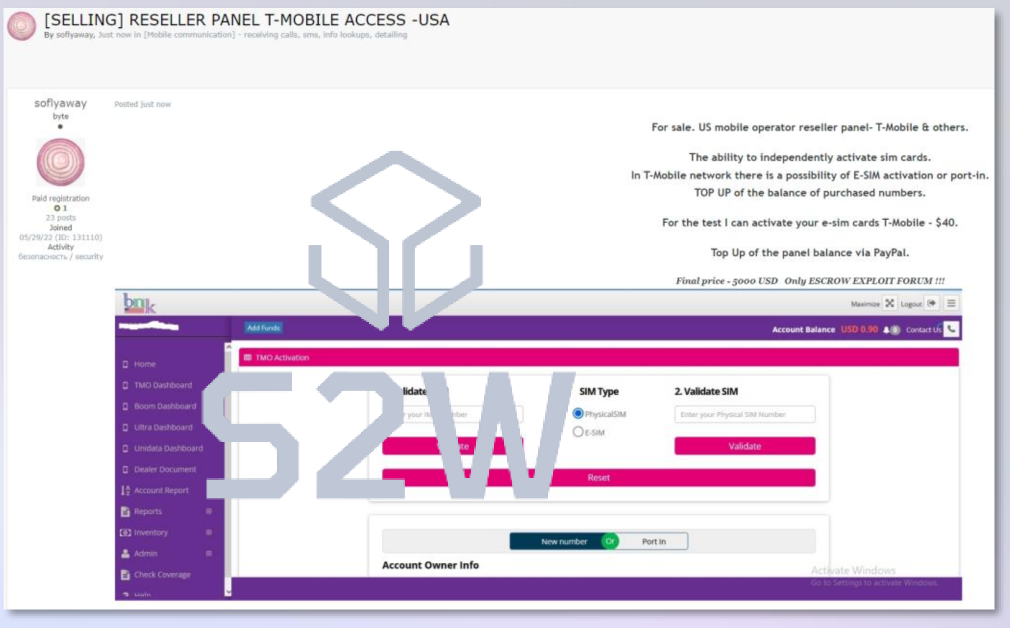
Dark web & Telegram
Weekly Highlights

April Week 2

A well-known telecom company's reseller internal data sales detected in the US. Concerns arise over SIM card fraud and smartphone data theft

- On April 7th, a post selling internal data of a US telecom company's SIM card reseller was detected on the Dark Web Russian hacking forum Exploit.in.
- According to the seller, the leaked data could be used to activate assigned SIM cards, steal balances, and potentially engage in identity theft, call interception, and message interception.
- The seller provided a sample of the leaked data, showcasing the reseller company's panel interface, with a sale price of approximately 6 million Korean Won.


[SELLING] RESELLER PANEL T-MOBILE ACCESS -USA
By soflyaway, Just now in [Mobile communication] - receiving calls, sms, info lookups, detailing

soflyaway
byte
Paid registration
1
23 posts
Joined
05/29/22 (ID: 131110)
Activity
безопасность / security

Posted just now

For sale. US mobile operator reseller panel- T-Mobile & others.

The ability to independently activate sim cards.
In T-Mobile network there is a possibility of E-SIM activation or port-in.
TOP UP of the balance of purchased numbers.

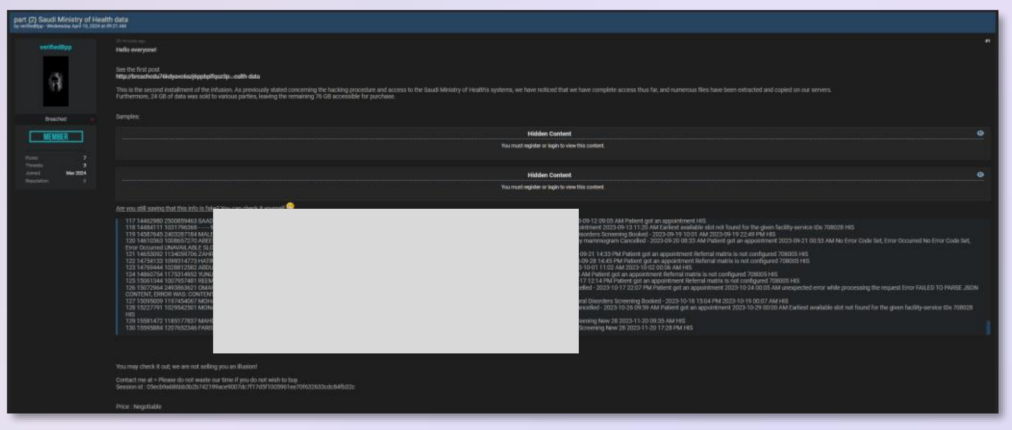
For the test I can activate your e-sim cards T-Mobile - $40.

Top Up of the panel balance via PayPal.

Final price - 5000 USD Only ESCROW EXPLOIT FORUM !!!

