



ZEROFOX[®]

Your Intelligence Digest

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

New Ransomware Project Open To Affiliates

New and untested threat actor “MNSTR” advertised a new ransomware-as-a-service (RaaS) project, dubbed “MONSTER”, on the Russian language Dark Web forum “RAMP”. This marks the second time in the past month that ZeroFox researchers have observed a ransomware gang advertising an affiliate program on the forum. This comes after months of silence from ransomware groups across the underground, indicating ransomware attacks are likely to rise. Features of the ransomware include:

- Does not contain software dependencies
- Works on machines that run any version of Windows
- Displays list of files being encrypted
- Automatically changes permissions to take full control of files
- Ends running processes to encrypt more files
- Empties Recycle Bin and deletes Restore Points to make recovery more difficult
- Encrypts hidden partitions
- Scans for files and shared folders across the network

The actor also specified that this ransomware checks the location and validates the IP address of a target to avoid spreading the malware in CIS countries. This differs from previous ransomware variants that leveraged system language information to make that distinction. ZeroFox researchers assess that this change in behavior is likely due to more publications advising organizations to install Russian language keyboards on their systems to avoid malware triggering on their systems, forcing ransomware developers to adjust their methods.

The threat actor agreed to split the profits from any successful ransom payments 80-20 in favor of affiliates.

Original post from threat actor “MNSTR” advertising a new ransomware-as-a-service (RaaS) project.

New Ransomware Project Open To Affiliates (Cont.)

[RaaS] MONSTER Ransomware
MNSTR · Wednesday at 12:01 PM

Forums > Market \ 市场 > Partners Program \ RaaS \ 合作伙伴计划

Jump to new Watch

**MNSTR**
Jun 14, 2022
Messages 2
Reaction score 1
Points 3

Wednesday at 12:01 PM
MONSTER Ransomware 80/20
[Spoiler: Скриншоты / Screenshots / 屏幕截图](#)

- Вкл/выкл интерфейса пользователя аргументом командной строки и/или комбинацией клавиш (может отображать список обрабатываемых файлов, есть возможность запуска отдельных функций, шифрования отдельных файлов/дисков/сетевых путей, старт/пауза/самоуничтожение и др.)
- Поддержка drag&drop и обработка параметров командной строки (обработка отдельных каталогов/файлов, возможность задавать свое расширение, вкл/выкл отдельных функций)
- Работа с привилегиями и правами доступа к каталогам/файлам (автоматическое получение прав и установка владельца)
- Быстрая одновременная разблокировка всех занятых файлов
- Завершение процессов/сервисов, очистка корзины и точек восстановления

Discord Spamming Service Announced

Moderately credible threat actor “Maduro” announced their new Discord spamming service on the Russian language Deep Web forum exploit[.]in. The actor claims that this service can send messages en masse to all users on a server, regardless of whether that server is public or not. The actor claims that operators can also specify which servers they would like to target by providing them with the appropriate channel invite codes.

Threat actors with the requisite technical skills could leverage this service to:

- Increase web traffic to malicious websites
- Spread malware
- Compromise cryptocurrency wallets

Prices for the service vary depending on the number of messages a threat actor would like to send, from \$125 USD for 5,000 messages to \$9,900 USD for 1,000,000 messages.

If legitimate, ZeroFox researchers assess that this service will likely lead to an increase in spam campaigns across Discord, since it effectively lowers the technical bar of entry for threat actors looking to launch these attacks.

Original post from threat actor "Maduro" announcing their new Discord spamming service.

Discord Spamming Service Announced (Cont.)

Maduro

megabyte

...



Paid registration

2

51 posts

Joined

10/01/20 (ID: 109121)

Activity

безопасность / security

Posted Saturday at 11:27 AM (edited)

Report post

Need to mass market your products and services all over targeted and untargeted Discord channels? Want to spam the hell out of a rival? Have a shit talking enemy who runs a Discord room with many users and you want to get your message across to all those users and convert them into your clients? Thats exactly what this service is about.

Why play fair in marketing when there are many shortcuts to take? No matter what your message is.....our Discord spam service will get your messages across no matter what.

Need traffic from gamers? We can do a drive-by spam hit and run with your message and your links. Need to circulate your crypted exe? A Discord spam hit and run is just what the doctor ordered. Crypto hunting? Same deal. A Discord spam run is what you want.

No matter what product, service, or website you want traffic to, a spam run on Discord will get it to you.

And who really cares what you are marketing? The point is to get your message across to the right people that are going to respond to whatever you have to sell, offer, or even give away.

