DATASHEET

CYBERCRIME THREATS TO THE TELECOMMUNICATIONS SECTOR

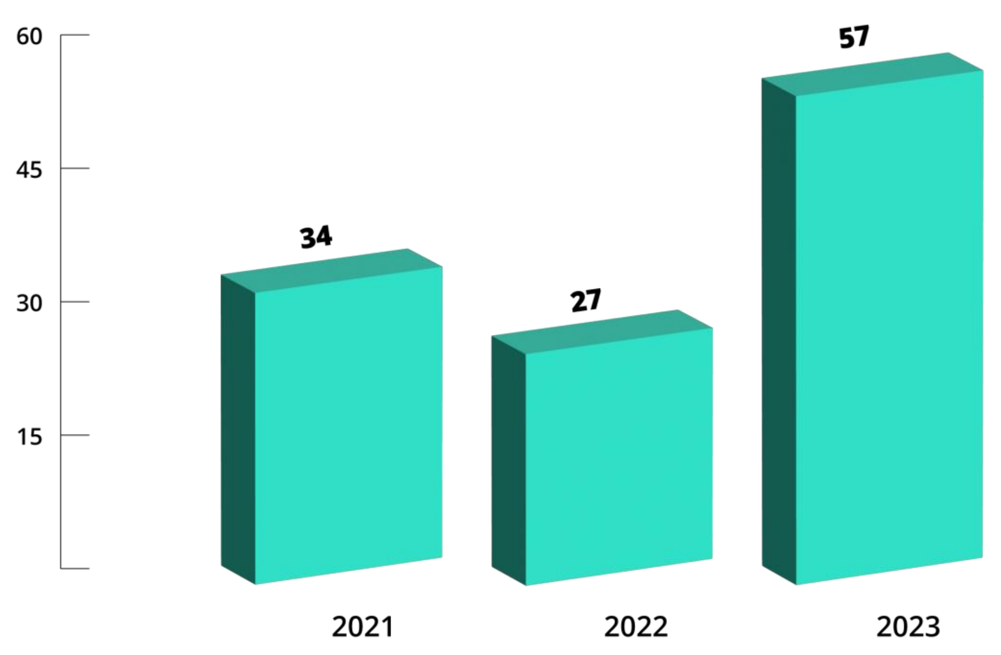
In our fast-paced connected world, the telecommunications sector remains an ideal target for cybercriminals. It involves a wide range of companies, from internet service providers (ISPs) to telephone, mobile, satellite corporations and more, providing opportunities to launch large-scale attacks that affect a wide range of customers and organizations. Moreover, disruptions in the telecom sector can cause significant social and economic impacts. For example, the Australian telecoms provider Optus had recently had a massive outage, which affected 40% of the country's population. This was the second incident after the company suffered a data breach in 2022, resulting in a leak of sensitive information of 10,000 Optus customers. This datasheet provides information about the persistent threats against the telecom sector.

MALWARE ATTACKS

Threat actors utilize diverse malware strains to target telecom companies. The most common malware in telecommunication networks was found to be a botnet malware that scans for vulnerable devices, a tactic associated with a variety of IoT botnets. Researchers found that malicious IoT botnet traffic targeting telecoms networks increased fivefold over 2022.

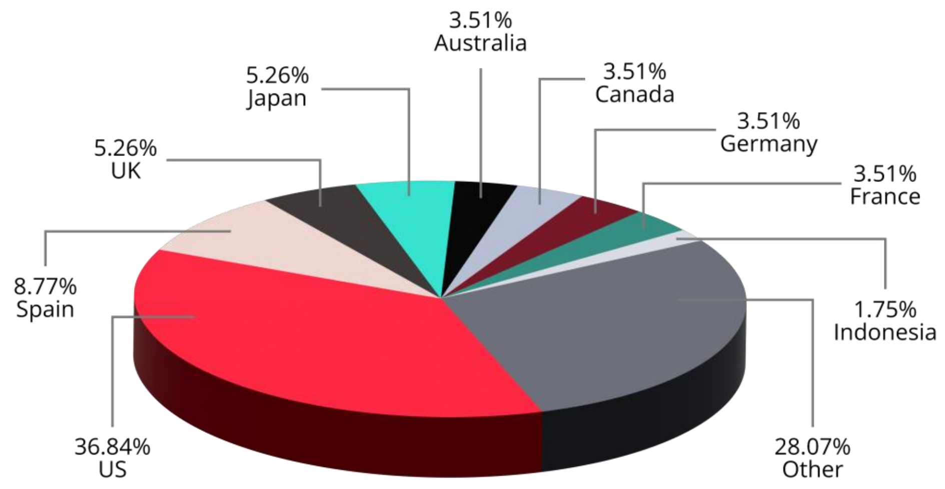
Ransomware actors are also targeting the telecommunication sector, aiming to deploy encrypting malware and steal information. KELA's analysis of ransomware victims and data leak activity shows that ransomware and extortion actors remained a persistent threat in 2023, impacting almost 60 victims, which is more than a two-fold increase compared to 2022, while the year is not yet over. The most targeted country is the US. Other top attacked countries are Spain, the UK, and Japan.

