



Shifts in Underground Markets

Past, Present, and Future

Mayra Rosario Fuentes

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

Trend Micro Research

Written by

Mayra Rosario Fuentes

With grateful acknowledgment to

Ahmed Kamal Aly

Stock image used under license from

Shutterstock.com

For Raimund Genes (1963-2017)

Contents

5

What does the Underground Market Offer?

26

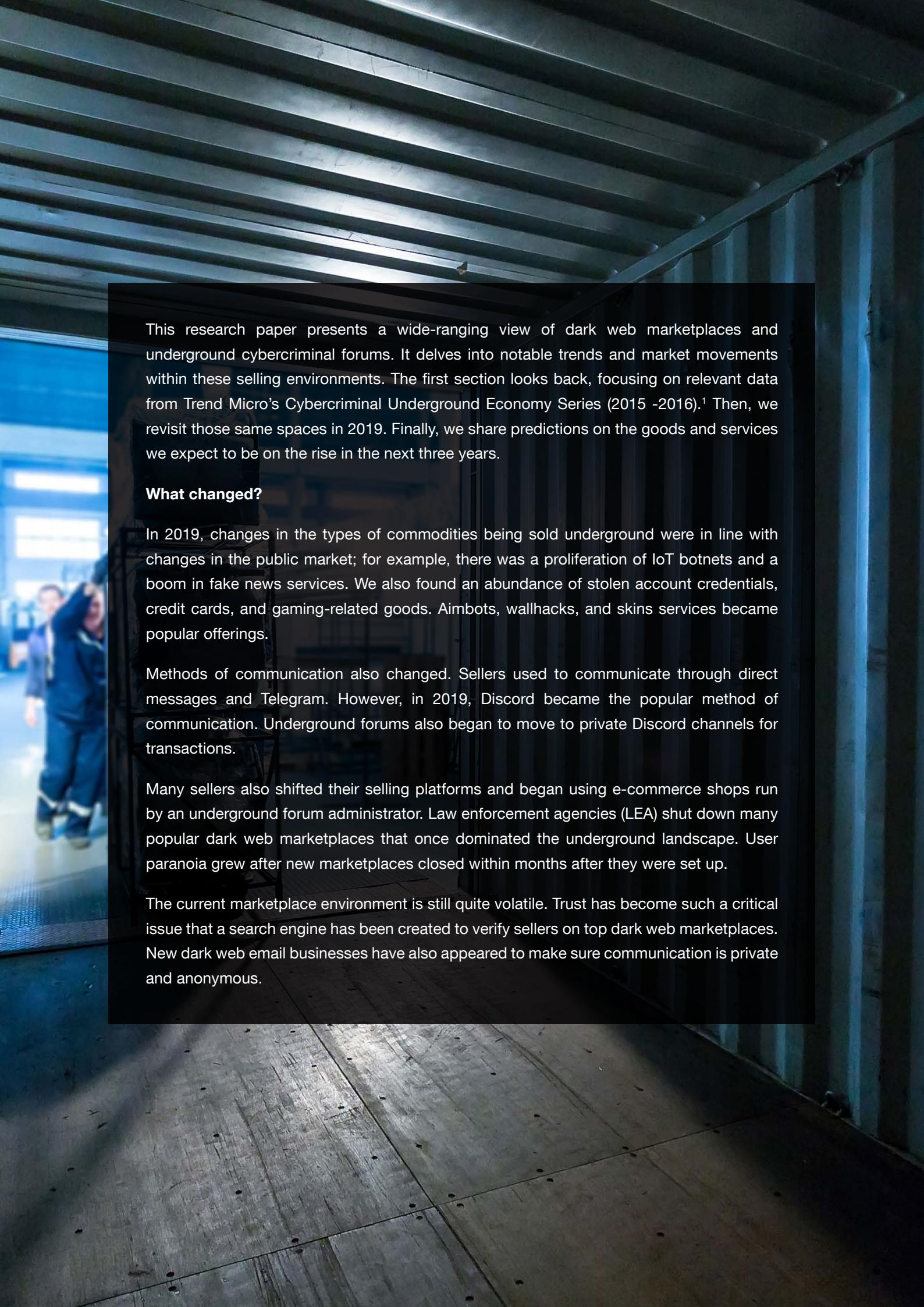
The Present State of Underground Forums and Marketplaces

62

The Future of Seller Spaces

63

Appendix of Prices



This research paper presents a wide-ranging view of dark web marketplaces and underground cybercriminal forums. It delves into notable trends and market movements within these selling environments. The first section looks back, focusing on relevant data from Trend Micro's Cybercriminal Underground Economy Series (2015 -2016).¹ Then, we revisit those same spaces in 2019. Finally, we share predictions on the goods and services we expect to be on the rise in the next three years.

What changed?

In 2019, changes in the types of commodities being sold underground were in line with changes in the public market; for example, there was a proliferation of IoT botnets and a boom in fake news services. We also found an abundance of stolen account credentials, credit cards, and gaming-related goods. Aimbots, wallhacks, and skins services became popular offerings.

Methods of communication also changed. Sellers used to communicate through direct messages and Telegram. However, in 2019, Discord became the popular method of communication. Underground forums also began to move to private Discord channels for transactions.

Many sellers also shifted their selling platforms and began using e-commerce shops run by an underground forum administrator. Law enforcement agencies (LEA) shut down many popular dark web marketplaces that once dominated the underground landscape. User paranoia grew after new marketplaces closed within months after they were set up.

The current marketplace environment is still quite volatile. Trust has become such a critical issue that a search engine has been created to verify sellers on top dark web marketplaces. New dark web email businesses have also appeared to make sure communication is private and anonymous.

According to an academic study on the cybercrime economy, cybercrime (which includes ransomware, sales of counterfeit goods, data theft, and others) generates around US\$1.5 trillion in annual revenue.² This widespread business outpaces top global revenue earners like Apple (US\$260 billion in 2019),³ Saudi Aramco (US\$356 billion in 2018),⁴ and Amazon (US\$281 billion in 2019).⁵

English and Russian remain the dominant languages in the cybercrime market. And although many markets have been taken down by law enforcement agencies, we found that some popular hacking and cybercrime forums were still operating at the start of 2020, namely: Exploit[.]im (forum moves around and also uses Exploit[.]jin), Hackforums, Nulled, Raid Forums and Joker's Stash. We also found that their membership numbers continued to increase.

