

Cybercriminals are targeting law enforcement agencies worldwide

resecurity.com/blog/article/cybercriminals-are-targeting-law-enforcement-agencies-worldwide

[Back](#)

Cybercrime Intelligence

19 Aug 2022

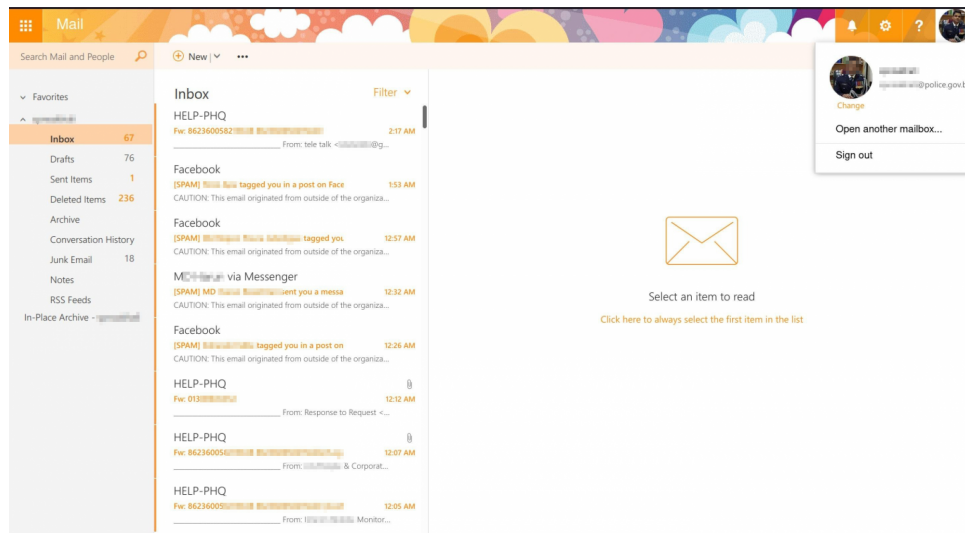
cybercrime, law enforcement, public safety, unauthorized access

Resecurity registered an increase in malicious activity targeting law enforcement agencies at the beginning of Q2 2022.

Threat actors are hacking e-mail accounts belonging to law enforcement officers, their aim is to leverage the accounts for further malicious purposes. Typically, they leverage social engineering tactics, however one of the recent trends is to address fake subpoenas and so called EDR's (Emergency Data Requests) to major technology companies and online-services such as Apple, Facebook (Meta), Snapchat, Discord to maliciously collect sensitive information about their targets.

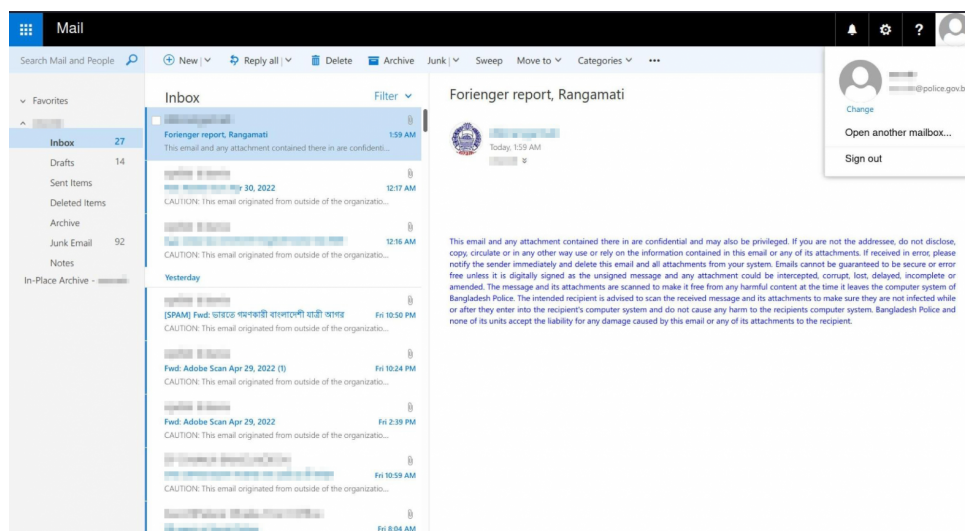
Threat actors are looking for billing history, geographical location, phone calls, text history, and other sensitive details which could be used to leverage extortion or cyberespionage purposes. Such incidents have become especially notable in cybercriminal group activities such as LAPSUS\$ and Recursion Group.

