>
<meta http-equiv="content-type" content="text/html;charset=utf-8">
<title>403 Forbidden</title>
</head>
<body text=#000000 bgcolor=#ffffff>
<h1>Error: Forbidden</h1>
```

We have Developed New tool Only for Termux (nonroot)

Tor IP Changer Developed by SkyNetDox AnonGhost JokerS Sec HEX4GON1 WarGhost
with reason to Fuck Zionists! Here Join to Telegram @JokersSec



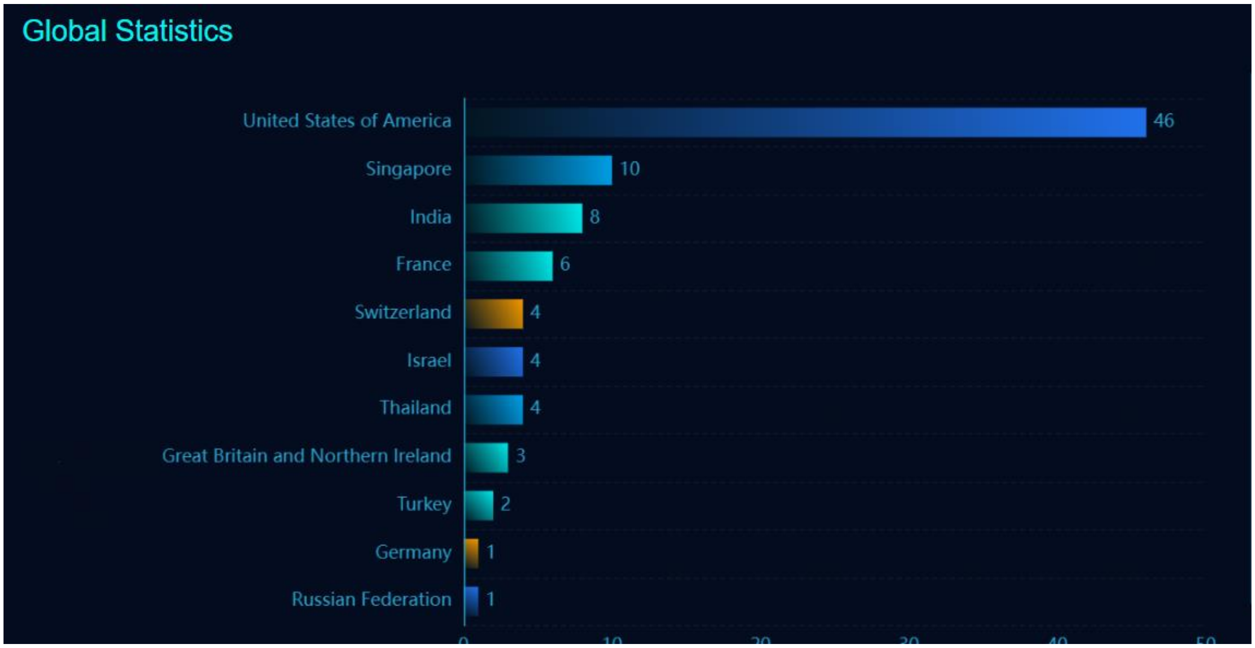
```
-- Botnet HULK Attack Started - Dont fucking sell this Code!--
Coded By SkyNetDox & JokerSec & AnonGhost

-- Fuck Israhell UN and Doctrine of Schools Religions Bankers  Vaticanist Zionist--
 Warriors of Palestine Gaza 🇵🇸 Fuck The System
Enter targets separated by commas:
https://www.astynomia.gr/,https://72.247.182.98,https://72.247.182.82,https://193.108.153.21,htt
ps://193.108.153.22,https://88.221.132.99,https://88.221.132.99,https://193.108.153.21,https://1
93.108.153.22,212.199.202.66,https://62.115.252.201,https://23.41.247.118,https://92.123.102.43,
https://23.48.96.155
Enter attack duration in seconds:
7000
```

-- Botnet HULK Attack Started - Dont fucking sell this Code!--
Coded By SkyNetDox & JokerSec & AnonGhost

-- Fuck Israhell UN and Doctrine of Schools Religions Bankers Vaticanist Zionist--
Warriors of Palestine Gaza 🇵🇸 Fuck The System
Enter targets separated by commas:
https://www.astynomia.gr/ https://72.247.182.98
https://72.247.182.82 https://193.108.153.21 https://193.108.153.22
https://88.221.132.99 https://88.221.132.99 https://193.108.153.21
https://193.108.153.22 https://212.199.202.66
https://62.115.252.201 https://23.41.247.118 https://92.123.102.43
https://23.48.96.155
Enter attack duration in seconds:
7000
Here is the zionist target:
You should put coma between urls for this tool

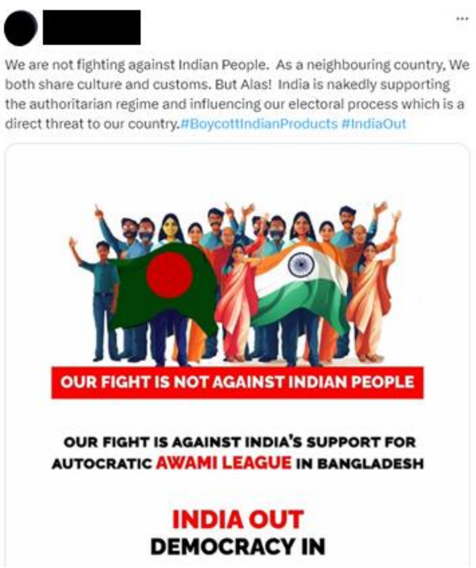
