



ZEROFOX[®]

Your Intelligence Digest

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

New Tool To Compromise VNC Servers

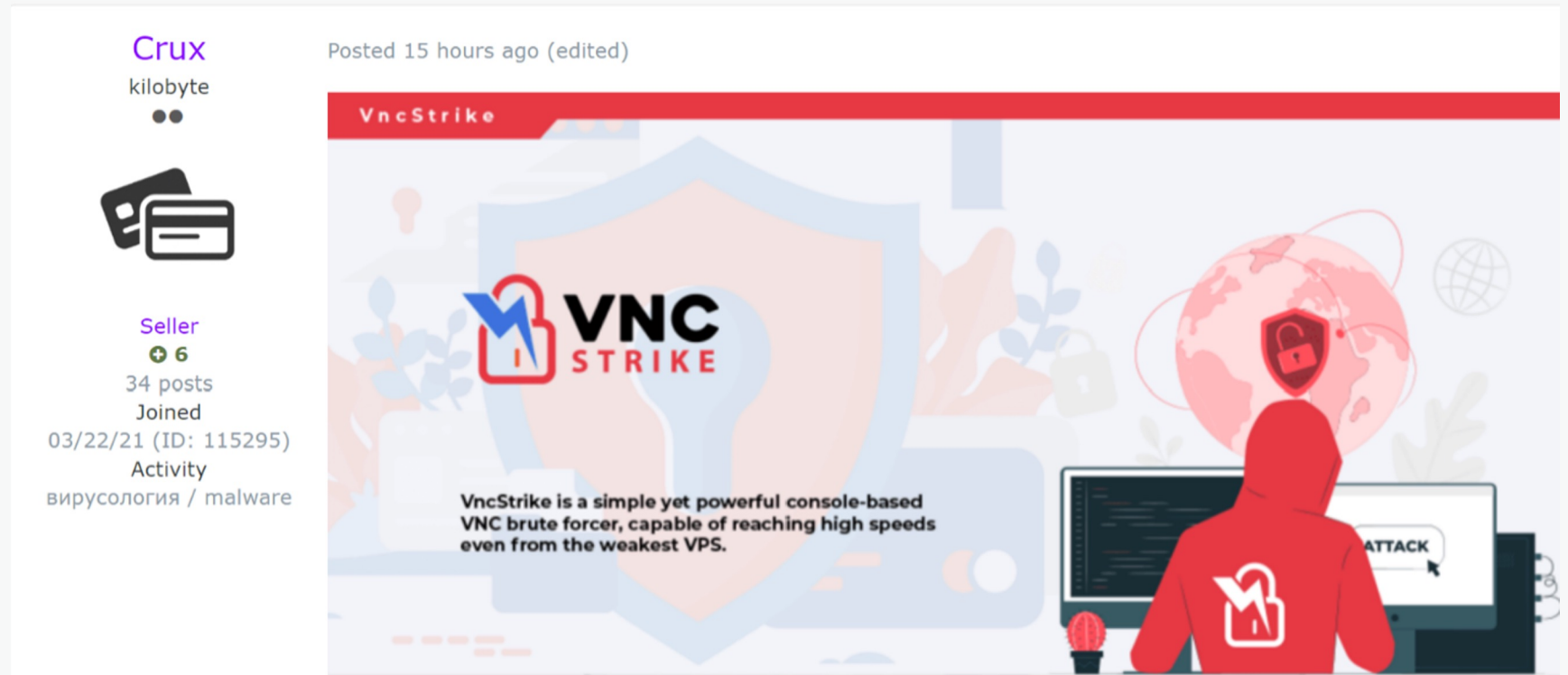
Well-regarded threat actor “Crux” advertised a new tool to compromise open virtual network computing (VNC) servers on the predominantly Russian language Deep Web forum “Exploit”. VNC is a cross-platform screen-sharing service that allows users to remotely control systems running Windows or Linux. The actor’s announcement is significant because it lowers the barrier to entry for threat actors to conduct these types of attacks by streamlining the process with an easy-to-use command line tool.

The actor specified the tool, dubbed VncStrike, works on hosts running most versions of Windows. According to the actor, this tool determines if IP address and port number combinations are associated with open VNC servers. If valid, the tool can use lists of known VNC passwords to perform credential stuffing attacks against the target machines. When a VNC server is successfully compromised, the tool will automatically return screenshots of the desktop. The actor claims the tool can compromise between 50 to 100 VNC servers per day, depending on the specifications of the host machine.