Resecurity has observed multiple marketplaces in the Dark Web where cybercriminals have monetized accounts and credentials belonging to police officers of various foreign countries (e-mails, VPNs, SSO, etc.). One such email account has previously been used to send fake EDR requests on behalf of the Bangladesh Police which has been recently covered in a [Bloomberg article](#) where the CEO of Resecurity Gene Yoo was quoted. The price of such accounts is typically not different from any other compromised accounts and varies in range between \$20-\$35 but in some cases independent actors with bigger access may sell it in a range of \$1,000-\$10,000.



account

Compromised email



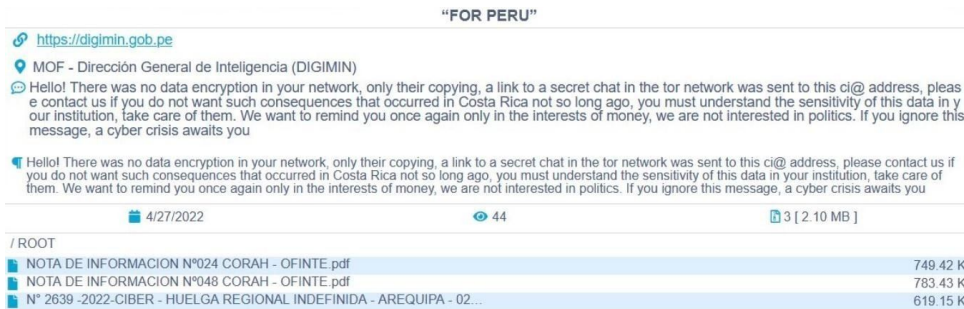
account

Compromised email

The incident has been timely reported by Resecurity to BGD e-Gov CIRT (Bangladesh e-Government Computer Incident Response Team) and over 5 compromised law enforcement accounts have been successfully recovered for further risk mitigation.

One of the biggest concerns – the visible security of the law enforcement IT infrastructure, which may create a significant risk to our society not just in cyberspace, but in real life too. Terrorists and extremist groups may leverage such access for malicious purposes.

The trend is continuing, and more law enforcement organizations have been impacted by cyberattacks this month. Just recently, the Conti ransomware group attacked the Intelligence Agency in Peru and leaked their data which created a significant precedent in the security community. Cybercriminals were extorting DIGIMIN, one of the national agencies, asking for payment in cryptocurrency.

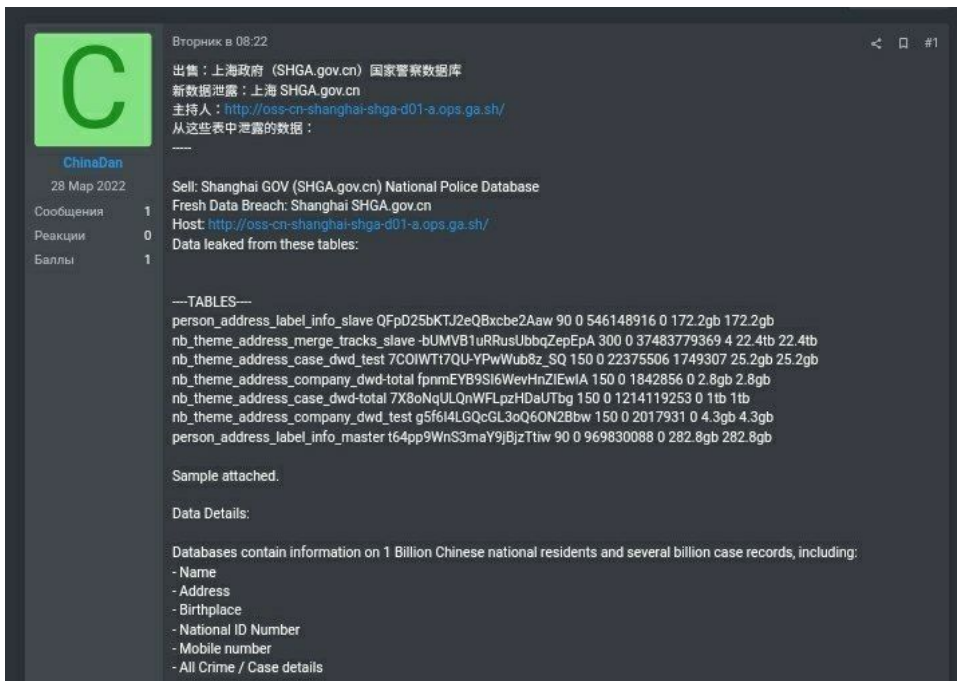


Conti Ransomware

Group

DDOS Secrets - another notable group of threat actors, has released 285,635 leaked emails from Nauru Police. The motivation of actors was different - hacktivists attempted to highlight possible abuses endured by asylum-seekers and refugees based on the island and to make them public.