The cybercriminal underground is not as separated by language as much as it was five years ago. We spotted overlapping posts and cross-market advertising in forums of different languages. Russian actors regularly participated in English and Arabic forums, while Spanish actors participated in English forums. It seems cybercriminals have adopted a more global view and found that advertising in multiple language forums is a must if they wanted to earn more money. Still, the cybercriminal underground economy remains diverse, and different markets carry unique goods and services for the country or region to which they cater.

Prices for different commodities have fluctuated since our 2015 reports on the Russian and English underground. In 2015, generic botnets started selling at around US\$200 in Russian underground forums. Generic botnet prices today cost around US\$5 a day, and prices for builders start at US\$100. United States credit cards were sold at US\$20 in 2015, but prices start at US\$1 in 2020. High-balance credit cards are selling for over US\$500 in 2020. Meanwhile, monthly crypting services dropped to around US\$20.

The cost of some services and goods remained relatively stable. Ransomware has not changed—ransomware-as-service prices still start at US\$5. Crypterlocker, which has been around since 2013, continues to demand a high price (around \$100). Scanned document services, such as copies of driver's licenses, passports, and bill statements, still start at US\$5 — similar to the prices in 2015. Similarly, the price of remote access tools (RAT) did not change, starting at US\$2 for malware-as-a-service (MaaS). NJRat, which has been around since 2012, continues to be found in multiple language forums for free. Online account credentials are still priced at around US\$1. The price of spam services has not changed, but they are now sending SMS rather than emails.

One notable trend we observed is accessible MaaS services for RATS, crypters, botnets, and ransomware. The MaaS service model delivers a complete package: infrastructure, support, and updates. These services are also affordable, with some MaaS offerings starting at around US\$20 a month. There is virtually no pricing barrier, and the technical skills that buyers need to have to setup attacks have been greatly reduced.

What does the Underground Market Offer?

Regular monitoring of the cybercriminal underground shows us that the range of available goods and services has not radically changed. Over ten years, underground market staples—stolen accounts, fake documents, credit card dumps, remote access tools, ransomware, and crypters—remain consistently available. Currently, the top offerings are stolen accounts (banking, social media, streaming services and music services), gaming-related content, and credit cards. Point of sale (POS) and ATM malware sales account for 6% of all the offerings.

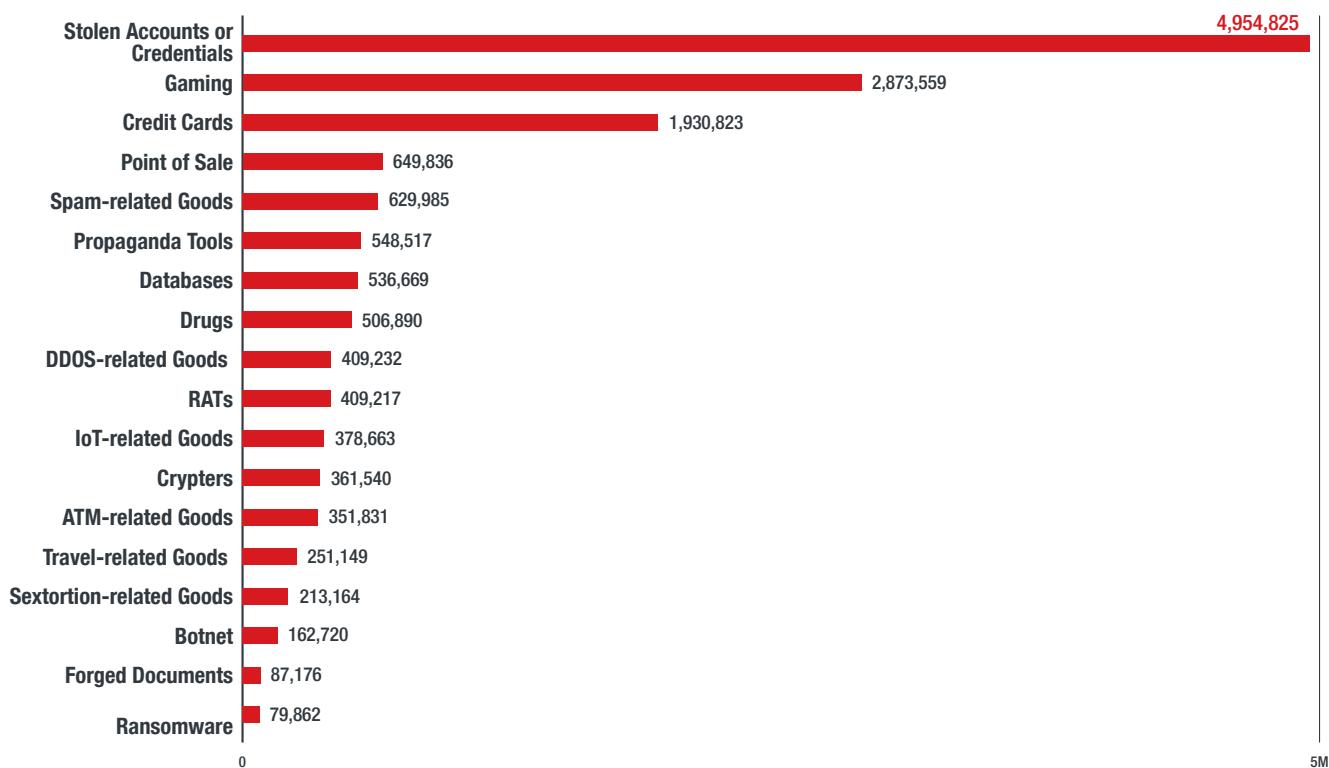


Figure 1. Popular underground goods and services

The above breakdown is based on the number of thread discussions in 600 forums across multiple languages. Every mention and thread reply related to the topic was included.

In this chart, “internet of things (IoT)” includes malicious goods or services affecting routers, doorbells, Nest devices, webcams, supervisory control and data acquisition (SCADA), industrial control systems (ICS), smart pumps, smart meters, Alexa devices, Google Home devices, smart lights, drones, and IoT-based botnets. “Travel-related goods” includes hotel tickets, airline tickets, food gift cards, Uber- and Lyft-related goods, and airline miles. “Gaming” includes stolen account sales, wallhacks, aimbots, gaming hacks, discussion about games, and skin sales.

The sections below will go into greater detail about the goods and services offered in English, Russian, Spanish, and Arabic underground sites, highlighting the basic costs and notable offerings within the forums.