Ransomware attacks against the telecom sector



January 2023- October 2023

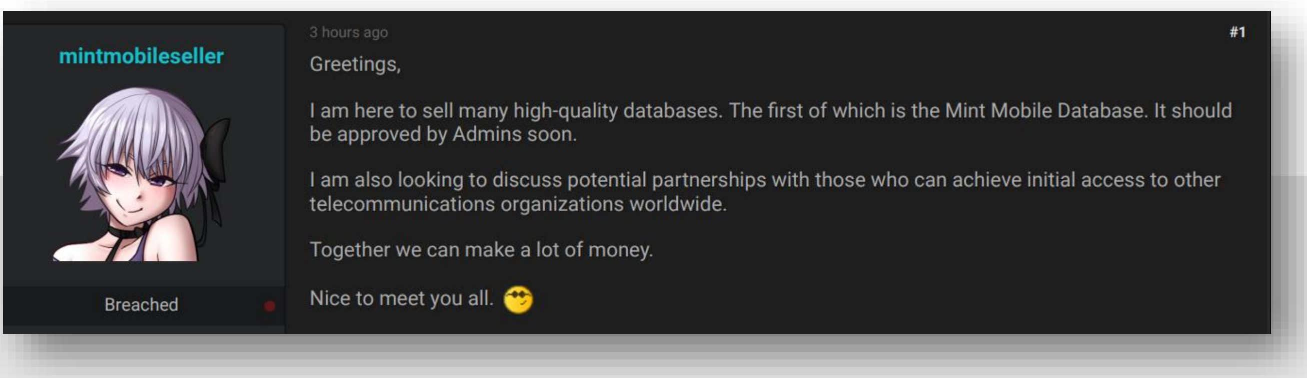
Top targeted countries in the telecom sector by ransomware actors



The most prolific ransomware groups targeting the telecom sector in 2023 were LockBit, Clop and Alphv, all spotted as the top actors targeting all industries in 2023.

NETWORK ACCESS SALES

Initial Access Brokers (IABs) play an important role in a ransomware-as-a-service supply chain by supplying access to compromised networks. Compromising telecom companies significantly expands future possibilities for a threat actor since telecom companies usually provide access to the internal data of customers and other enterprises. KELA identified around 55 network access listings to companies from the telecom sector for sale in 2023. The telecom sector is in the top 10 targeted sectors in 2023 by IABs.



mintmobileseller

3 hours ago

#1

Greetings,

I am here to sell many high-quality databases. The first of which is the Mint Mobile Database. It should be approved by Admins soon.

I am also looking to discuss potential partnerships with those who can achieve initial access to other telecommunications organizations worldwide.

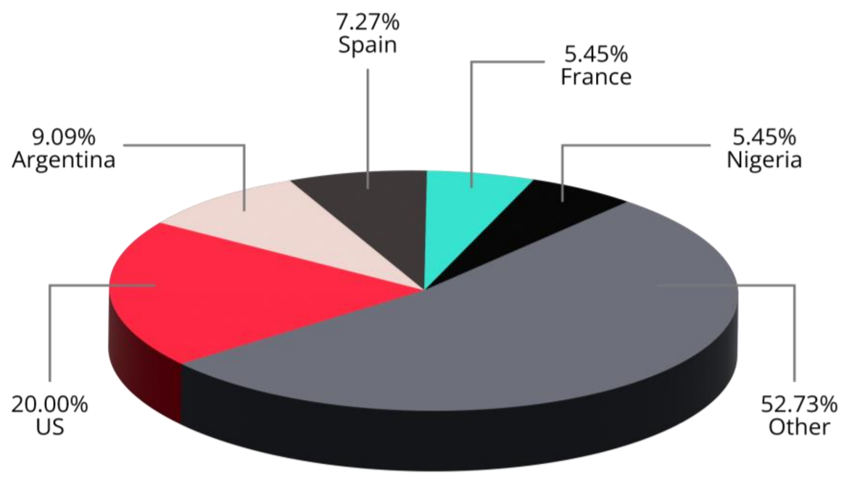
Together we can make a lot of money.