The bad actor in Dark Web offered for sale Shanghai Police database including 1B+ records about Chinese citizens. Multiple postings have been identified around July 2 with reference to actor "ChinaDan". According to several sources, the actor was offering 23 Terabytes of data for sale.



Later, this information has been offered by other independent actors for 3 BTC (\$60,500). Using anonymous channels and IM like Telegram the actors were looking to monetize the stolen data in Dark Web.

MG7

In 2022, the Shanghai National Police (SHGA) database was leaked. This database contains many TB of data and information on Billions of Chinese citizens.

Sell: Shanghai GOV ([SHGA.gov.cn](http://shga.gov.cn)) National Police Database

Host: <http://oss-cn-shanghai-shga-d01-a.ops.ga.sh/>

Data leaked from these tables:

---TABLES---

```
person_address_label_info_slave QFpD25bKTJ2eQBxcbe2Aaw 90 0
546148916 0 172.2gb 172.2gb
nb_theme_address_merge_tracks_slave -
bUMVB1uRRusUbbqZepEpA 300 0 37483779369 4 22.4tb 22.4tb
nb_theme_address_case_dwd_test 7COIWTt7QU-YPwWub8z_SQ
150 0 22375506 1749307 25.2gb 25.2gb
nb_theme_address_company_dwd-total
fpmEYB9SI6WevHnZIEwIA 150 0 1842856 0 2.8gb 2.8gb
nb_theme_address_case_dwd-total 7X8oNqULQnWFLpzHDAUTbg
150 0 1214119253 0 1tb 1tb
nb_theme_address_company_dwd_test
g5f6l4LGQcGL3oQ6ON2Bbw 150 0 2017931 0 4.3gb 4.3gb
person_address_label_info_master t64pp9WnS3maY9jBjzTtiw 90 0
969830088 0 282.8gb 282.8gb
```

Data Details:

Databases contain information on **1 Billion Chinese national residents** and several billion case records, including:

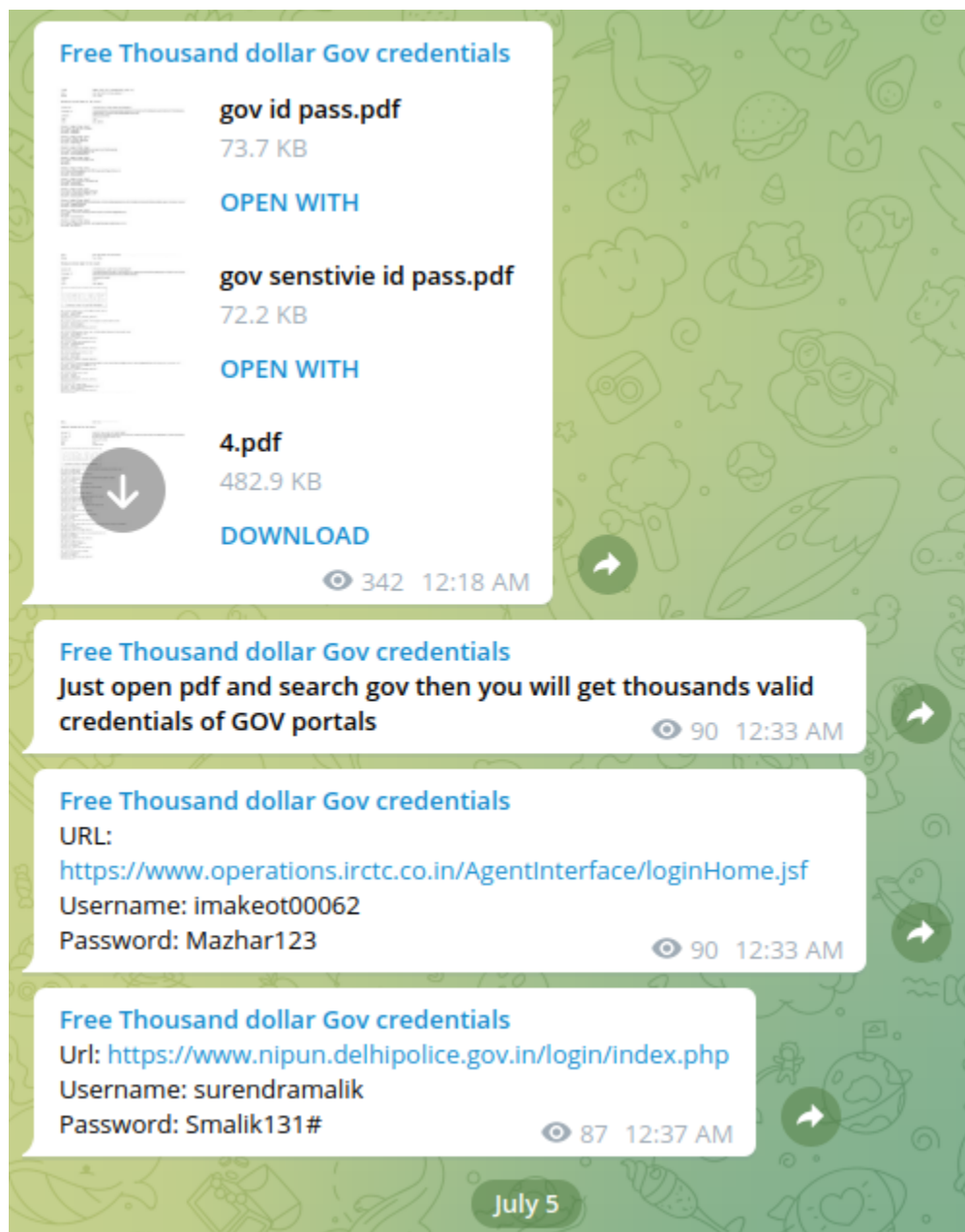
- Name
- Address
- Birthplace
- National ID Number
- Mobile number
- All Crime / Case details

Price: 3BTC (\$60500 USD Only)

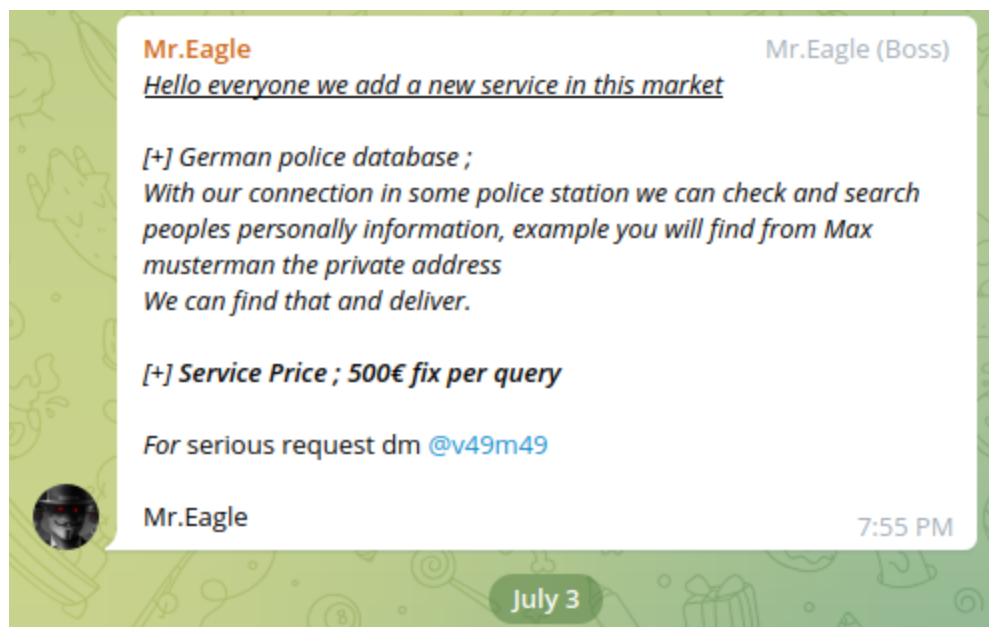
Contact: [@v0x_machina](https://twitter.com/v0x_machina)