Distributed-Denial-of-Service and Botnets (non-Mirai)

Many different botnet services are sold in the underground: cryptocurrency mining, click-fraud, IoT device attacks, spamming, and spreading banking trojans. In our Russian underground report from 2015,⁶ botnet prices averaged around US\$200. Five years later, the most expensive non-Mirai botnets we found cost US\$1,500, and buyers can pay a daily, weekly, or monthly fee starting at US\$5. Aside from the Mirai-based botnets, Android botnets usually demand higher prices in the underground.

The screenshot shows a forum post from March 10, 2019, titled "Powerfull DDoS Service # 1 powerful DDoS service No. 1". The post details a DDoS service offered by a team that provides services for DDoS attacks on Layer 7 (sites) / Layer 4 (servers) / ONION sites. It lists various types of attacks including UDP, TCP, and DNS amplification, mentioning private software developed personally by the user. The post states that attacks are performed 24/7 and guarantees enforcement of any site even if others have failed. It also mentions blackmail schemes and offers unlimited sites. A section titled "Our Advantages" lists numerous benefits such as experience, private software, no intermediaries, fast tests, power range from 100,000 to 50,000,000 PPS, Kruglosutochny Monitoring, full anonymity, online 24/7, and flexible conditions for customers. Payment methods listed include BTC, ETH, DASH, QIWI, WebMoney, and YandexMoney. The price is noted as starting from \$50 a day.

Figure 2. DDOS service from a Russian language forum starting at US\$50 a day

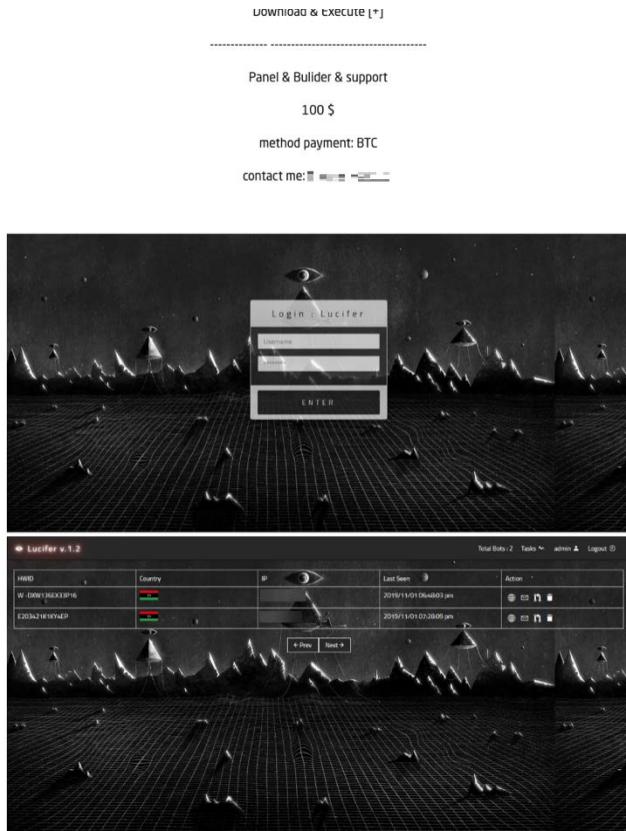


Figure 3. Lucifer botnet advertised in an Arabic and Russian language forum for US\$100

The screenshot shows a forum post with the following text and interface elements:

I offer you high-quality DDoS Attack!

A round-the-clock DDoS service specializing in conducting powerful high-speed attacks.
We will help you solve problems on the Internet.
Disable Internet Sites, Forum!

About Us (RU):

- > Online 24/7.
- > Customer anonymity.
- > The solution to any conflicts among competitors.
- > We work with protection of any complexity.
- > We make analysis, test.
- > Target monitoring.
- > We work without intermediaries.
- > Our software guarantees high quality services.
- > Resellers and Scammers - please do not worry.
- > We resolve the remaining issues on the spot.

About Us (ENG):

- > Online 24/7.
- > Anonymity of the client.
- > Solving any conflict among competitors.
- > We work with any complexity protection.
- > We do the analysis, we test.
- > Monitoring the goal.
- > We work without intermediaries.
- > Our software guarantees high quality of services.
- > Resellers and testers - please do not worry.
- > We will answer the rest of the questions on the spot.

Types of attacks:
get / post / syn / udp / icmp / dns-ampl / xmppc

Prices from \$ 50

Figure 4. DDOS-as-a-service starting at US\$50; the service includes 24/7 support, reseller services, and target monitoring

Botnet (non-Mirai) prices	
Generic Android botnet	Up to US\$1,500
Generic DDOS botnet	US\$50 a day
Panel.builder for a form grabber botnet	US\$100
Botnet rentals	US\$5 and up
Generic botnet builds	Free and up

Remote Access Tools

Remote access tools (RATs) allow cybercriminals to control a system remotely, and variations of these tools are commonly sold in underground forums and sites. Buyers can purchase RATs with additional features such as keylogging, downloading and executing commands, and capturing audio and video using microphones or webcams. The cost of RATs remains unchanged since 2015, with prices still starting at around US\$5. Source code for older RATs like NJRat and RevengeRAT are often found for free — likely because they have been around for many years — and security solutions are equipped to deal with them. Spynote, which has been around since 2016, continues to be sold for US\$2 and up. Generic RATs start at around US\$50 for a build.

The screenshot shows a forum post for the "PENTAGON RAT". The post includes the following details:

- [PENTAGON RAT'S][2018][CAMERA ATTACK-HVNC-CONTROLPANEL][49.99\$]**
- 08-29-2018, 05:06 AM
- [PENTAGON RAT]**
Best 2018 Remote administration Rats with evil functions
- Keyloggers**
-Attack Camera
-Hack files
-Hidden Remote Desktop Acces
-Panel of Bots with function
- [PRICE]**
Builder+File+How setup -> 49,99\$
- [RULES]**
 - All sales are Final
 - We sell Builder and files
 - We can setup the Rats for additional price
 - We are not responsible of your use of the tools
 - Payment by BTC/ETH
- [CONTACT]**
- PENTAGON**

