BREAKING CYBERSECURITY NEWS: INDOHAXSEC – EMERGING INDONESIAN HACKTIVIST GROUP INTENSIFIES CYBERATTACKS

Vairav Cyber Security News Report

Date: March 19, 2024

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A new report by Arctic Wolf Labs highlights the growing activities of INDOHAXSEC, an Indonesia-based hacktivist group engaged in DDoS attacks, ransomware deployments, and website defacements. Since its establishment in October 2024, the group has carried out politically and ideologically motivated cyberattacks, primarily targeting entities perceived as supporting Israel. Additionally, INDOHAXSEC has allied with the pro-Russian NoName057(16) hacktivist group, indicating potential geopolitical motivations. The group leverages GitHub repositories, Telegram channels, and social media platforms to distribute malware, coordinate attacks, and spread propaganda.

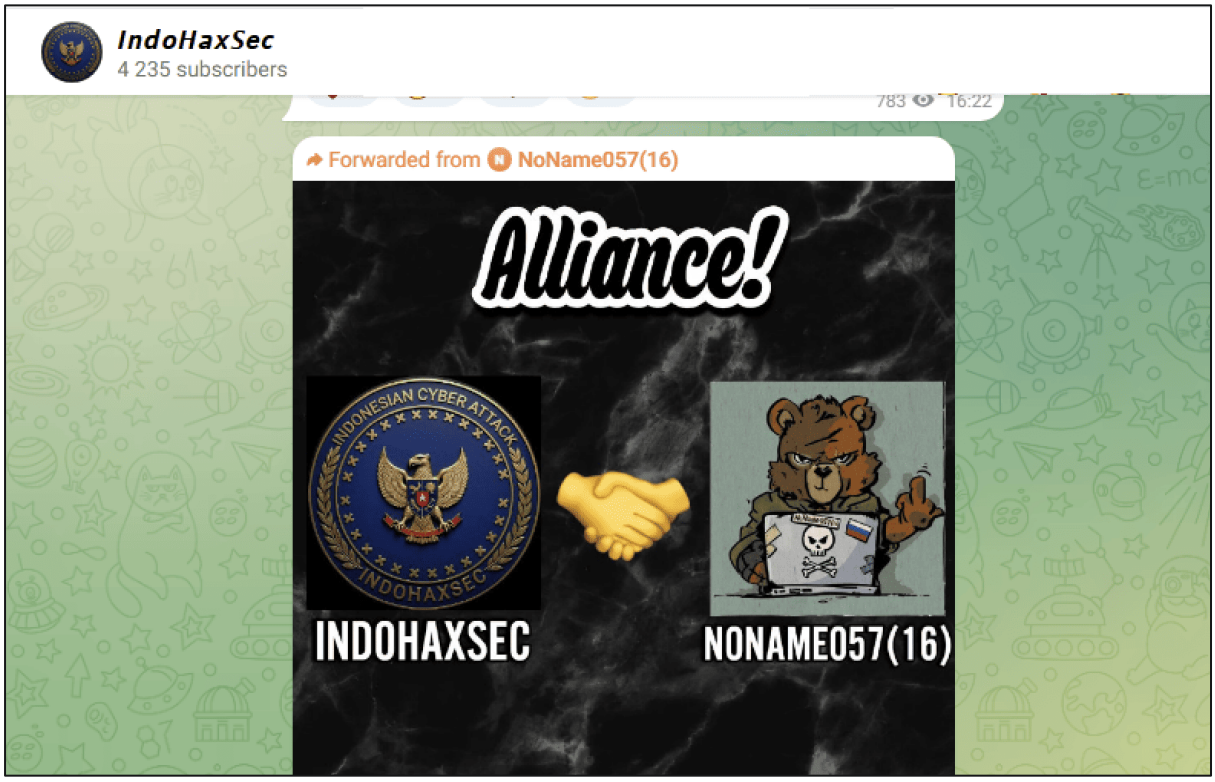


Figure 1: INDOHAXSEC Telegram channel announcing their partnership with NoName057(16)

INCIDENT DETAILS

AFFILIATED REGIONAL HACKTIVIST GROUPS

These groups share members, tools, or overlapping tactics with INDOHAXSEC, contributing to its evolving cyber activities.