12:19 PM

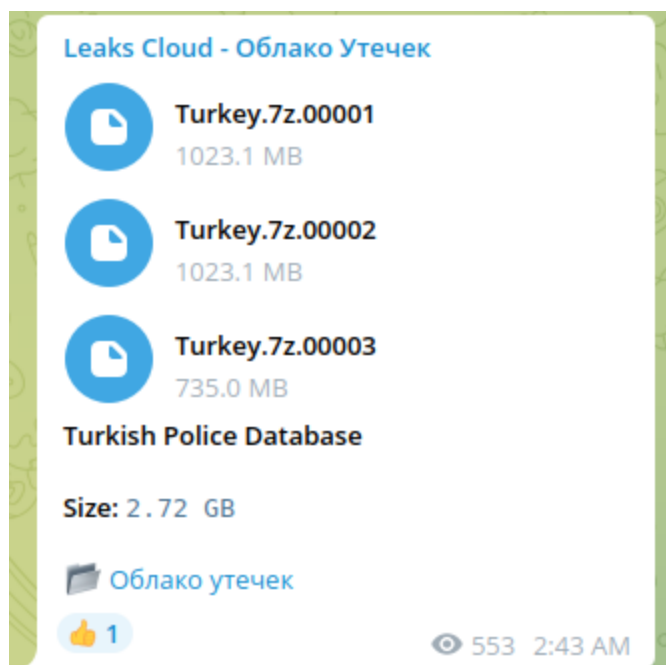
July 5, 2022 - the bad actor was offering access to Indian law enforcement portal and government resources in India. Based on further analysis, the credentials and associated data offered by the actor were likely compromised by password stealers such as Mars Stealer, X-Files Stealer or Azorult.



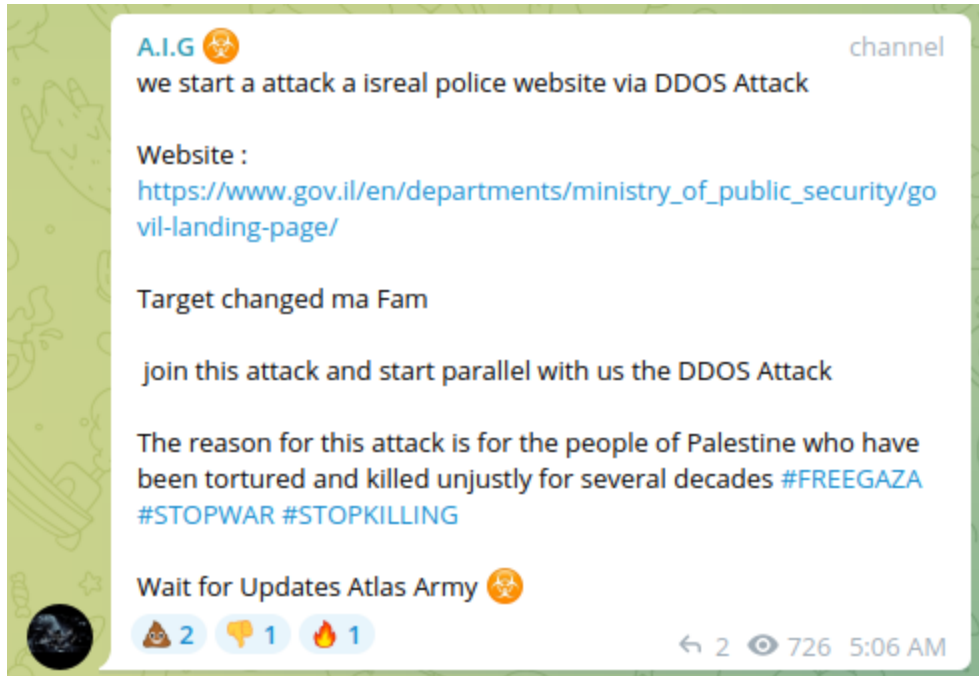
Cybercriminals abuse law enforcement databases and offer various illegal services in Dark Web creating significant risk for users' privacy. Using unauthorized access or insider contacts they're able to extract sensitive information and to monetize it in the underground. July 3, 2022 - there was identified an actor Mr.Eagle selling a "look-up" service for 500 euro (per query / per person).