Figure 5. Pentagon RAT offered for US\$49.99 in an English language forum

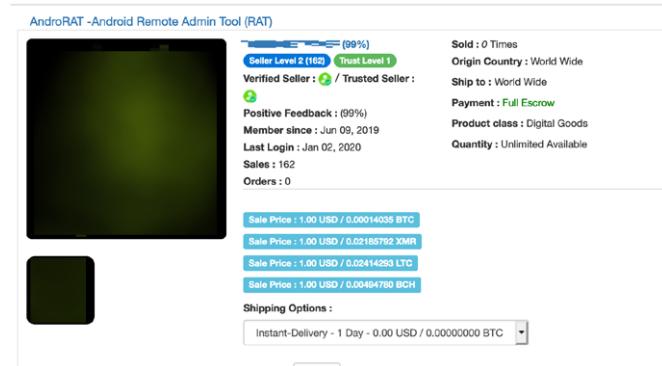


Figure 6. A dark web marketplace offering AndroRat install for US\$1

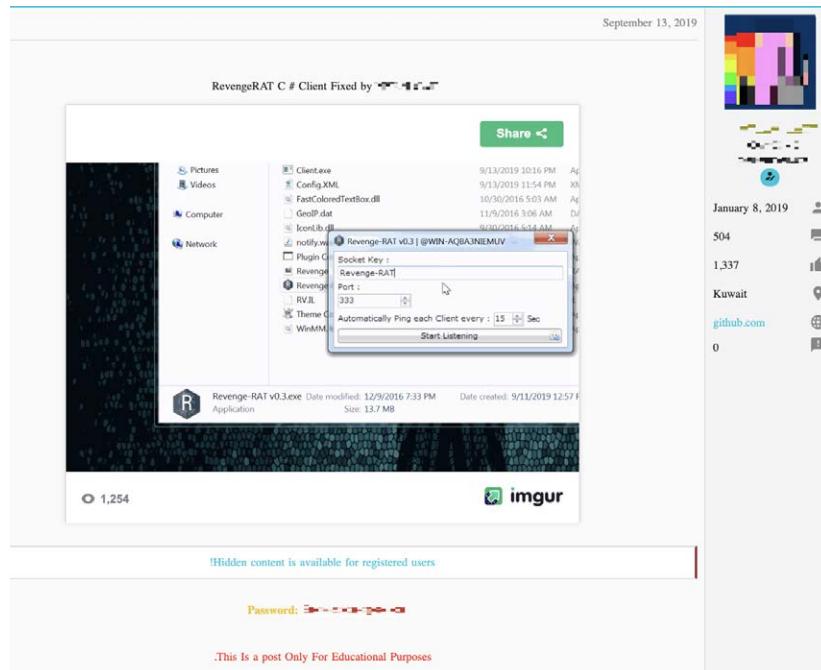


Figure 7. Free RevengeRat offered in an Arabic language forum

RAT prices	
RevengeRAT/NjRAT	Free
Generic Android RATs	US\$1 and up
Source code for a generic RAT	US\$49 and up
Monthly RAT subscriptions	US\$5 and US\$25

Ransomware

In 2016, ransomware was estimated to have generated at least US\$1 billion in global revenues.⁷ The affordability of ransomware during this period likely contributed to growth and earnings. In 2015, generic ransomware builds only cost around US\$5. And now, in early 2020, the cost for generic builds still starts at around US\$5. However, popular ransomware often mentioned in the news can cost more than US\$1,000.

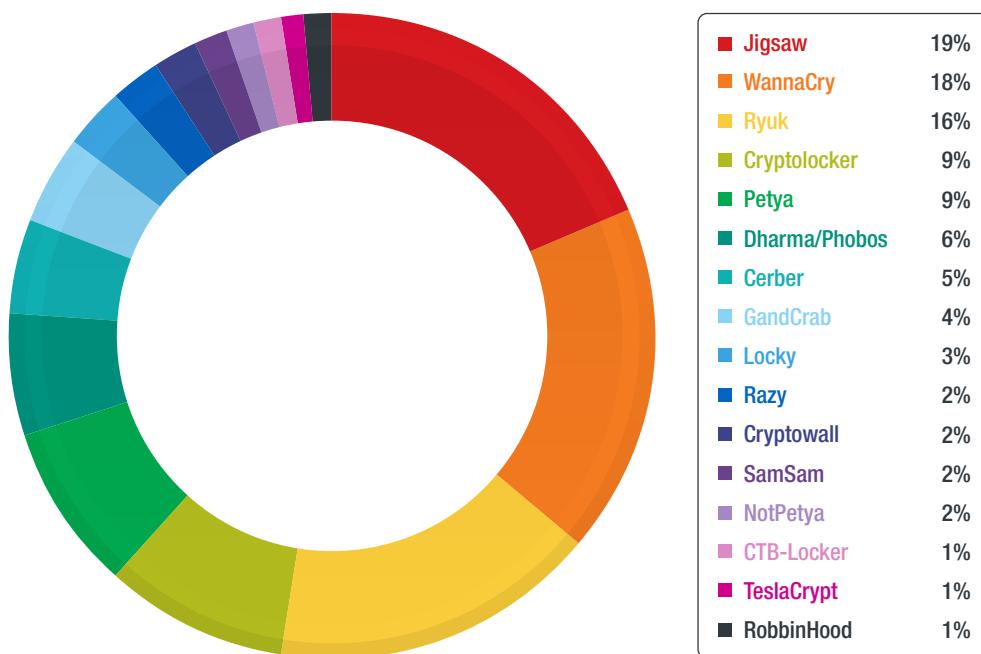


Figure 8. Top ransomware offerings

In 2019, ransomware prices varied depending on the family. Cryptolocker has been a pervasive threat since 2013 and continues to be one of the top five ransomware actively attacking victims. Builds for this variant can be found for US\$100 in Russian language forums. The Jigsaw ransomware family, which has been around since 2016, currently sells for US\$3,000 in English language forums. The Ranion ransomware-as-a-service has been around since 2017, with a yearly subscription that can cost up to US\$900. WannaCry is still available in the underground, but it's usually distributed for free.