All we need from you to start is your messages, any graphics you want included, and the channel invite codes for the channels you want us to blast. We'll handle the rest.

Pricing for Messaging Packages:

5,000 Messages:	\$125 USD
10,000 Messages:	\$225 USD
25,000 Messages:	\$500 USD
50,000 Messages:	\$750 USD
100,000 Messages:	\$1250 USD
250,000 Messages:	\$2350 USD
500,000 Messages:	\$4400 USD
750,000 Messages:	\$6700 USD
1,000,000 Messages:	\$9900 USD

Telegram Contact: <https://t.me/proxiestv>

Threat Actor Scheme Targets Wealthy Cryptocurrency Investors

Untested threat actor “millyrock59” is looking for partners who can supply them with databases that contain the PII of wealthy cryptocurrency investors, on the Russian language Deep Web forum exploit[.]in. The actor claims they can scan these datasets for AT&T email domains and reset the passwords to perform account takeovers. Some of the alleged email domains include:

- @att.net
- @bellsouth.net
- @sbcglobal.net
- @currently.com
- @flash.net
- @nvgbell.com

The actor or group claims that they have previously compromised AT&T email accounts associated with different cryptocurrency wallets and tax services to identify their victims’ cryptocurrency assets and seed recovery phrases.

ZeroFox researchers assess that this threat actor could be exploiting a vulnerability in Yahoo Mail, since the AT&T email domains they referenced leverage this service.

Original post from threat actor “millyrock59”, who is looking for partners to supply them with databases that contain the PII of wealthy cryptocurrency investors.

Threat Actor Scheme Targets Wealthy Crypto Investors (Cont.)



We can reset passwords for all AT&T emails e.g. @att.net, @bellsouth.net, @sbcglobal.net and many more

By millyrock59, Saturday at 08:41 PM in [Mobile communication] - receiving calls, sms, info lookups, detailing

Follow 2

Start new topic

Reply to this topic

millyrock59

byte



Paid registration



11 posts

Joined

12/27/21 (ID: 123663)

Activity

activity / other

Posted Saturday at 08:41 PM

We're looking for new partners that have wealthy crypto investor mail lists / databases. It is not good enough if it is just crypto related, it has to have indications that the targets from it are wealthy. Below is a list of some databases we already did in the past.

Crypto tax software databases (easy to see where all the money is):

- Zenledger
- Coinledger
- Accounting
- Koinly
- Taxbit

Wallet databases (good for finding seed phrases):

- Trezor
- Ledger/Ledger Enterprise
- Keepkey
- Coinomi

Report post

New Telegram Shop Selling Compromised Facebook & Google Accounts

Well-regarded and established threat actor “fooble” advertised a new, automated Telegram shop that specializes in the sale of compromised Facebook and Google accounts on the Russian language Deep Web forum exploit[.]in. This follows a recent trend observed in the underground as more threat actors are leveraging automation to streamline their operations. Services such as Telegram offer threat actors a cheaper, more secure alternative to traditional shops on the Deep or Dark Web.

According to the actor, this new shop has Facebook accounts with spending limits between \$250 USD to \$1,500 USD from the U.S. and various European countries. The price per account starts at \$0.30 USD.

The shop also has Google Pay and Gmail accounts from \$0.40 USD each.

Additionally, the actor takes requests to check their logs for additional compromised accounts for services other than Facebook or Google for a minimum of \$100 USD per request.


FACEBOOK & GPAY-GOOGLE - AUTO SALE BOT
 By fooble, June 18 in [Finance] ~ billing, banks, accounts, logs

fooble

Logs



Paid registration
 54
 878 posts
 Joined
 06/03/20 (ID: 104955)
 Activity
 xavier / hacking
 Deposit
 0.033157

Posted June 18

AUTO SALE TELEGRAM BOT
Now You could buy fresh Facebook and Gpay in our store at any time.

FACEBOOK:
Limits accs 250-1500\$ in stocks
Unsettled accounts
TOP GEO(US,EU,MIX)
Spends accounts with Limits 250-1500\$
prices from 0.3\$

GOOGLE:
Gpay (No ads)
Gpay + spends
GMAIL (no ads)
prices from 0.4\$

LINKS REQUEST:
We have more then 200kk email:pass/log:pass , will find any of you link request contact to support.
minimum order 100\$

*Fast supporting and money back system , Special prices for bulk customers, Low prices at markets.
Welcome , we a waiting you guys.*