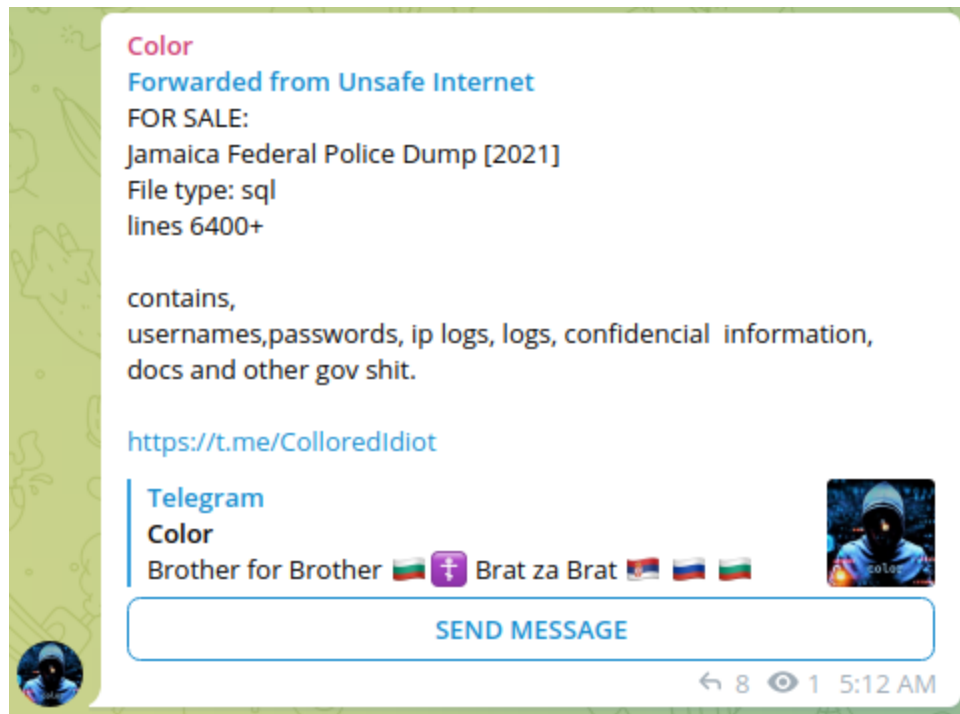
Last year, the bad actor released a dump of data presumably originating from an unnamed law enforcement system in Turkey. Notably, 6 years ago a hacker going by the online alias ROR[RG] has released a large amount of data that belonged to a Turkish National Police database and it's thought to contain large amounts of sensitive private information. ROR[RG] is aligned with the Anonymous hacktivist group and has leaked the data that was supposedly stolen from Turkish General Directorate of Security (EGM) onto a number of peer-to-peer sites for anyone to download and examine. The data was released through The Cthulu website, which has been a host of a number of leaks by members of Anonymous in the past, including a serious hack against a US Police union.



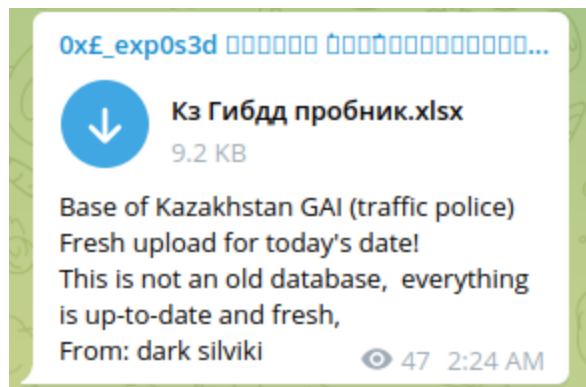
In context of ongoing geopolitical tensions, bad actors are actively attacking law enforcement WEB-sites leveraging various types of DDoS activity to create protest narratives.