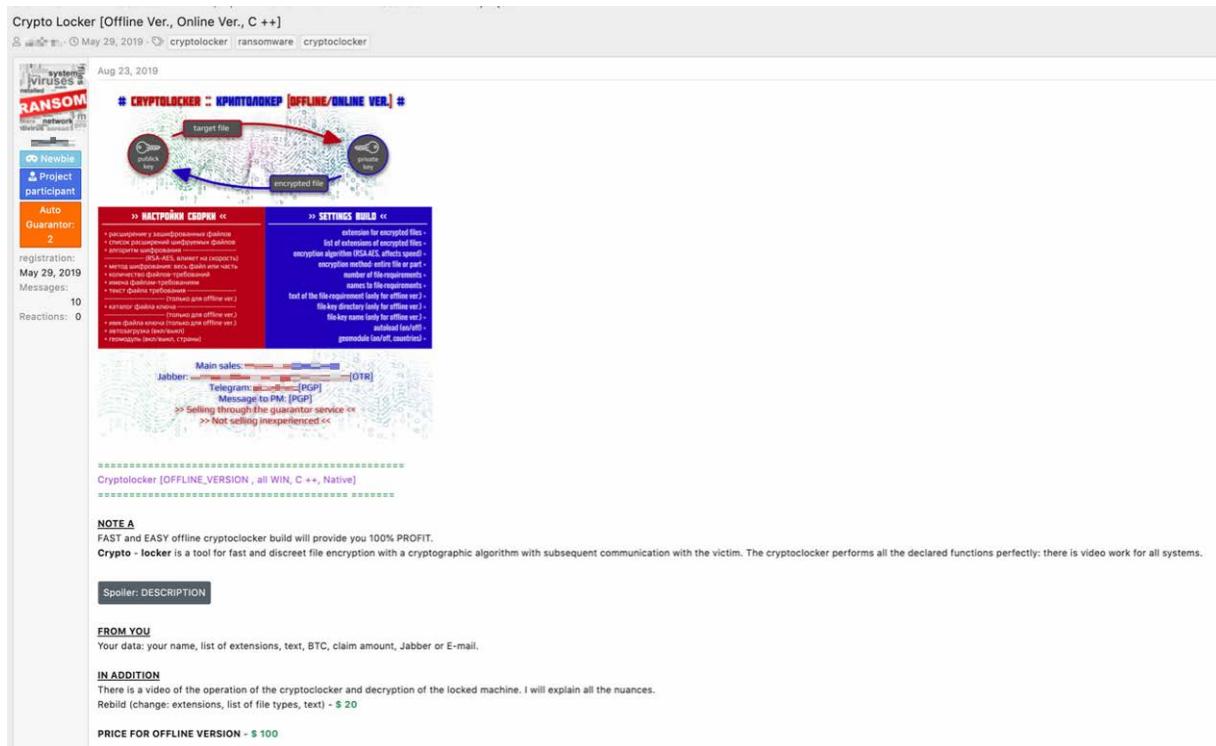


Figure 9. An offline version of Cryptolocker being sold for US\$100

Subscription Plans			
1 MONTH	3 MONTHS	6 MONTHS	1 YEAR
\$ 99 .99	\$ 249 .99	\$ 399 .99	\$ 699 .99
Darknet Dashboard	Unlimited Builds	Darknet Dashboard	Darknet Dashboard
Unlimited Builds	Offline Encryption	Unlimited Builds	Offline Encryption
Offline Encryption	Custom Disk Encryption	Offline Encryption	Custom Disk Encryption
24/7 Support	24/7 Support	Custom File Extensions	Custom File Extensions
		24/7 Support	24/7 Support

Figure 10. Ransomware subscription plan for Ghostly locker

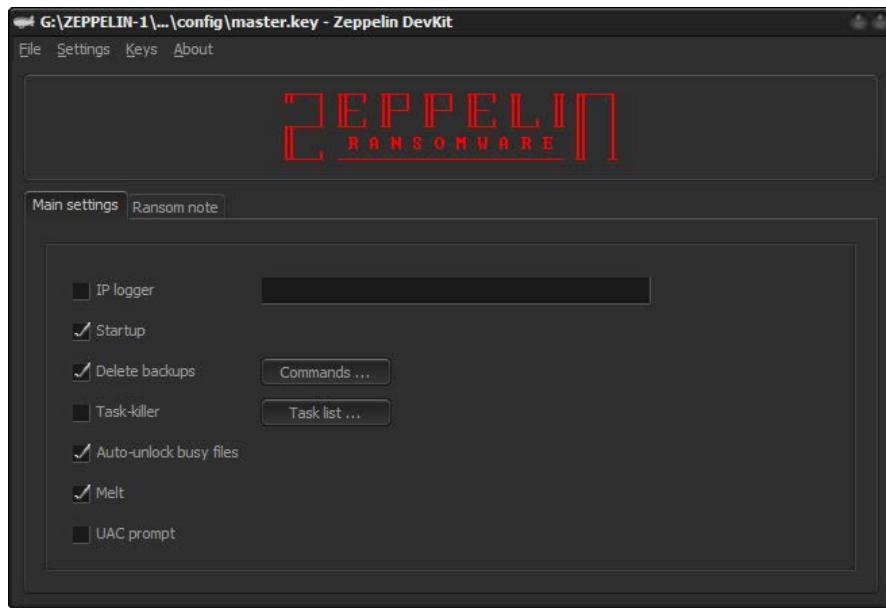


Figure 11. Zeppelin ransomware advertised in a Russian language forum

Jigsaw Ransomware V2.2019

Posted 07 April 2019 - 06:38 PM

This Ransomware was outdated and useless so we took the source code and rewrote it.

Now version 2 source code is available for sale as well as pre-configured already compiled version with many improvements:

Interface.

- Windows frame and icon in windows taskbar are now invisible, however you can still drag around the ransomware main window with the mouse to clear the browser visibility to make the payment,
- Instructions have now background transparency so the image of the Jigsaw is never opaqued
- A copy to clipboard Bitcoin Address button has been added for convenience.
- Links to both Bitcoin technology explanation and payment website address were added.
- Cool Wallpaper changer.
- Market BTC value is shown in real time in main interface.
- A Skinned version of the project is also available so you can easily change the look and feel if you wish to do so.

Payment system.

- The payment engine has been rewritten to make use of Block.io API interface (remember Blockr.io is dead). The engine is able to correctly locate and calculate the coinbase bitcoin price in USD and the present balance of your account to determine if payment was successful. You don't need to risk by giving any email address.

Security is enhanced.