Nice to meet you all. 😎

Breached

An actor is looking for initial access to telecommunications companies

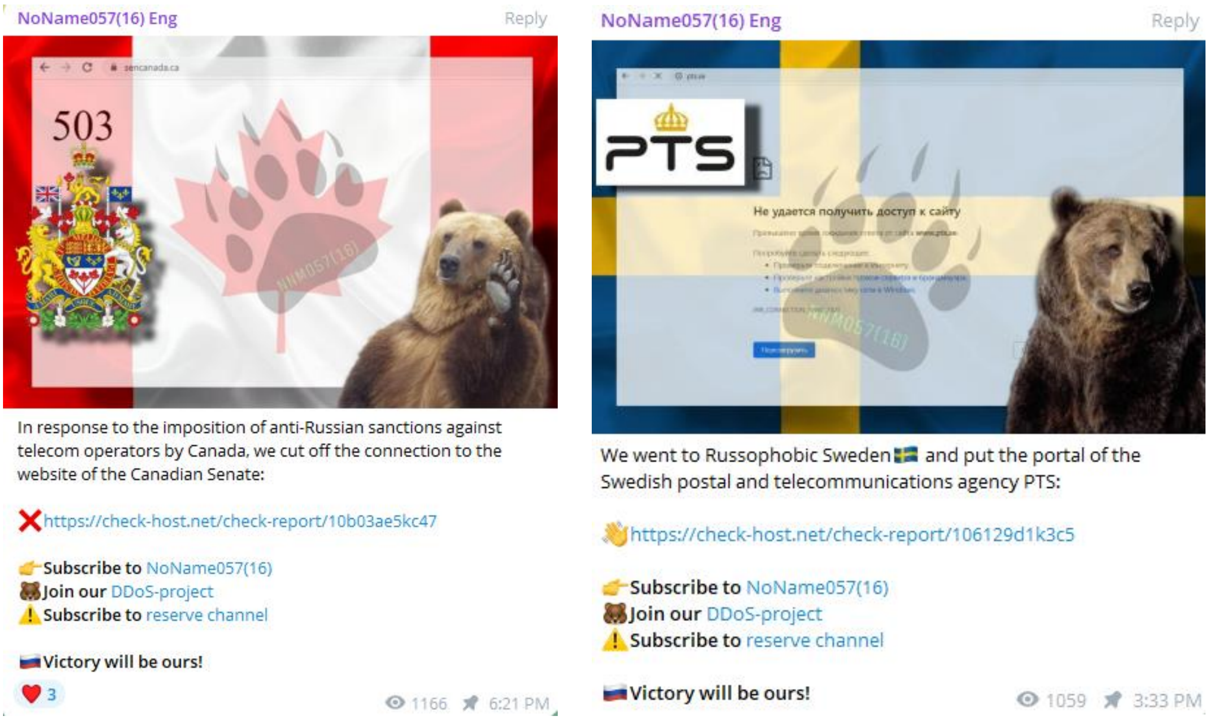
Top targeted countries in the telecom sector by IABs



January 2023- October 2023

DDOS ATTACKS

Distributed Denial of Service (DDoS) attacks pose a significant threat to the telecommunications sector, potentially resulting in damage to reputation and financial loss. These attacks, designed to overwhelm a network's resources and render services inaccessible, pose significant challenges to the reliability of communication infrastructure. Some attacks are performed by hacktivist groups that are driven by ideological motives, launching attacks against specific countries or companies. For example, the pro-Russian hacktivist group NoName057(16) launched several DDoS campaigns targeting telecom companies, usually of countries that support Ukraine.