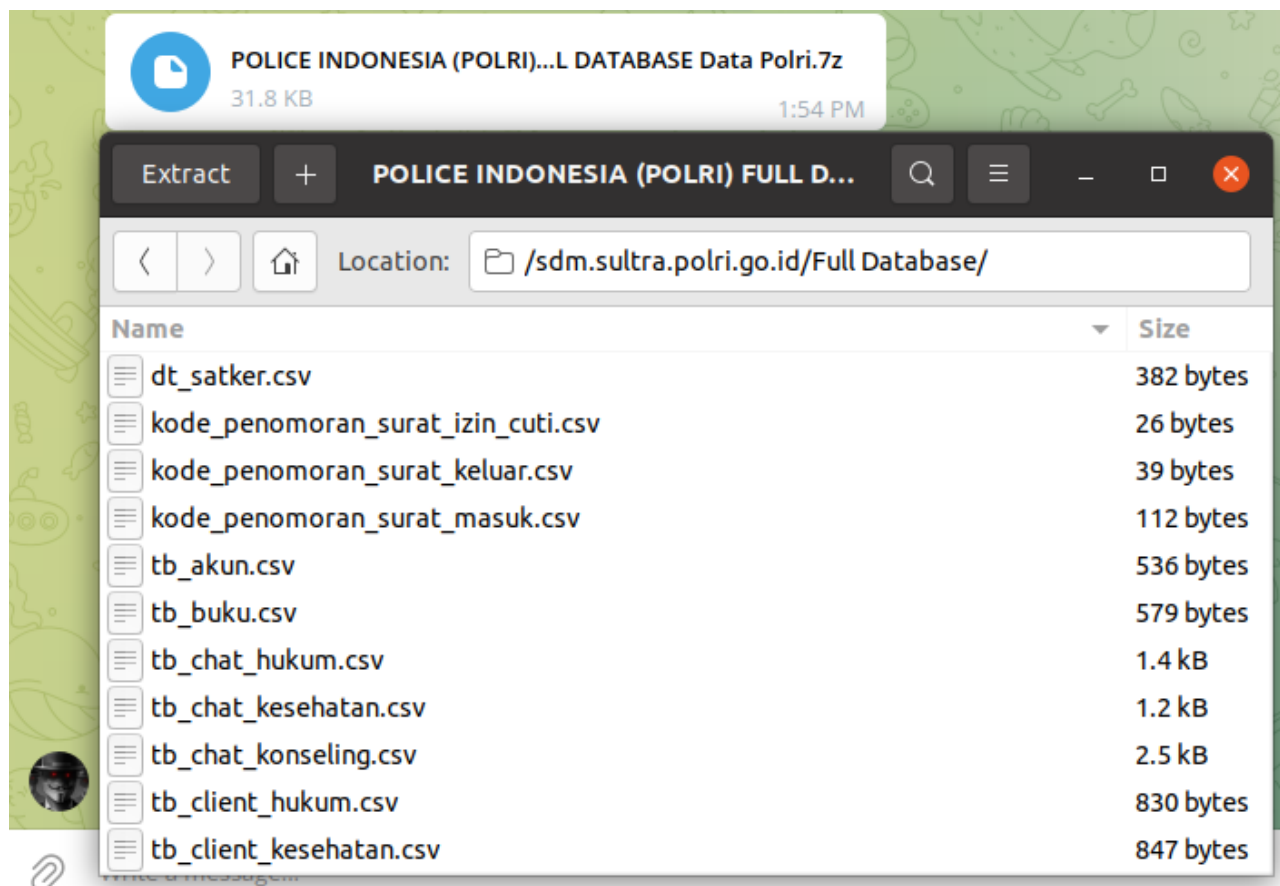
The bad actor was offering a dump of hacked law enforcement portals in Jamaica. Based on further assessment, he was able to exploit a MySQL injection vulnerability in one of the insecure modules of the official Jamaica Federal Police WEB-site.



Bad actors released a road traffic & vehicle database of Kazakhstan presumably acquired from a law enforcement system. Such access allows to check car numbers, vehicles registration, and other PII related to citizens. Such offerings are also available commercially in Dark Web covering different geographical regions. The cost of "look-up" varies from \$50 to \$250.



The bad actor was selling compromised database of WEB-application presumably belonging to a law enforcement in Indonesia. The stolen data also included internal communications and law enforcement employee information.



The bad actors are also offering abuse service of law enforcement agencies, technically leading to fake incidents notifications and other types of malicious activity. While some of such tactics may look primitive, unfortunately, they may generate serious damage to innocent people on practice.

Deleted Account
Forwarded from Early Swats
SWAT CITY

-OFFICER SWAT-
80\$
Few officers come in to check for house party's or family abuse.

-PARAMEDICS-
100\$
paramedics come in to check for an overdose, someone sick, etc...
(for a dead body it's 50\$ extra)

-SWAT TEAM-
150\$
Swat team comes in for terrorists, illegal weapons, someone convicted for murder, we organize everything.

-ATF INVESTIGATION-
170\$
An organization will come looking for guns, explosives and more.

-FIREFIGHTERS-
180\$
They will come looking for a fire and after finding out nothing was there we blackmail the person y'all ordered and they have to pay a huge fine

-DEA investigation-
200\$
They come in your house look for drugs if they find even a little bit of weed they go to jail, depending on state / amount on person.