- The ransomware now disables the task manager (it is restored after payment) to prevent being killed from memory.
- The ransomware also sets itself as an unkillable process. In case the user manages to kill it, the whole windows will crash with a BSOD.
- A doomsday counter is configurable. If the user kills the ransomware too many times, then its clear he won't pay so better erase the whole hard drive and kill boot sector.
- Available public jigsaw ransomware decrypers can not decrypt the files.
- Virus is totally FUD in the hard drive after processed by our method.
- The virus does not relies on costura.fody to deploy its dll files because it is unreliable. Now the virus includes and deploys its own required dll files.
- USB Stick Spreading.
- Network drive spreading.
- Spreading through email attachment.
- Autorun enabler for removable devices.
- EternalBlue Exploit scanner. Results are sent by email to the attacker.
- Windows defender is disabled. Can't be turned back on easily and it will stay off after restart. Also AVG and MalwareBytes.
- Bot Killer added.
- Hidden visit website feature. It will regularly visit any website of your choice using the victim's connection. Can be used to increase visits counter as an example (won't work for monetizing links).
- Windows explorer options modified so hidden files can not be seen (might not always work depending on OS version or may require restart).
- Anti sniffers code.
- Windows Update Disabler.
- System Restore Killer (might not work in all windows OS).
- Disable UAC (no admin for victim).
- Disable Regedit.
- Disable CMD.
- Windows Serial Number retrieval. Send back to attacker by email.
- Second method for extensive password dump&retrieval (including browsers, ftp clients, email clients and other goodies).
- New USB spreading technique not relying on autorun being turned on.
- DoublePulsar Exploit implementation. It can upload a DLL file to vulnerable computer. Three DLL examples are provided: To add a admin user, to download and execute any file from a selected website, to reboot system.
- Use the app as ransomware or as worm. Option to not encrypt any file and not request any ransom, only spread through different mechanisms and install rat or any other file of choice.
- Change permissions of all files belonging to all the users in a server so they can now be encrypted.
- Businesses and Enterprises databases encryption.

Figure 12. Jigsaw ransomware offered in an English language forum for US\$3,000

Ransomware prices	
Generic ransomware build	US\$5 and up
Ranion ransomware	US\$900 a year
Cryptolocker binary	US\$100-400
Cryptolocker source code	US\$3,000
Jigsaw ransomware source code	US\$3,000
Dharma binary	US\$100
Ryuk ransomware as a service	US\$395-1,200 a month
Zeppelin builder	US\$2,000

Crypting Services

Our research paper on the North American Underground in 2015⁸ found that monthly crypting services were being sold for up to US\$1,000 a month. The prices for these services have since become significantly lower. The average cost for crypting is around US\$100 a month, but some services can be found for as low as US\$20.

In the Russian underground, basic prices remain at around US\$20, the same as in 2015. More sophisticated crypters found in Russian language forums can sell for up to US\$2,000.

11/05/2019 Topic Author #1

We present to your attention the ZEPPELIN offline cryptographic builder.

We took into account all feedbacks and wishes, working with an affiliate program, implemented the planned bells and whistles in file encryption, combined with existing developments and received a completely new product with a universal data processing algorithm. After conducting serious tests, it was decided to build a builder so that everyone who bought a license for our software had a unique opportunity to work regardless of any affiliate program.

Screenshots of the main window of the builder: Some features of the builder:



- Support for multiple master keys
- Saving locker in .EXE, .DLL and .PS1 (PowerShell) formats
- Options: IP logger / autoload / start of the specified commands on the attacked machine (deleting recovery points) / termination of the processes on the list / auto-unlock of files that are not writable / self-deletion / request for rights / ransom request editor
- Saving and resetting settings

A short list of features of the current implementation:

- A strong encryption algorithm that has established itself as extremely reliable and unbreakable (custom implementation of AES CBC, without CryptoAPI, its own RNG is used, brute force is impractical)
- Installation into the system under a randomly selected name, obtained on the basis of a list of processes running on the system under attack
- Using multi-threaded asynchronous file search, where for each drive and network path a separate stream works
- Encryption of files with "bands", this guarantees the impossibility of even partial recovery of large files with databases and archives
- The ability to execute arbitrary commands before starting the search and data encryption (deleting recovery points, etc) // optional
- The completion of processes on the attacked machine according to the list // optional
- Automatic termination of processes blocking access to files if they are not available for encryption // optional
- All builds (.EXE, .DLL and .PS1) function correctly on the entire OS line from Windows XP to later
- Builds do not work on CIS systems

Scope of delivery: builder + configs + manual.

Starting price for the builder: \$ 2000, global updates \$ 100, small fixes - free.

Figure 13. Zeppelin crypto builder offered at US\$2,000 in a Russian language forum

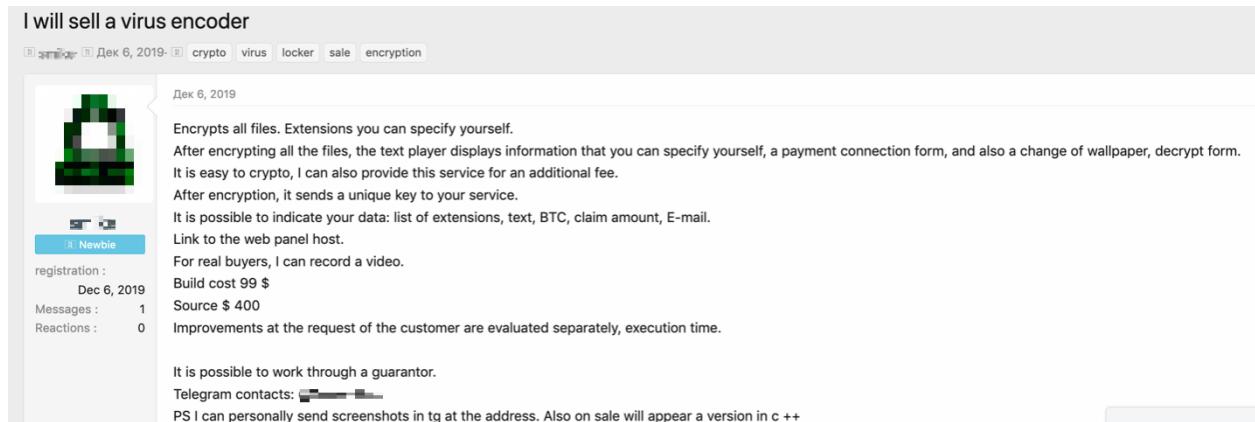


Figure 14. A crypter source code offered for US\$400 in a Russian language forum

Price Plan	Price
1 month	20 eur
6 month	100 eur
1 year	170 eur
lifetime	300 eur

Figure 15. Crypter service from US\$25 a month in an English language forum

Crypter prices	
Generic crypter builders	US\$99 and up
Crypter as a service	US\$20 and up

Banking Malware

We have been observing the banking malware landscape for years, independently and in collaboration with Europol's European Cybercrime Centre (EC3). Our most recent report, *Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground*⁹ was released in June 2019. Observing the landscape throughout 2019, we noted that the Cutlet Maker, Hello World, and WinPot banking malware variants continue to be found on Russian-speaking underground markets, priced at around US\$2,000.

