



ZEROFOX®

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

T-Mobile SIM Swap Service Advertised

Well-regarded threat actor “s.lott” advertised a SIM swap service for T-Mobile on the predominantly Russian language Deep Web forum “Exploit”. Unlike similar services that often turn out to be scams, ZeroFox researchers note this actor’s thread gained significant traction in recent weeks, with several well-regarded peer threat actors stating they successfully used the service. This indicates the actor likely has the capabilities to perform the SIM swaps they claim.

To initiate the service, the actor said they would need partners to supply them with login credentials for compromised bank or cryptocurrency exchange accounts. The actor claims they can check these credentials to determine which ones are associated with T-Mobile numbers, and then transfer these numbers over to a SIM card they own. This would allow the threat actor to receive the SMS one-time-password (OTP) codes to log into the bank or cryptocurrency exchange accounts and drain the funds.

If legitimate, ZeroFox researchers assess the actor likely has a social engineering method or an OTP bot designed to exploit T-Mobile procedures, or that the actor has a T-Mobile insider, since the service is only applicable to T-Mobile.

Original post from
threat actor "s.lott"
advertising a SIM swap
service for T-Mobile

T-Mobile SIM Swap Service Advertised (Cont.)



I can finally simswap T mobile again 24/7

By s.lott, June 16 in [Mobile communication] - receiving calls, sms, info lookups, detailing

Follow 1

Start new topic

Reply to this topic

s.lott

megabyte

●●●



Paid registration

8

52 posts

Joined

11/11/21 (ID: 121993)

Activity

фрикинг / phreaking

Posted June 16

I want partners with logs either bank/crypto logs to work with me on % basis I can swap Unlimited t mobile numbers 50/50 message me on telegram if you want to work serious people !
@s_lot111

+ Quote

Report post

Network Access To Unnamed Central Bank Alleged

Moderately credible threat actor “4c3” advertised virtual desktop infrastructure (VDI) and virtual private network (VPN) access with domain administrator rights to the internal network of an unnamed central bank on the predominantly Russian language Deep Web forum “Exploit”. The actor suggested that skilled threat actors could leverage this access to steal funds directly from the bank.

According to the actor, there are approximately 10,000 devices on the network. They specified that most of these systems are running Windows. The actor claims to have access to various resources, including chat applications, a file server with more than 4 TB of sensitive data, and an Oracle FLEXCUBE database.

The actor is selling the access outright for \$500,000 USD, which is rare, because most threat actors typically auction this level of network access at much lower prices. Despite the high cost, ZeroFox researchers assess the actor likely possesses the access they claim because they agreed to use the forum’s escrow service and they have deposited funds on the forum to serve as collateral in a brokered deal.

Original post from
threat actor "4c3"
advertising network
access to the internal
network of an
unnamed central bank

Network Access To Unnamed Central Bank Alleged (Cont.)



SELLING ALL NETWORK ACCESS AT A CENTRAL BANK

By 4c3, 9 hours ago in [Access] - FTP, shells, root, sql-inj, DB, Servers

Follow

Start new topic

Reply to this topic

4c3

byte



Paid registration

3

10 posts

Joined

05/15/21 (ID: 116589)

Activity

хакинг / hacking

Deposit

0.010400 B

Posted 9 hours ago (edited)

Hello everyone,

I am selling all network at X central bank, the internal network filters for TCP, UDP, HTTP and HTTPS or any other kind of protocol that looks suspicious, we have DA, the domain has around 10k machines configured (most of them are Windows), theedr of the machines are Symantec. Their funds in the billions and there are several machines running on several different subnets, employees communicate between office chat services, there is file server with more than 4 TB of internal data including share folder for every user on the network and they also have a flexcube database.

We can provide VDI & VPN and all password of domain dump (include DA users).

This access is perfect for a rob Swift , it only takes a strong team and persistence (something that I can't do alone). For obvious reasons, I will not say which Central Bank is, only people with reputation on exploit.in can make the purchase, and seems to start the conversation will have to send a message in my private.

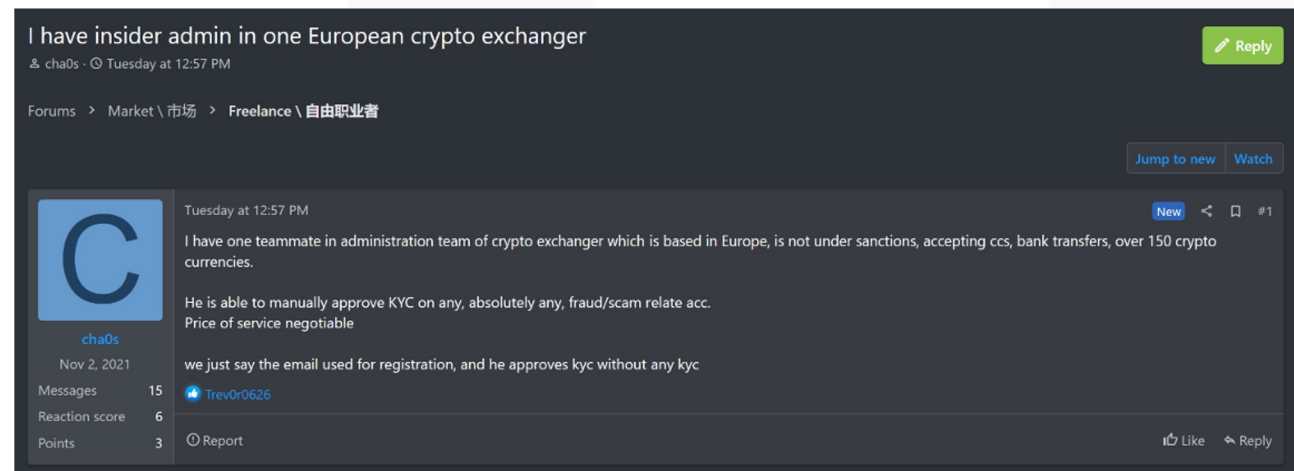
Price: \$ 500,000

Accepted only escrow of exploit.in

Report post

Insider Service Verifies Accounts For Undisclosed Cryptocurrency Exchange

Moderately credible threat actor “cha0s” advertised a service to verify accounts for an undisclosed cryptocurrency exchange based in Europe on the English language Deep Web forum “CryptBB”. The actor claims to have an insider who can manually approve the verification process for any account, including new accounts made using stolen PII or locked accounts suspected of fraud. The actor specified that the exchange accepts payment cards and bank transfers from Russia, indicating this service is almost certainly intended for threat actors looking to circumvent Russian sanctions. If legitimate, ZeroFox researchers assess this service could lead to an increase in fraudulent activity on the exchange, since it streamlines the process of creating money mule accounts for threat actors.



Actor Touts Automated Bot To Bypass PayPal OTP Codes

Well-regarded threat actor “VodafonePrime” advertised an automated bot they claim bypasses SMS one-time-password (OTP) codes for PayPal on the predominantly Russian language Deep Web forum “Club2Crd”. The announcement follows a recent trend where more threat actors are offering sophisticated OTP bots to bypass multi-factor authentication, especially in SIM swap scams.

The actor claims the bot works best to confirm payment transactions. The actor said that operators can also use the bot to log into a victim’s account but cautioned against this because doing so can trigger a new device alert that is automatically sent to the victim’s email account. While there are private licenses available for the bot, the actor claims they are also willing to negotiate a deal for the source code. This is significant because it could lead to the proliferation of new OTP bots with expanded functionality.