The actor charged \$500 USD for the tool. They also agreed to use an escrow service, indicating the actor is more likely to have what they claim.

Original post from threat actor "Crux" advertising a new tool to perform credential stuffing attacks against Windows machines running virtual network computing (VNC) instances

New Tool To Compromise VNC Servers (Cont.)



Automated Service Checks Validity Of Stolen Payment Cards

New and untested threat actor “Alphas” advertised an automated service to check the validity of stolen payment cards on the predominantly Russian language Deep Web forum “Club2Crd”. The actor claims this new service, also dubbed “Alphas”, will not trigger alerts to victims or card issuers. Additional features of the service include:

- Checks up to 500 cards per hour
- Free BIN search to identify card issuers
- Leverages stolen card data from various countries, including the U.S., U.K., Australia, and Canada
- Determines if cards have 3D Secure (3DS) enabled for multi-factor authentication
- Verifies CVV2 security codes
- Supports various payment card brands, including Visa, Mastercard, American Express, and Discover

The actor charged \$0.01 USD per check. They also claimed to offer discounts on orders of \$100 or more.

If legitimate, ZeroFox researchers assess this service could lead to a surge in payment card fraud since it increases the likelihood of a threat actor’s success by identifying payment cards with weaker security controls to target.

Original post from threat actor "Alphas" advertising a new automated service to check the validity of stolen payment cards

Automated Service Checks Validity Of Stolen Payment Cards (Cont.)

20-08-2022, 08:57

Alphas ▾
Junior Member



ALPHAS

Card Checking Service

NO Kill / NO Flag / Free 3DS check / Free Bin Check

Our Card Checking service automated website Features :.

- * Bulk checking (each user can check up to 500 cards Per hour) .
- * Automatic Deposits system supports 11 crypto currencies : XMR / BTC / ETH / BCH / Doge / LTC / TRX / USDT (trc20) / SOL / DOT & UNI
- * Free Bin search user can check up to 1000 Bins in 1 click for free . our Bin Database supports over 370,000 Bins 2021 updated.
- * Ticket message system / jabber / Telegram & TOX Support .
- * TOR + Direct URL Available

Checker Gate 1 Is our first Payment Gateway Integrated into our online card checker system . more payment gateways will be added soon

Join Date: Aug 2022

Posts: 7

Reputation: 0 [+/-]

Balance: 0.00\$



Actor Claims PII Of 2 Million Individuals Tied To U.K.-Based Lender

New and positively trending threat actor “Entropy” advertised access to a database and Amazon S3 bucket they claim contains the PII of two million individuals associated with a U.K.-based peer-to-peer lender, called The Money Platform, on the predominantly Russian language Deep Web forum “XSS”. In addition to the full information of victims, the actor said these resources also contain 32,000 scanned copies of sensitive documents used for customers verification purposes, including:

- Driver’s licenses
- Passports
- Photos of victims holding their ID cards

The actor charged \$2,000 USD for the access.

ZeroFox researchers assess that a deal involving this data will likely lead to more cases of identity theft against users of The Money Platform because the leak contains a comprehensive set of PII and verification documents impacting a high volume of lenders and borrowers.

theMoneyPlatform | UK Payday Loans | 2 Million Borrowers | 32K KYC Docs | Access DB & S3

Entropy · Четверг в 16:38

В ЭТОЙ ТЕМЕ МОЖНО ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКИЙ ГАРАНТ!

+ Новая сделка



Entropy
HDD-drive
Пользователь
Регистрация: 05.06.2022
Сообщения: 25
Реакции: 7

Четверг в 16:38

1 - MAIN DATABASE:
contains 2million borrowers records, equifax searches...
you can find all tables of the database in this diagram
DB ERP



Verified Bank Accounts For Money Mule Operations Advertised

New and untested threat actor “BullFrog” advertised Blackcatcard bank accounts verified using stolen PII on the predominantly Russian language Deep Web forum “WWH-Club.” This follows a recent trend where more threat actors are leveraging alternative banking services, such as Blackcatcard or Revolut, for money mule operations. These services allow threat actors to create free bank accounts with integrated cryptocurrency wallets that can be leveraged to cash out funds from compromised bank accounts or payment cards.

Additionally, the actor specified that Blackcatcard users can generate an unlimited number of virtual credit cards (VCCs) for fraudulent operations.

The actor charged \$400 USD per account. After purchase, the actor said they would also provide the buyer with a copy of the stolen PII used to verify the account.