The Kronos banking trojan, which first appeared in 2014 in Russian language forums, evolved into Osiris and offered for US\$3,000 in 2019. Android banking trojans continue to be popular in the underground for US\$300 and up. And even though multiple GozNym cybercriminals were arrested in mid-2019,¹⁰ the malware itself is still highly valued. GozNym continues to be sold in the underground at US\$750.

The screenshot shows a forum post titled "OSIRIS BOTNET - TOR CONNECTION | NATIVE | HVNC + MORE Showing all posts" from August 07, 2019, at 06:44 PM. The post has one reply (#1). The user is identified as "[VIP] [REDACTED]" and is a "V.I.P User". The post discusses the features of Osiris, a C++ Trojan over Tor, previously known as kronos. It highlights its native bulletproof botnet, support for various browsers (Internet Explorer, Firefox, Chrome, Opera, Edge), and various attack vectors like Formgrabber, Web Injects, Keylogger, Log Parser, and Bot Update. It also mentions password recovery for Outlook and Address Book Extractor, and support for VMware, AntiSandbox, and AntiDebug. The bot is described as being 330kb in size and having a hidden VNC feature. The price is listed as \$5000, with a note that it includes a lifetime license and free updates.

OSIRIS BOTNET - TOR CONNECTION | NATIVE | HVNC + MORE Showing all posts
by [REDACTED] August 07, 2019 at 06:44 PM #1

[VIP] [REDACTED]
What is Osiris?
It is a C++ Trojan over Tor. Previously known as kronos.

Why should i get Osiris?
Osiris cannot be tracked or closed because uses Tor connections and fully supports Win Vista/7/8.1/10 Natively.

V.I.P User
VIP

Posts	32
Threads	7
Joined	Jul 2019
Reputation	0

What are the Features?
+ Tor Connection (It's a native bulletproof botnet)
+ Formgrabber fully supported on Internet Explorer,FireFox, Chrome, Opera and Edge all latest versions.
+ Web Injects Support on Internet Explorer,FireFox, Chrome, Opera and Edge all latest versions.
+ Keylogger
+ Log Parser (filtering rules to extract logs from the big database)
+ Download & Execute
+ Bot Update
+ Browser Password Stealer (Chrome,Firefox,Internet Explorer,Edge)
+ SMTP Outlook 2007,2010,2013,2016 Password Recovery
+ Address Book Extractor Outlook 2007,2010,2013,2016
+ AntVMware, AntiSandbox, AntiDebug Support
+ Normal VNC
+ Socks5 Support
+ Hidden VNC [HVNC] (Copy and Paste supported, Chrome, Firefox, Internet Explorer)
+ Hidden Teamviewer + Filemanager of Teamviewer fully Supported
+ Screenshots (Customizable by words and timings)
+ Active Caption (Last Running Caption)
+ Remote CMD / Remote Powershell
What is the Size of the bot?
The size its 330kb

What is the price:
We only sell lifetime license now.
\$5000\$ All included lifetime license | free updates.

Figure 16. Osiris, a Kronos banking variant, was offered for US\$5,000 in the summer of 2019 and then for US\$3,000 in an English language forum later in the year

03.10.2019

MULTI-STAGE ANDROID BANKING MALWARE ON SALE

WHAT'S ON SALE? Original Multi-Stage Android Banking Malware BOTNET with FULL SOURCE CODE for the Web based C2 PANELS, The Trojan Dropper and Final Payload

PRICE: \$350 | ONLY ACCEPTING BTC

This is an original FUD Multi-stage Android trojan specially designed to target the USSD menu on Android phones

It has a Multi-Stage design, meaning it is divided into two parts, The Dropper and the actual Payload, making it extremely difficult to detect

Both the Dropper and Payload are FUD, easily slipping past Google Play Protect and other Security Solutions

The C2 panel is web based and the address can be dynamically updated on the bots as will be explained below, making the botnet resistant to Control panel take downs

Specifically made for android 9,8,7,6,5,1 Versions

Dropper Capabilities

- #Hide icon to hide presence on bot
- #Bind to any application of choice to use as a decoy during spreading
- #Download and Install final payload
- #Gather preliminary data like Android version, Geo Location etc
- #Receive additional APK download links from C2
- #Install any other APK of choice on infected bot
- #Delete payload files once installed
- #Add custom Install message from C2 when installing any APK[Useful for further Social Engineering]

Payload Capabilities

- #Hide Icon to conceal infection
- #Gather bot Info like Android Version, Location etc
- #Dial any USSD number from the bot
- #Special logic to bypass "sim select" popup on double line phones
- #Keylogger to capture any info typed into USSD window
- #Interact with USSD menu by supplying feedback from C2 in realtime
- #Intercept SMS from specific numbers as dynamically specified from the C2
- #Become default SMS application to intercept specific SMS's before they reach victim inbox ****
- #Gain Administrator privileges to Lock bot, factory reset bot and resist uninstall attempts
- #Silence bot
- #Dim bot screen to hide activity
- #Get bot location at all times
- #Capture all SMS or specify specific numbers
- #Display Custom Alert Box on bot with info from C2
- #Put bot in Idle for specified time to reduce load on C2 incase of many bots
- #Transfer bot to another C2 URL
- #Factory reset bot
- #Geo Locked to specific countries i.e Only targeting bots from specific countries or regions****
- #Persistence i.e the bot is still active even after multiple reboots
- #Works on Android 6,7,8,9
- #Uninstall Resistance...even Antivirus cannot remove it ****

Figure 17. Android banking malware bot offered for US\$350 in a Russian language

[50% OFF] ATM EMV Malware - Models List Updated!