- AnonBlackFlag
- Hacktivists Indonesia
- PaluAnonCyber

- KUNINGAN EXPLOITER
- CIPINANG BL4CK
- FoxCrack-ID
- HIZBULLAH CYB3R TEAM
- Esteem Restoration Eagle
- QLAVER XPLOIT SECURITY

HACKTIVIST ATTACKS AND TARGETED SECTORS

INDOHAXSEC's cyberattacks focus on politically motivated disruptions targeting both government and private organizations. Their primary methods include:

- **DDoS Attacks** – Overloading targeted websites and networks to cause downtime. Recent attacks have impacted financial institutions, government websites, and telecommunications providers in Southeast Asia.
- **Website Defacements** – The group replaces website content with political messages, slogans, or digital graffiti supporting their causes. Malaysia's NC4 issued an alert after repeated defacements of Malaysian government sites.
- **Ransomware Deployments** – INDOHAXSEC members have been linked to ExorLock ransomware, a strain they previously used under the alias AnonBlackFlag. ExorLock was allegedly deployed against an Indian government website during the May 2024 elections.
- **Hack-and-Leak Operations** – The group steals and leaks sensitive data from victim organizations. Most recently, INDOHAXSEC claimed to have breached Solace Infotech Pvt. Ltd. in India, leaking 200,000 records from its PhpMyAdmin database.

USE OF AI IN MALWARE DEVELOPMENT

INDOHAXSEC is suspected of leveraging AI tools like ChatGPT to improve their malware. The group's TikTok videos reveal interest in file encryption and altering permissions, with some timestamps aligning with the GitHub commit history of Dancokware malware.

- **Dancokware Malware** – A website-destroying PHP script capable of encrypting entire web directories. It was promoted on TikTok by INDOHAXSEC members.