While using an asset’s exposure tool and by conducting specific queries, it's evident that hacktivist groups have launched cyber-attacks on numerous countries in support of – or in the guise of supporting – the Palestine conflict. It’s noteworthy that multiple sources are available to track websites defacement, providing a glimpse into the global cyber vandalism of websites around the world.

Body= ”hacked” && body=”savepalestine”



Recent Heat

A campaign called "India Out" has come into force and is supported by opposition parties and some civilians within Bangladesh. They claim that the Indian government interfered in Bangladesh's recent election, where Prime Minister Sheikh Hasina's Awami League won a fourth term. The opposition party boycotted the polls, and now the hashtag #IndiaOut is trending, with hackers from Bangladesh and similar groups preparing to launch attacks against India as a response.

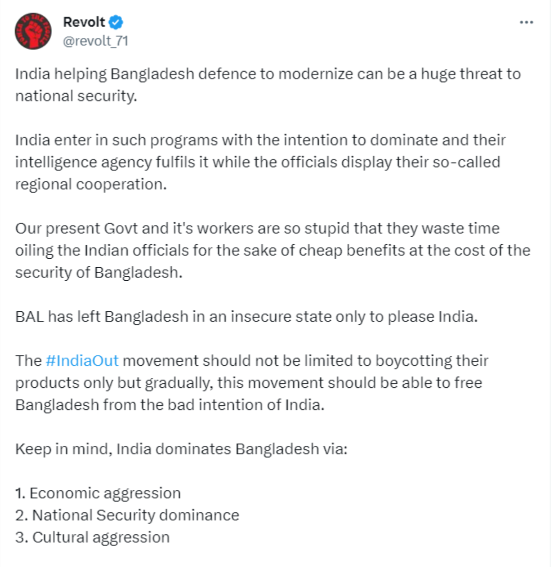

[redacted]

We are not fighting against Indian People. As a neighbouring country, We both share culture and customs. But Alas! India is nakedly supporting the authoritarian regime and influencing our electoral process which is a direct threat to our country.#BoycottIndianProducts #IndiaOut

OUR FIGHT IS NOT AGAINST INDIAN PEOPLE

OUR FIGHT IS AGAINST INDIA'S SUPPORT FOR AUTOCRATIC AWAMI LEAGUE IN BANGLADESH

INDIA OUT
DEMOCRACY IN


Revolt
@revolt_71

India helping Bangladesh defence to modernize can be a huge threat to national security.

India enter in such programs with the intention to dominate and their intelligence agency fulfils it while the officials display their so-called regional cooperation.

Our present Govt and it's workers are so stupid that they waste time oiling the Indian officials for the sake of cheap benefits at the cost of the security of Bangladesh.