NoName057(16) Eng

In response to the imposition of anti-Russian sanctions against telecom operators by Canada, we cut off the connection to the website of the Canadian Senate:

❌https://check-host.net/check-report/10b03ae5kc47

👉Subscribe to NoName057(16)
🐻Join our DDoS-project
⚠️Subscribe to reserve channel

🇷🇺Victory will be ours!
❤️ 3 1166 6:21 PM

NoName057(16) Eng

Не удается получить доступ к сайту

We went to Russophobic Sweden🇸🇪 and put the portal of the Swedish postal and telecommunications agency PTS:

👋https://check-host.net/check-report/106129d1k3c5

👉Subscribe to NoName057(16)
🐻Join our DDoS-project
⚠️Subscribe to reserve channel

🇷🇺Victory will be ours! 1059 3:33 PM

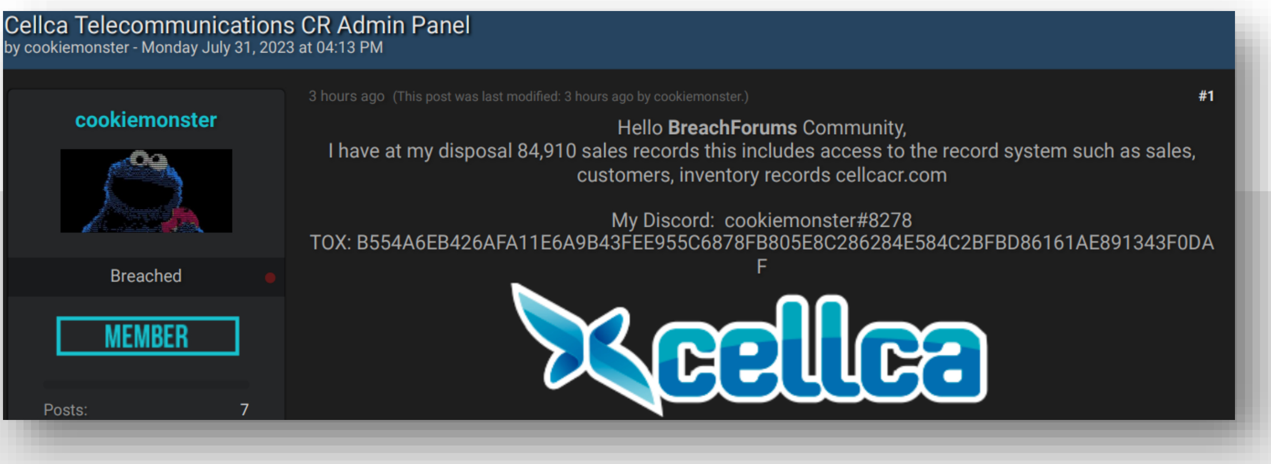
NoName launched DDoS attacks against telecom companies in June-July 2023

As part of the cyber attack accompanying the Israel-Hamas war, KELA observed various DDoS campaigns targeting telecom companies as they considered a critical target, causing disruption to telecom companies during the ongoing war. The attacks targeted both sides of the war and also countries that support one of the parties.

FRAUD ACTIVITIES

Fraud targeting the telecom sector takes many forms, from subscription fraud and identity theft to SIM card swapping. Examples of fraud-related chatter observed by KELA in its monitored cybercrime sources include:

- **SIM swapping services**, which is a malicious technique used by cybercriminals to take control of an individual's phone number. Threat actors are either offering or searching for SIM-swapping services.
- **Sale of stolen E-SIMs**, which allows actors to use digital SIM cards that are registered by other people to conduct their activities.
- **VoIP call spoofing services**. These tools or platforms allow users to manipulate the caller ID information displayed during a phone call.
- **Sale of access to telecom admin panels**, which could be used by threat actors to activate E-SIMs, access company and clients' data, and more.
- Users looking to **buy bulk phone numbers** that are used for fraud and scam activities. The actors set up call forwarding for incoming calls to their own numbers, making it harder to track their identities.