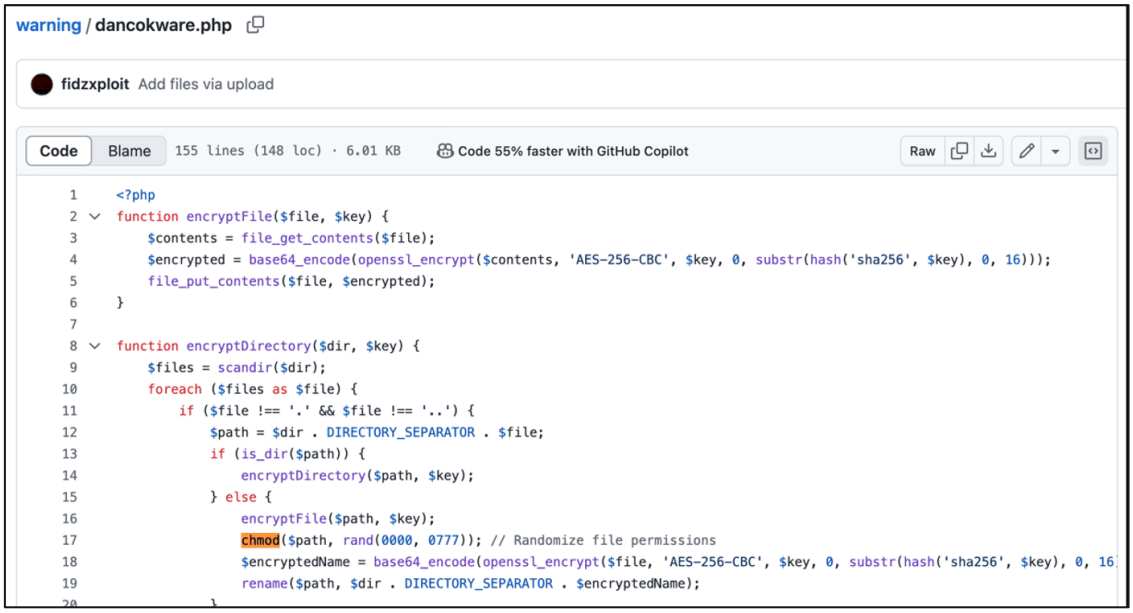


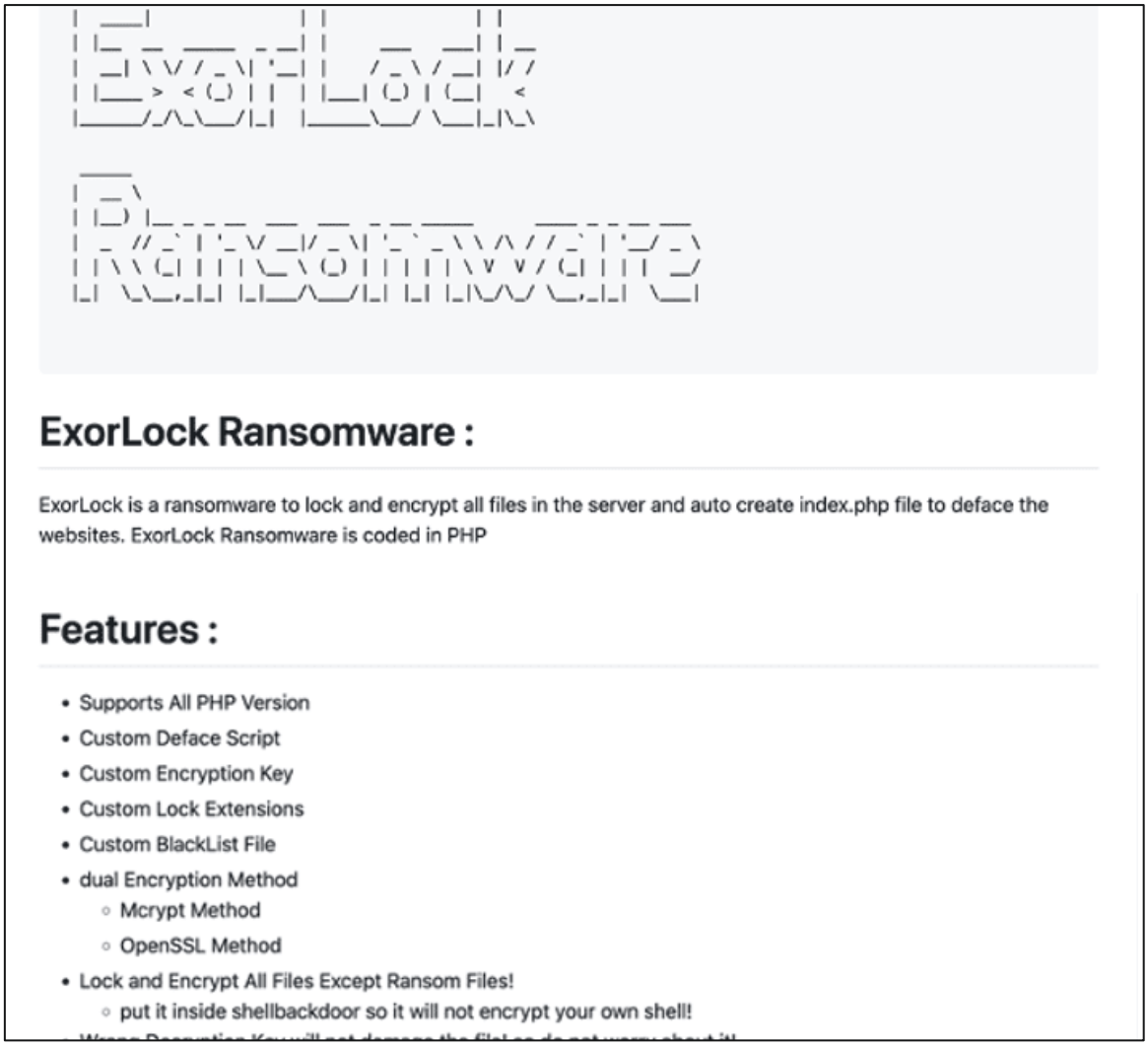
Figure 2: Dancokware Malware – File Encryption and Chmod

- **ChatGPT Abuse** – While unconfirmed, threat actors using AI for malware generation pose an increasing risk, lowering technical barriers for cybercriminals.

CUSTOM MALWARE REPOSITORY ON GITHUB

INDOHAXSEC maintains a GitHub repository containing custom tools for cyberattacks. The repository includes:

- **Xss_Fucker** – A Python tool used to identify cross-site scripting (XSS) vulnerabilities on websites.
- **DDoS Scripts** (NUKLIR, RUDAL) – Used for launching large-scale denial-of-service attacks.
- **Backdoor Shells** (Rudal-shell) – PHP scripts enabling remote access to compromised web servers.
- **Ark-Cheat-Detector** – A compromised anti-cheat tool for ARK: Survival Evolved, modified to install a PHP-based backdoor.
- **ExorLock Ransomware** – Custom ransomware is written in Go Language, encrypting files with ChaCha20 encryption.