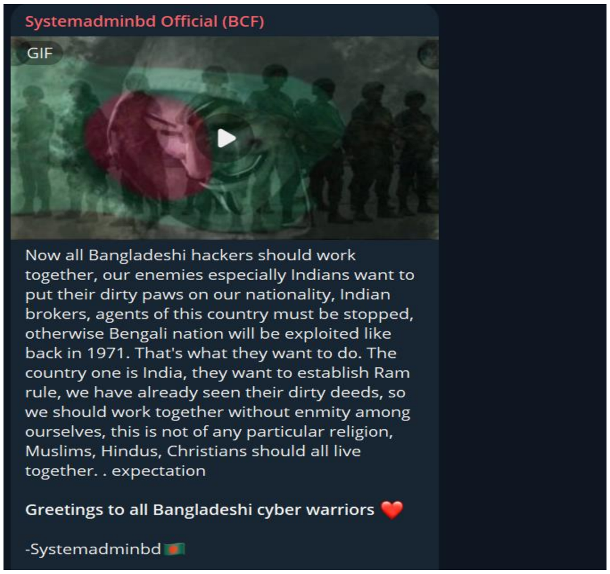
BAL has left Bangladesh in an insecure state only to please India.

The #IndiaOut movement should not be limited to boycotting their products only but gradually, this movement should be able to free Bangladesh from the bad intention of India.

Keep in mind, India dominates Bangladesh via:

1. Economic aggression
2. National Security dominance
3. Cultural aggression

SystemadminBD and other hacktivist groups like Sylhet Gang-SG are actively preparing attacks against Indian targets, indeed SystemadminBD have recently leaked data from private organizations, and provide free access to Indian government portals as part of their campaign.

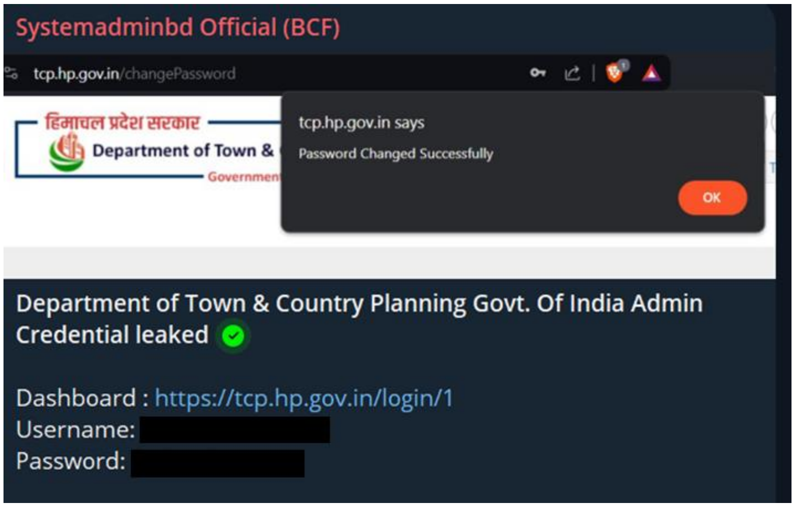

Systemadminbd Official (BCF)

Now all Bangladeshi hackers should work together, our enemies especially Indians want to put their dirty paws on our nationality, Indian brokers, agents of this country must be stopped, otherwise Bengali nation will be exploited like back in 1971. That's what they want to do. The country one is India, they want to establish Ram rule, we have already seen their dirty deeds, so we should work together without enmity among ourselves, this is not of any particular religion, Muslims, Hindus, Christians should all live together. . expectation

Greetings to all Bangladeshi cyber warriors ❤️

-Systemadminbd

The admin credentials for the Town & Country Planning Department of the Himanchal Government are provided freely on SystemadminBD Telegram channel.