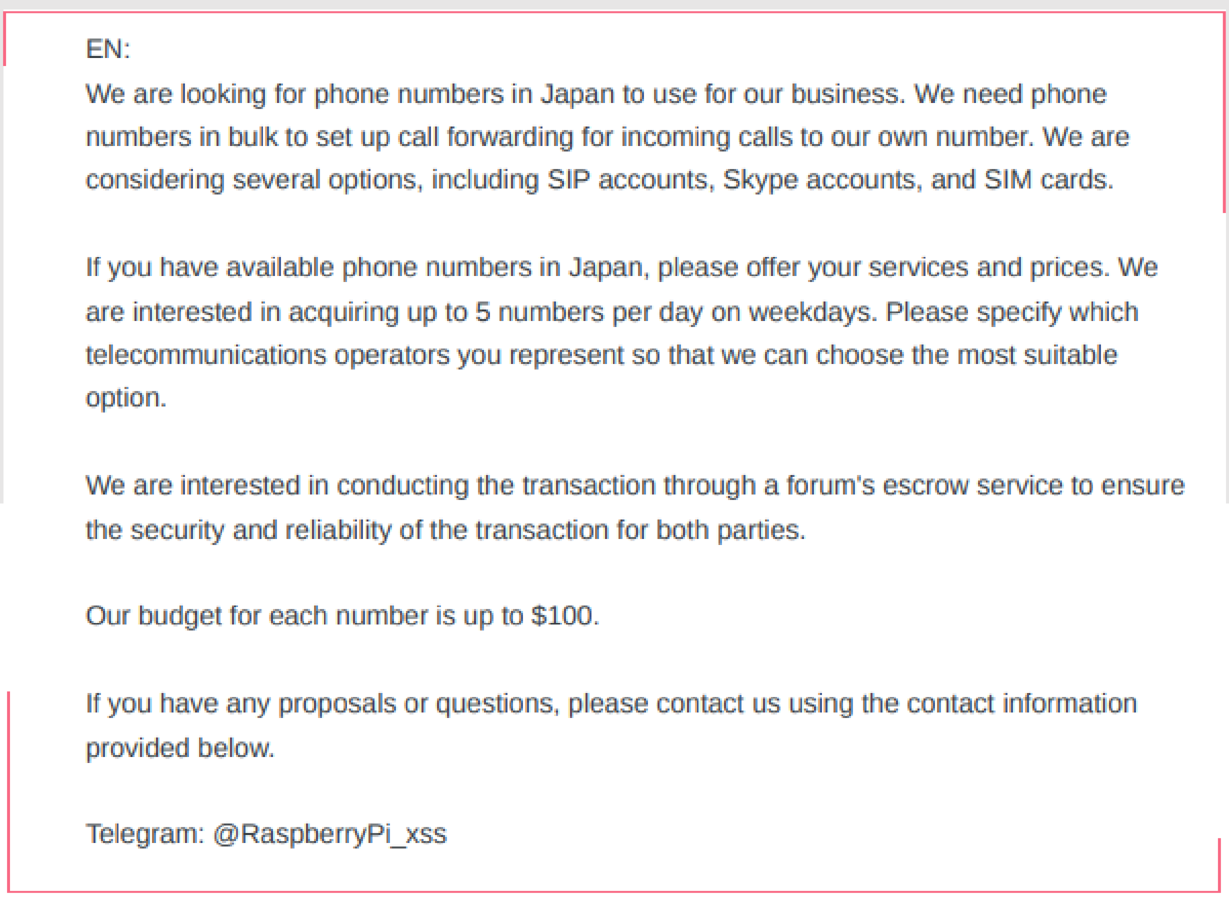
Cellca Telecommunications CR Admin Panel
by cookiemonster - Monday July 31, 2023 at 04:13 PM

3 hours ago (This post was last modified: 3 hours ago by cookiemonster.) #1

Hello **BreachForums** Community,
I have at my disposal 84,910 sales records this includes access to the record system such as sales, customers, inventory records cellcacr.com

My Discord: cookiemonster#8278
TOX: B554A6EB426AFA11E6A9B43FEE955C6878FB805E8C286284E584C2BFBD86161AE891343F0DAF

An actor offering access to admin panel of the Telecom company



EN:

We are looking for phone numbers in Japan to use for our business. We need phone numbers in bulk to set up call forwarding for incoming calls to our own number. We are considering several options, including SIP accounts, Skype accounts, and SIM cards.

If you have available phone numbers in Japan, please offer your services and prices. We are interested in acquiring up to 5 numbers per day on weekdays. Please specify which telecommunications operators you represent so that we can choose the most suitable option.

We are interested in conducting the transaction through a forum's escrow service to ensure the security and reliability of the transaction for both parties.

Our budget for each number is up to $100.

If you have any proposals or questions, please contact us using the contact information provided below.