ExorLock Ransomware :

ExorLock is a ransomware to lock and encrypt all files in the server and auto create index.php file to deface the websites. ExorLock Ransomware is coded in PHP

Features :

- Supports All PHP Version
- Custom Deface Script
- Custom Encryption Key
- Custom Lock Extensions
- Custom BlackList File
- dual Encryption Method
  - Mcrypt Method
  - OpenSSL Method
- Lock and Encrypt All Files Except Ransom Files!
  - put it inside shellbackdoor so it will not encrypt your own shell!

Figure 3: ExorLock Ransomware README

SOCIAL MEDIA OPERATIONS

INDOHAXSEC uses Telegram, TikTok, and X (formerly Twitter) for cyber operations and propaganda:

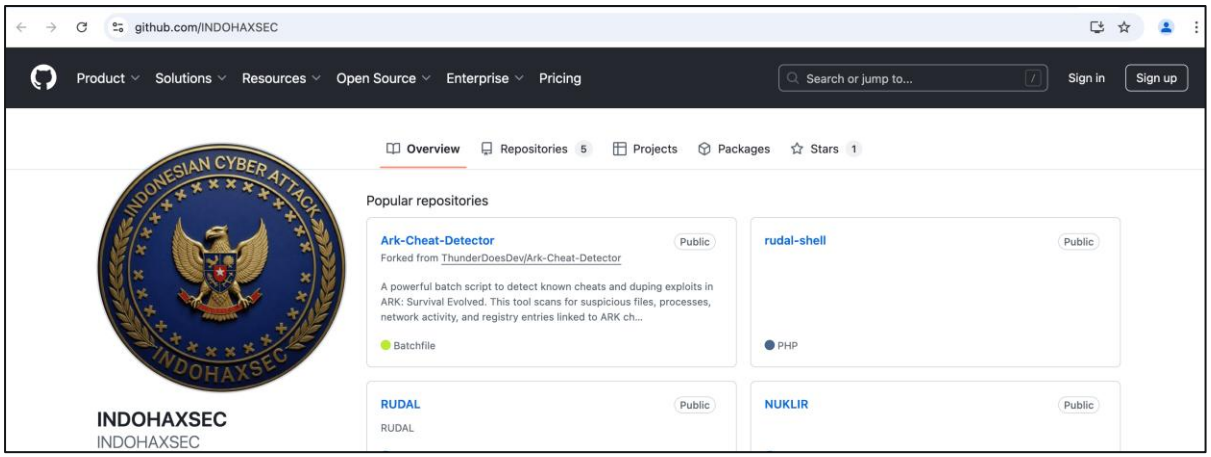


Figure 4: INDOHAXSEC's official GitHub page

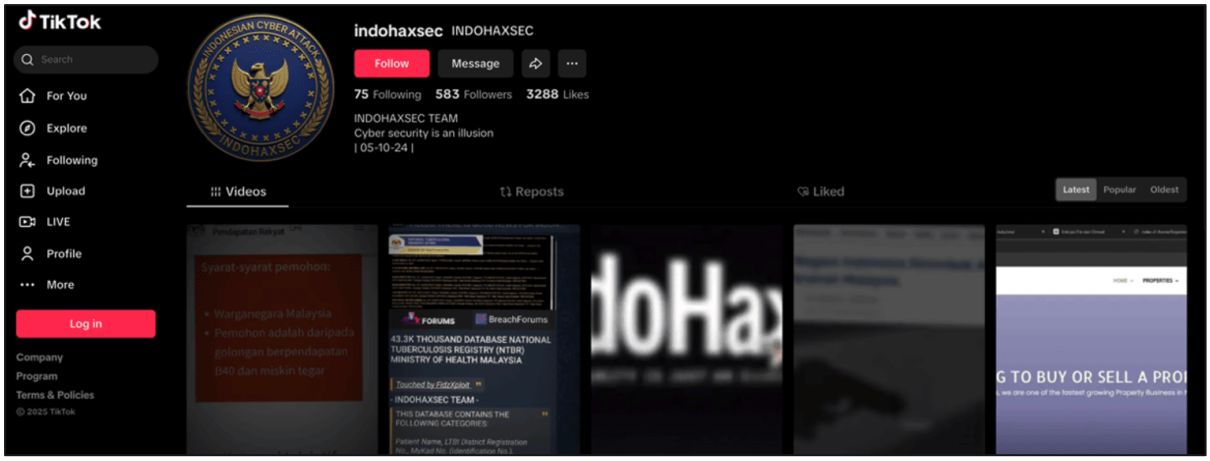


Figure 5: INDOHAXSEC's TikTok Social Media channel

- **Telegram Coordination** – Their main channel has over 4,000 subscribers, used for communication, planning, and publicizing attacks.