--+--
BOMB SQUAD
--+--
House - 250\$
Restaurant - 300\$
School - 350\$
Mall - 400\$
We send swat teams and local police to the area y'all want are armored around 7 cars 4 vans looking for explosives

-BLACKMAIL-
500\$
we blackmail someone and they get on the news and go to jail/
juvie

DA

2575

Resecurity identified multiple underground services selling police reports about individuals what allows bad actors to collect sensitive information. Such services can be widely used by foreign intelligence and organized crime to target individuals and organizations of interest.

00:15 🔊

SERVICE KOZMAP



Hey famz! I offer you very suitable draw service!

We provide u high quality docs plug for all situations!

We have been working in these direction for a long time and u can rely on us!

The best quality n the customer service for the average price.

🟡 We print all our documents so all of them look as real as they could. Real shadows. Real metainfo. Real scans.

- DLs, IDs scans for verification
- Vaccine Cards Scans!!!
- SSN cards, birth certificates
- Bank statements
- Utility bills
- EIDL n EDD docs
- IRS and SBA docs
- Police reports
- Photoshop works
- And a lot of other draw services!

🟡 We work not only on USA documents, we provide service worldwide.


- 🔄 Contact me: [@kozmap](#)
- 🔄 Feedback: [@kozmapfeedback](#) (Our vouches)
- 🔄 Channel: <https://t.me/joinchat/LI0I6PaHLA8wY2I6> (Price list)
- 🔄 Our works: [@kozmapworks](#) (You can judge our quality)

LX

👁️ In addition to it, we provide DL and other lookups services!




 **Indonesia Police / POLRI DB** 

◆ **DATABASE COUNTRY :** Indonesia 

◆ **DATABASE STATES :** 34 Province in Indonesia.

◆ **DATABASE RECORD :** +/- 467.149 Police Personnel Full info.

◆ **DATABASE LEAK YEAR :** 2021

◆ **WE ALWAYS ACCEPT ESCROW** 

◆ **DATABASE FORMAT :** TXT

◆ **DATABASE CONTENTS :**

Ranks - Name - Unit - Email - Mobile Number

◆ **DATABASE SAMPLE :**

```
(431692, 'KOMPOL', 'AGUS SUWONDO, SH ', 'GADIK MUDA  
13 SPN POLDA JATIM ', '08121631273 ',  
'a.suwondo@yahoo.com', '2021-11-03 16:09:23'),
```

```
(431694, 'KOMPOL', 'TOTOK NUR ARIFIN, S.H. ',  
'KANIT II SUBDIT III DITRESNARKOBA POLDA JATIM ',  
'03170797878/081230557878. ', 'ditresnarkoba-  
poldajatim@yahoo.co.id', '2021-11-03 16:09:23'),
```

```
(431695, 'KOMPOL', 'SUHARTI ', 'KAURBIA SUBBIDBIA
```

Indonesia Police / POLRI DB

DATABASE COUNTRY : Indonesia

DATABASE STATES: 34 Province in Indonesia.

DATABASE RECORD : +/- 467.149 Police Personnel Full info.

DATABASE LEAK YEAR: 2021

WE ALWAYS ACCEPT ESCROW

DATABASE FORMAT: TXT

DATABASE CONTENTS:

Ranks - Name - Unit - Email - Mobile Number

DATABASE SAMPLE:

(431692, 'KOMPOL', AGUS SUWONDO, SH', 'GADIK MUDA 13 SPN POLDA JATIM , 08121631273, 'a.suwondo@yahoo.com', '2021-11-03 16:09:23'),

(431694, "KOMPOL", 'TOTOK NUR ARIFIN, S.H. KANIT II SUBDIT III DITRESNARKOBA POLDA JATIM '03170797878/081230557878. ', 'ditresnarkobapoldajatim@yahoo.co.id', '2021-11-03 16:09:23'),

(431695, 'KOMPOL', SUHARTI, KAURBIA SUBBIDBIA

Resecurity® is committed to protecting consumers and enterprises all over the globe, and is actively involved in public-private partnerships to share actionable cyber threat intelligence (CTI) with financial institutions, technology companies and law enforcement to ultimately minimize the risk of credentials being compromised and data breaches being executed.

Newsletter

Keep up to date with the latest cybersecurity news and developments.

By subscribing, I understand and agree that my personal data will be collected and processed according to the [Privacy](#) and [Cookies Policy](#).

Cloud Architecture