Internal data from the Saudi Ministry of Health up for sale, including detailed personal information of Saudi patients, totaling 76GB

- On April 10th, user verifiedBpp, active on the well-known hacking forum BreachForums on the Dark Web, posted about selling internal data from the Saudi Ministry of Health.
- According to the seller, the leaked internal data contains detailed personal information of Saudi patients, including names, identification numbers, contacts, and medical records. To prove this, they posted personal information of over 100 individuals.
- The leaked data reportedly amounts to 100GB, with 24GB already sold, leaving the remaining data for sale.


part (2) Saudi Ministry of Health data
by verifiedBpp - Wednesday April 10, 2024 at 09:21 AM

verifiedBpp
Breached
MEMBER

Hello everyone!

See the first post
http://breachedu76kdyavc6szj6ppbplfqoz3p...ealth-data

This is the second installment of the infusion. As previously stated concerning the hacking procedure and access to the Saudi Ministry of Health's systems, we have noticed that we have complete access thus far, and numerous files have been extracted and copied on our servers. Furthermore, 24 GB of data was sold to various parties, leaving the remaining 76 GB accessible for purchase.

Samples:

Hidden Content
You must register or login to view this content.

Hidden Content
You must register or login to view this content.

Are you still saying that this info is fake? You can check it yourself!

[redacted]

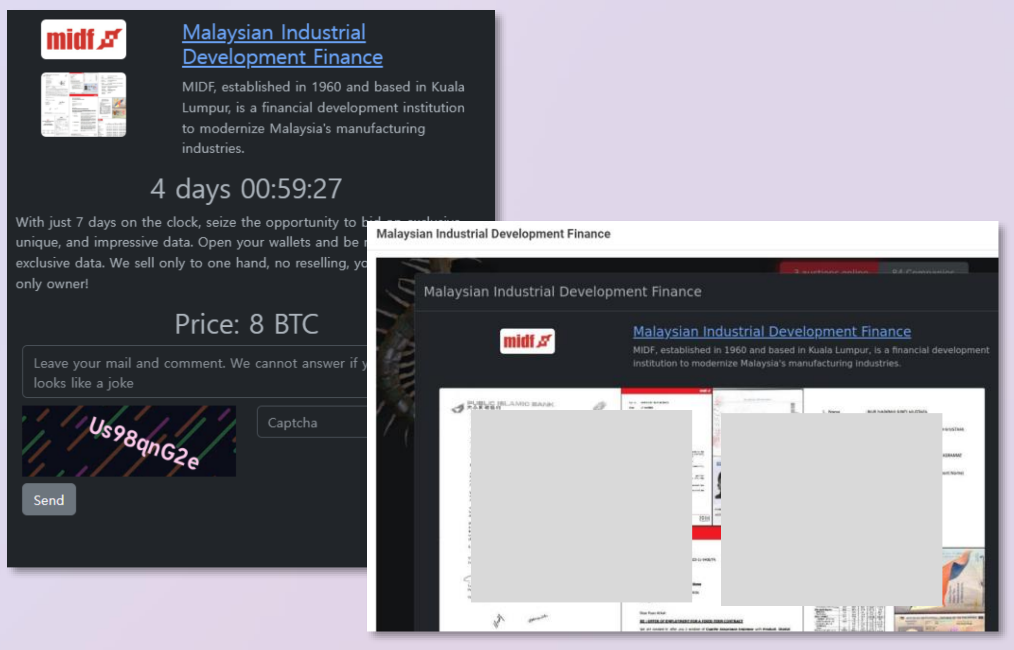
You may check it out; we are not selling you an illusion!

Contact me at > Please do not waste our time if you do not wish to buy.

Price : Negotiable

Malaysia's Industrial Bank suffers data leakage from a ransomware attack, with hackers demanding 800 million KRW in ransom

- Malaysian Industrial Development Finance (MIDF) was hit by a ransomware attack, leading to data exposure.
- On April 10th, the ransomware group Rhysida disclosed some of MIDF's internal data on their Dark Web platform.
- This includes documents and identification materials suspected to be from the bank. Rhysida has given MIDF four days to negotiate, demanding 8 bitcoins, approximately 800 million KRW at current rates.


Malaysian Industrial Development Finance

MIDF, established in 1960 and based in Kuala Lumpur, is a financial development institution to modernize Malaysia's manufacturing industries.

4 days 00:59:27

With just 7 days on the clock, seize the opportunity to b unique, and impressive data. Open your wallets and be r exclusive data. We sell only to one hand, no reselling, yo only owner!

Price: 8 BTC

Leave your mail and comment. We cannot answer if y looks like a joke

Captcha

Send

Malaysian Industrial Development Finance

Malaysian Industrial Development Finance

Malaysian Industrial Development Finance

MIDF, established in 1960 and based in Kuala Lumpur, is a financial development institution to modernize Malaysia's manufacturing industries.

[redacted]

[redacted]

About S2W

- S2W is a big data intelligence company specialized in analyzing hidden channels and cryptocurrencies.
- S2W captures massive amount of data from various channels and conducts analysis with the unique AI based multi-domain analytics engine.

- S2W offers a threat intelligence solution S2-XARVIS,
- Detection of brand abuse site, phishing site, real-time threat monitoring solution QUAXAR,
- Cryptocurrency anti-money laundering solution S2-EYEZ,
- Digital fraud detection system S2-TRUZ.

Contact

For any queries, please contact support@s2w.inc / www.s2w.inc

The information contained in this document is proprietary and confidential.
If you are not the intended recipient, please note that any use or circulation of this document may be cause for legal action.