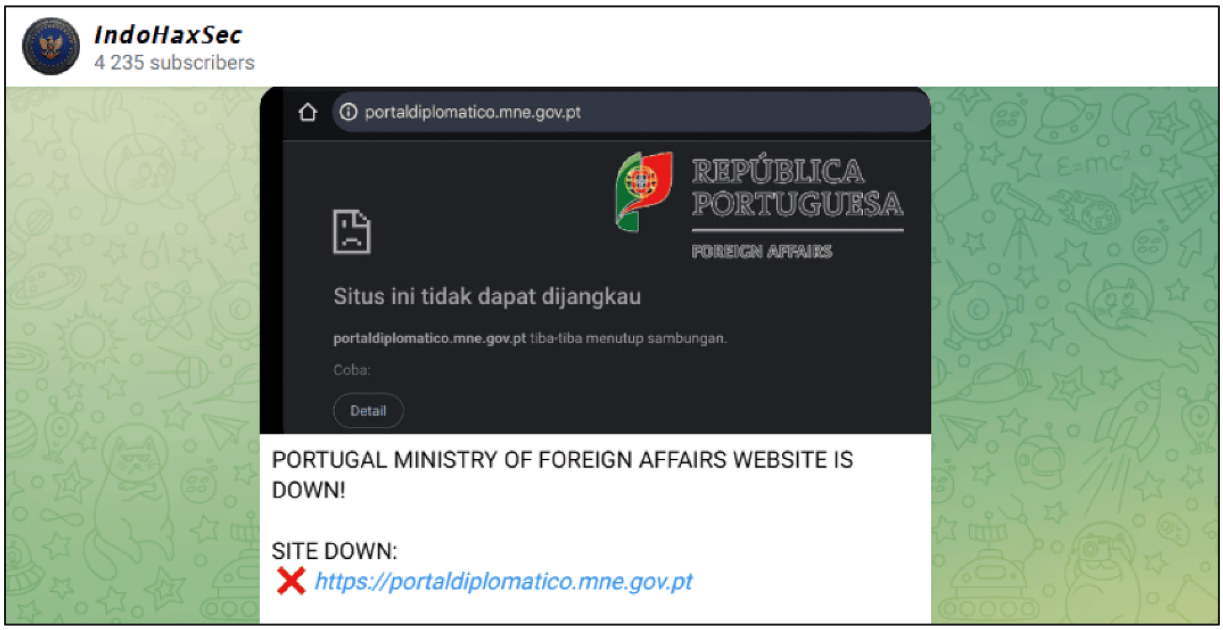


Figure 6: INDOHAXSEC Telegram Channel

- **Social media** – The group leaked personal details of Malaysian officials, escalating tensions after the January 2025 fatal shooting of an Indonesian migrant worker by Malaysian authorities.
- **WannaCry 2.0 Claims** – INDOHAXSEC falsely claims to have developed a successor to the infamous 2017 WannaCry ransomware. No code samples have been verified, suggesting the claim is a publicity stunt to intimidate targets.