Systemadminbd Official (BCF)

tcp.hp.gov.in says

Password Changed Successfully

Department of Town & Country Planning Govt. Of India Admin Credential leaked ✓

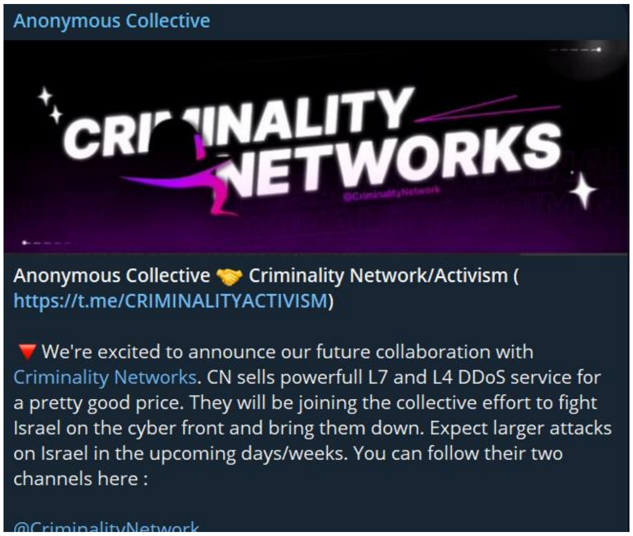
Dashboard : https://tcp.hp.gov.in/login/1
Username: [redacted]
Password: [redacted]

In a recent conversation with an alleged spokesperson of the hacktivist network; Sylhet Gang, we inquired about their views on India:

Sylhet Gang-SG Spokesperson: "the Indians are showing aggression along the Bangladeshi border, so our other admin moderators held a meeting, **and we are waging a war against India now."**

EXTERNAL THREAT LANDSCAPE MANAGEMENT

- In recent conversations with multiple hacktivist groups:
  - They claim to support Palestine and use hacktivism as a means to raise awareness.
  - They operate with the support of more than 30 teams and keep their skills and tools private.
  - The spokesperson claimed that they have targeted countries like the UK, South Korea, India, and Germany, striking in response to various causes.
  - The groups assert they do not monetize their operations and work for free, emphasizing a commitment to their cause.
  - When asked about Saudi Arabia's stance on Israel, the spokesperson criticized the Saudi rulers as "hypocrites". They declared that more attacks will come as long as the groups exist.
- Anonymous Collective recently joined forces with Criminality Networks; a group that sells DDoS services. This collaboration aims to impact Israel and its allies in the cyber realm by unleashing powerful DDoS attacks.



Anonymous Collective

Anonymous Collective 🤝 Criminality Network/Activism (https://t.me/CRIMINALITYACTIVISM)

🔻 We're excited to announce our future collaboration with Criminality Networks. CN sells powerfull L7 and L4 DDoS service for a pretty good price. They will be joining the collective effort to fight Israel on the cyber front and bring them down. Expect larger attacks on Israel in the upcoming days/weeks. You can follow their two channels here :

@CriminalityNetwork

- A statement jointly issued by Australia, Bahrain, Canada, the Netherlands, the United Kingdom, and the United States about additional strikes against the Houthis in Yemen could potentially trigger more hacktivist activity.

  As observed in this report, these hacktivists, who support Yemen and Palestine, might be preparing further attacks, having already targeted the USA, Bahrain, and the UK.

- With moderate confidence, we caution that they are likely to extend their efforts to disrupt upcoming events, such as the Paris Olympics in 2024. In doing so, they may attempt to DDOS or deface websites of hotels, food stores or ticketing websites and others to promote their motives and ongoing campaigns.