Telegram: @RaspberryPi_xss

Actors are interested in buying bulk phone numbers in Japan

APTS TARGETING TELECOM

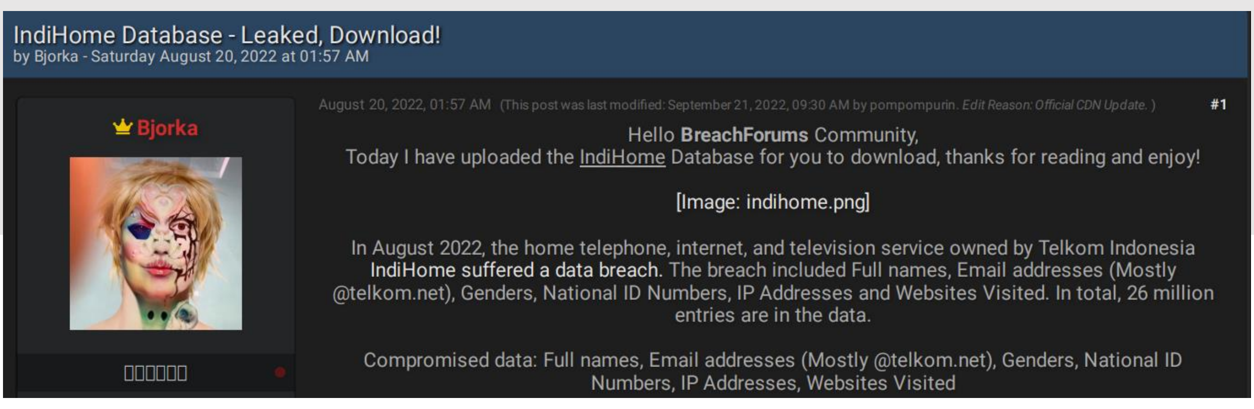
State-sponsored cyber attackers may target telecommunications infrastructure to conduct surveillance, monitor communications, and gather intelligence. This can include intercepting sensitive government, military, or corporate communications. KELA identified several APT campaigns targeting telecommunications providers since the beginning of 2023:

- Chinese-sponsored APT41 has been using WyrmSpy and DragonEgg spyware to target mobile devices and in another campaign aimed at stealing intellectual property (IP).
- Lancefly APT has been using the Merdoor backdoor to attack South and Southeast Asian telecom orgs.
- Russian-sponsored Winter Vivern APT has been using the Aperitif malware to attack European government organizations and telecommunication service providers.
- Chinese state-sponsored Gallium APT has been using a custom variant of Mimikatz called mim221 to target telecommunications providers in the Middle East.
- Sandman APT has been utilizing LuaJIT platform to deploy a backdoor and attack telecommunication providers in the Middle East, Western Europe, and the South Asian subcontinent.

DATABASE DUMPS

Threat actors are highly interested in data of telecom companies as it might include valuable information of third parties and can be leveraged for further attacks. A successful telecom data breach exposes records such as contact details, social security numbers, and credit card information of millions of customers. Some threat actors focus on telecom: for example, IntelBroker offered for sale several databases of telecom companies (AT&T, Charter Communications, Verizon Wireless, Comcast and US Cellular).

Another big breach occurred in August 2022, when threat actor Bjorka shared a database of Indonesian internet services provider IndiHome, which was allegedly breached in the same month. The leak exposed approximately 26.7 million records, and includes users' email addresses, names, ID numbers, keywords, IP addresses, physical locations, browsers and genders.*



IndiHome Database - Leaked, Download!
by Bjorka - Saturday August 20, 2022 at 01:57 AM

August 20, 2022, 01:57 AM (This post was last modified: September 21, 2022, 09:30 AM by pompompurin. *Edit Reason: Official CDN Update.*) #1

Hello **BreachForums** Community,
Today I have uploaded the IndiHome Database for you to download, thanks for reading and enjoy!

[Image: indihome.png]

In August 2022, the home telephone, internet, and television service owned by Telkom Indonesia **IndiHome suffered a data breach.** The breach included Full names, Email addresses (Mostly @telkom.net), Genders, National ID Numbers, IP Addresses and Websites Visited. In total, 26 million entries are in the data.

Compromised data: Full names, Email addresses (Mostly @telkom.net), Genders, National ID Numbers, IP Addresses, Websites Visited

An actor is sharing a database of an Indonesian telecom company

RECOMMENDATIONS

•**Monitoring cybercrime sources**: tracking and monitoring cybercrime underground forums is a crucial aspect of protection efforts. Organizations must be aware of cybercriminals' activities, TTPs, new tools and following cybercrime chatter regarding illicit services, data breaches, etc in order to understand and mitigate potential threats.

•**Supply chain security:** Telecom companies can be part of supply chain attacks and therefore it's important to ensure the security practices of third-party vendors and partners.

•**DDoS protection:** deploy DDoS mitigation solutions to safeguard against large-scale attacks that can disrupt services. This involves having the capacity to absorb and mitigate the impact of such attacks.

•**Backups and disaster recovery**: regularly back up critical data and ensure a robust disaster recovery plan is in place. This allows for a quicker recovery in case of a successful cyber attack.

[1] See KELA's profile on Bjorka on the platform.