EXPANSION OF TARGETING & RETALIATORY ATTACKS

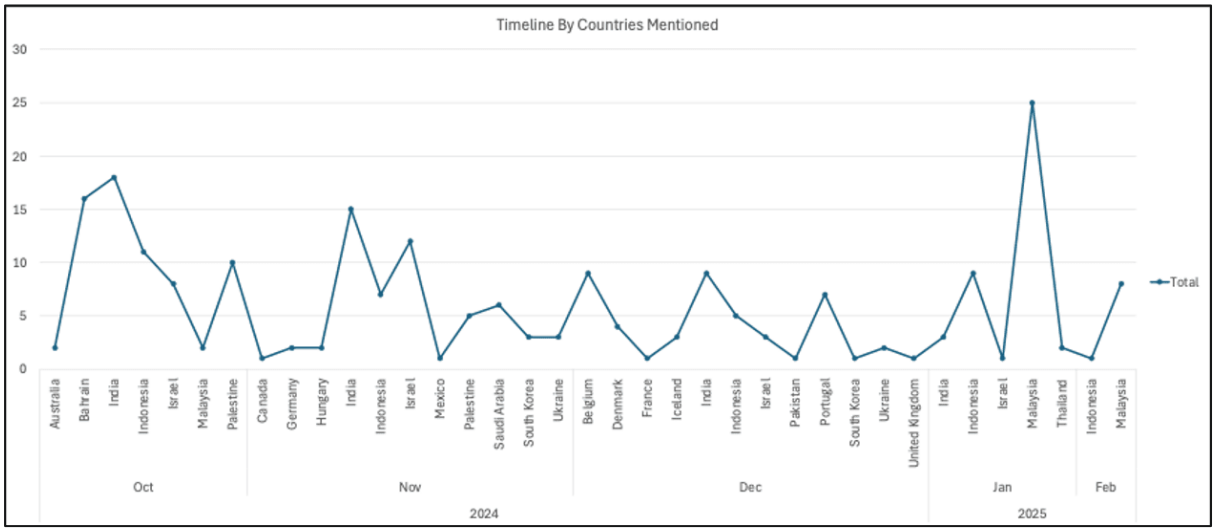


Figure 7: Countries most often mentioned on the group's Telegram

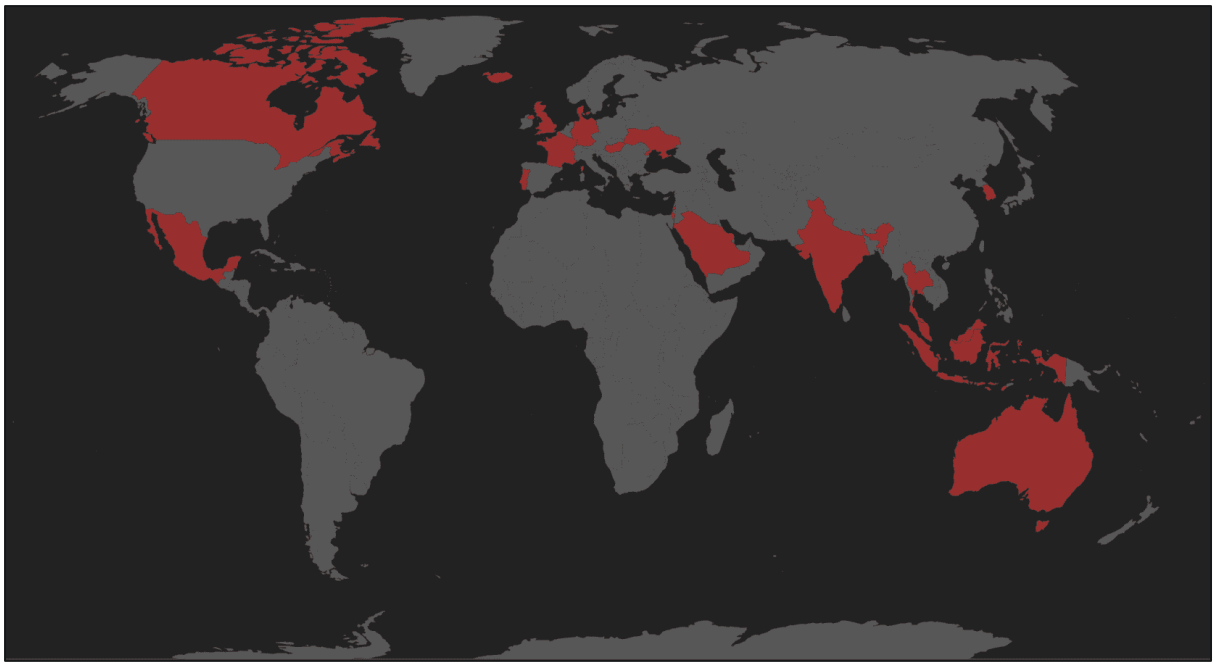


Figure 8: World map of countries targeted by INDOHAXSEC

INDOHAXSEC's attack patterns mirror real-world geopolitical tensions:

- **Pro-Palestinian Hacktivism** – The group frequently targets entities supporting Israel.
- **India & Malaysia Focus** – Malaysia's National Cyber Coordination and Command Center (NC4) issued an advisory in response to INDOHAXSEC's repeated cyberattacks on government agencies.
- **Retaliatory Threats** – The group temporarily paused attacks on Malaysia in February 2025 but warned they could release a large Malaysian government database if provoked.