Below is a list of hacktivist groups known to be targeting Israel's allies (please note that this is not an exhaustive list):

- Riski haxor
- Gaza children hackers group
- Kromsec
- Anonymous Arabic
- 313 team
- Turkhackteam
- Esteem restoration eagle
- Areaghostnet
- ETHERSEC TEAM CYBER
- Nusantara
- GARUDA_CYBER_OPERATION
- GHOST_[6669]_TEAM
- C.E.S
- GHOST_OF_PALESTINE
- Anonymous_Global
- Anonymous_Muslims
- GBAnon17
- Anon Black Flag
- Fredens Of Security
- Ganosec Team
- Cyber Sederhana Team
- Bandung Cyber Team
- LEGION7_HACKERS_TEAM
- Jakarta Ghost
- Esteem Restoration Eagle
- KETAPANG_GRAY_HAT
- HIZBULLAH_CYB3R_TEAM
- IXP666SECTEAM
- FromLammerToMastah
- SukowonoBlackHat
- Jambi_Cyber_Team
- TigerGroupCommunity
- Union_Of_Greats
- CIPINANG_BLACKHAT
- KuninganExploiter
- ZERO-XPLOITS-ID
- 5UL4WES1_TENG4H_BL4CKHT
- STATE_OF_SECURITY
- TEAM_HEROX
- IRoX_TEAM
- Anonymous Africa

APT Groups

- Cyber Av3ngers
- Agrius/Agonizing Serpens/ DEV-0227

Attacking Palestine's Allies

- Garunops
- Termux Israel
- Israel Cyber Defense
- Network nine
- Team UCC
- Team DarkCyber Warrior
- Team BlackDragonsec
- Team NWH Security
- KERALA CYBER BLACK SQUAD
- Kerala Cyber Xtractors
- INDIAN CYBER SANATANI
- Silent-one
- IndianCyberForce
- Hacktivist Vanguard

CONCLUSION

Whenever there are regional conflicts, we have seen hacker groups getting involved by attacking the websites of countries that oppose their agenda. For example, Indian hackers targeted countries like Bangladesh, Pakistan, and Turkey to support Israel, while hackers from Bangladesh, Pakistan, Turkey target the USA, UK, France, India, Bahrain, and other Israeli allies, providing training and tools to carry out attacks and reputational damage. Conflicts such as these highlight the importance of nations maintaining strong cybersecurity measures, especially if they have different geopolitical stances to those in their region.

Hacktivist attacks can lack sophistication, however, and don't impact businesses unless a critical service in a major supply chain gets targeted for several days in a row, and defacement attacks are performed on websites of small businesses which lack basic cybersecurity hygiene. These attacks can be effective if carried out against entities like reservation websites or tracking consignment sites, for instance, we have observed a similar case regarding Indian post's website, which was down for 3 days, resulting in widespread customer dissatisfaction.

RECOMMENDATIONS

Strategic Recommendations

- **Threat intelligence sharing:** encourage regional and international threat intelligence sharing to improve awareness of ongoing threats. Collaborative efforts can help predict and mitigate attacks more effectively.
- **Diplomatic engagement:** governments should engage in diplomatic discussions to de-escalate geopolitical tensions, reducing the motivation for hacktivist activities at their source.
- **Public awareness campaigns:** launch public awareness campaigns to educate citizens about cyber threats, including phishing and disinformation. An informed public is less susceptible to hacktivist propaganda.
- **International norms and agreements:** advocate for international agreements and norms regarding cyber warfare. Establishing clear rules of engagement in cyberspace can deter hacktivist groups.

Management Recommendations

- **Cybersecurity training:** invest in training and awareness programs for employees and government officials. A well-informed workforce is a critical defense against social engineering attacks.
- **Resource allocation:** allocate resources for enhancing critical infrastructure security. Ensure that budgetary support is provided for cybersecurity measures that protect essential services.
- **Regular drills and exercises:** conduct regular cybersecurity drills and exercises to test incident response plans and identify areas for improvement.
- **Collaborative partnerships:** foster partnerships with cybersecurity firms and organizations that can provide threat intelligence, incident response support, and security expertise.

Tactical Recommendations

- **Enhance DDoS mitigation:** given the prevalence of DDoS attacks in this cyber conflict, organizations and governments should invest in robust DDoS mitigation technologies and strategies. Employing real-time traffic analysis and traffic scrubbing can help minimize service disruptions.
- **Regular vulnerability scanning:** continuous vulnerability scanning of critical infrastructure is crucial. Identifying and addressing vulnerabilities promptly reduces the risk of exploitation by hacktivist groups.

- **Multi-factor authentication (MFA):** implement MFA for all privileged accounts and critical systems, including RDPs and VNCs. This adds an extra layer of protection against unauthorized access.
- **Incident response planning:** develop and regularly update an incident response plan. Ensure that security teams are well-prepared to respond to cyber incidents swiftly and effectively.

CYFIRMA
DECODING THREATS

CYFIRMA is an external threat landscape management platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver early warning, personalized, contextual, outside-in, and multi-layered insights. Our cloud-based AI and ML-powered analytics platform provides the hacker's view with deep insights into the external cyber landscape, helping clients prepare for impending attacks. CYFIRMA is headquartered in Singapore with offices across APAC, US and EMEA. The company is funded by Goldman Sachs, Zodius Capital, Z3 Partners, OurCrowd and L&T Innovations Fund.