INDICATORS OF COMPROMISE (IOCS)

cd8a7350b07311f2257eba7ed5d992cf7f00e869461f9a2c3c2003a05bfdcce0

9391014b5a567f4821603c97802c38d8f3053469f47533c57bcfdb787fd9cd57

09092c5061322e3cdc33e3eb4d8379f77ec20ff121acd42b159e87407e421a57

e9a2379991d7ad9f3031c9cd62eab9277b9a2d0179a066b36dd95737182574c8

3b1cb2248bf6b2c9cb493f6ef226a943042ccd8a5e98f4869c55a4efe0a0f835

ac9b107e35f7a8055bb4a556a1835b824f7b32bbc8af0c05dc67164678f25008

464087d09b85c0bbed20e5369264ae21537926da24efca8aed4136c70fe5b1e0

eae18c62dbb29bc6749347d410a16b190cb1b2fdaff6d8318ca9ecb5e572391d

efd85fd28bcf10f32f0ac934ee0e9e71d34a0cbae66ee83abad9a929c3ca91f9

9325343e22181eda59efce7b9d6a54c5565c1798337cb42f07a24dbe93f5b117

7fd271225602c021306c68157a2e17ace5f42853b4762c49f4d82ae8a4e2ebe3

02c3d44ec9a44558f516a5922b09b736c5786d2a675b89b2e86ce8f16e4041b6

0c5e744a5aefe6d6d432b85c33f92f2e2beb75af311421806acb550f766dda41

658f468bc8a762ebef233d284bccb97d64d5b214ea49d9c1cac8b9976ee6c3dc

f9a3f810fb81b3a605038d997341223eb6914aed4f13f4d93466906dc83b1942

1ba3ce9a93262e82a660b8b566134e08fa9680de8716a2893e4e4617086276f4

959cce59fc5d15540e348945b0a18516d9afb56b1f21fd2db4ed209e87cf2657

393bff0edb5c229064ba54343eb38ba1b301246caaa30c20021776c822383bf2

a5c8d558af0e8e3853cdd03be91dc7d915113a291466383005dbe1951809f663

49cf4ae0d9ffbfc0ff4918e34b1c5b066e62663eeee6da4d0fa91172850e03d6

a82e254ec16d3505322b487cfa2cc0f9e629ef72a4f474dbae81b1ec5bd7f2c2

b3a7f14df7b52a0acadc02c58d602bd21e28b7968621f9181531d4977e216ba1

CONCLUSION

INDOHAXSEC exemplifies how geopolitical tensions in the Indo-Pacific region fuel hacktivist activities. Focused on disruption, the group targets both government and private entities using a wide range of cyber tools. Organizations must enhance security, monitor threats, and adhere to cybersecurity best practices to mitigate risks, especially those previously targeted by the group. Continuous threat intelligence monitoring and collaboration with cybersecurity communities are crucial to staying ahead of evolving threats.

RECOMMENDED ACTIONS

Strategic Recommendations:

- Continuously monitor INDOHAXSEC's activities across platforms like GitHub, Telegram, and social media to identify potential threats early.
- Strengthen cyber resilience by implementing multi-layered defense strategies, including proactive threat intelligence and rapid incident response planning.
- Establish clear policies and security frameworks to mitigate the impact of hacktivist attacks, including DDoS, website defacements, and ransomware incidents.

Technical Recommendations:

- Deploy robust DDoS mitigation solutions, Web Application Firewalls (WAF), and Intrusion Prevention Systems (IPS) to prevent service disruptions and unauthorized access.
- Regularly update and patch all software, including CMS platforms, to eliminate vulnerabilities exploited in defacements and ransomware infections.
- Leverage advanced endpoint protection (EDR/XDR) and SIEM solutions to detect, investigate, and block malicious activities in real-time.
- Conduct regular threat-hunting exercises to identify suspicious network traffic, unauthorized logins, or unusual system modifications.

Operational & Awareness Recommendations:

- Educate staff on recognizing social engineering tactics, phishing emails, and malicious download attempts.
- Enforce role-based access controls (RBAC) and multi-factor authentication (MFA) to limit lateral movement within networks.
- Actively report and take down malicious domains, phishing pages, and compromised GitHub repositories linked to INDOHAXSEC.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://securityonline.info/indohaxsec-emerging-indonesian-hacktivist-collective-targets-southeast-asia/

https://arcticwolf.com/resources/blog/indohaxsec-emerging-indonesian-hacking-collective/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com