Seller Level 0 (47)
Trust Level 3
Verified Seller : / Trusted Seller :
Positive Feedback : (100%)
Member since : Oct 13, 2019
Last Login : Jan 01, 2020
Sales : 47
Orders : 0
Sold : 0 Times
Origin Country : World Wide
Ship to : World Wide
Payment : Full Escrow
Product class : Digital Goods
Quantity : Unlimited Available
Sale Price : 2500.00 USD / 0.35087178 BTC
Sale Price : 2500.00 USD / 54.64480874 XMR
Sale Price : 2500.00 USD / 60.35731531 LTC
Shipping Options : Default - 1 Day - 0.00 USD / 0.00000000 BTC
Quantity : 1

Figure 18. ATM malware offered at US\$2,500 in a dark web marketplace

[50% OFF] GozNym 2.0 Banking Bot

Seller Information:

- Verified Seller :
- Trusted Seller :
- Positive Feedback : (100%)
- Member since : Oct 13, 2019
- Last Login : Jan 01, 2020
- Sales : 47
- Orders : 0

Sold : 0 Times **Origin Country :** World Wide **Ship to :** World Wide **Payment :** Full Escrow **Product class :** Digital Goods **Quantity :** Unlimited Available

Shipping Options :
Default - 1 Day - 0.00 USD / 0.0000000 BTC

Quantity :

Purchase Options:

- Purchase with BTC**
- Purchase with XMR**
- Purchase with LTC**

Product Description **Refund Policy** **Product Tags** **Feedback** **Public PGP Key**

50% DISCOUNT!
Version 2.0 of GozNym Banking Bot.

Main functionality -
Formgrabber (Chrome, Firefox, IE, Tor-Browser (HTTP, SSL, SPDY ...))
DNS Spoofer (Chrome, Firefox, IE)
Track 1/2 arabber

Figure 19. GozNym banking botnet sold in a dark web marketplace for US\$750

Banking malware prices	
Kronos based malware	US\$3,000 and up
Generic Android banking malware	US\$100 and up
ATM malware	US\$2,000 and up
GozNym	US\$750

Spamming Services

The price for spam distribution tools has not changed significantly since 2015. Typical spam services can be found from US\$20 and up. We have observed more spam offerings geared toward SMS messages than email. The price of bulk mailer programs averages around US\$50.

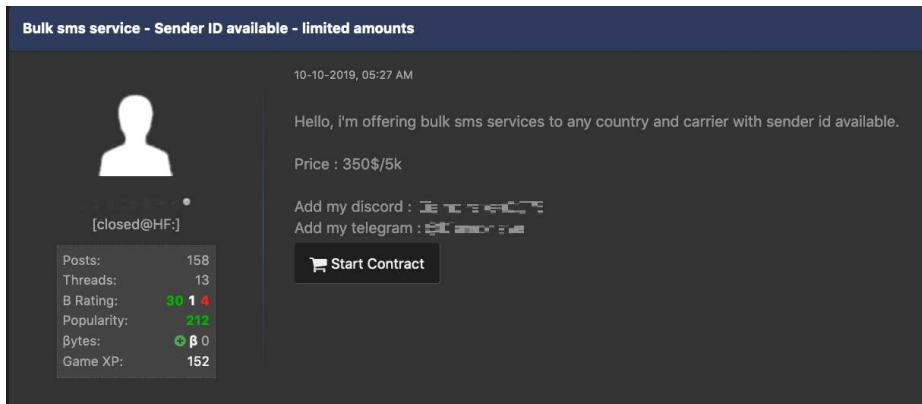


Figure 20. Bulk SMS service starting at US\$350 for 5,000 messages, advertised on an English language forum

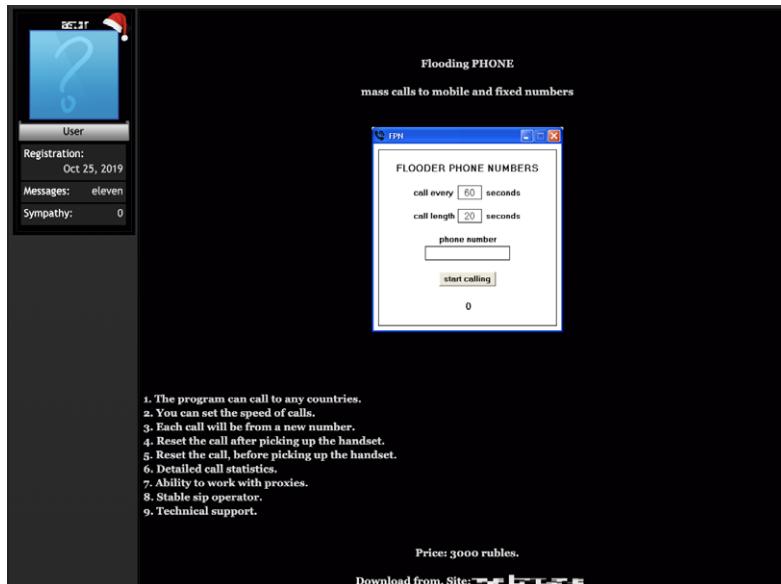


Figure 21. Phone Flooder program sold for US\$50



Figure 22. SMS Sender offered in an Arabic Forum for US\$499

Spamming Prices	
Phone flooder	US\$50 and up
SMS bulk sender	US\$25 to US\$500
SMS sender monthly	US\$2 and up

Online Account Credentials

Online account credentials for different services such as banking, food delivery, entertainment, and more, continue to be sold for low prices. Users can find available credentials for popular media services such as Netflix, Amazon, Hulu, and Spotify. The market is actually oversaturated—stolen accounts make up 32% of all underground offerings. Most accounts start from US\$1, with only a few high tier accounts demanding premium prices. Disney only launched their new streaming platform, Disney+, in November 2019, but available account credentials have already flooded the market.

Products / Digital Goods

★★★★★ 1x NETFLIX ACCOUNT UHD 4K WITH LIFETIME WARRANTY! ★★★★★

Quality: [] [] [] []
rate:

Type: **Digital**

Offers: • 2.13 \$ per piece, for at least 1 product

Coins: **BTC** **XMR**

Left/Sold: 9998 pieces / 1 piece

Verified Vendor
Please ensure you check feedback and read a vendor's terms before purchase.

Seller information
Level 1
0 0 0
Send message
Seller's products (34)

Figure 23. Netflix account sold in a dark web marketplace

Welcome to my brand new account shop!

All accounts are **FRESH** and high quality.

My shop is new, but new sites are being added constantly.

Streaming

1. Netflix Basic/HD Plan - 1,00 €
2. Netflix UHD Plan - 4,00 €
3. Hulu - 1,00 €
4. Hulu (No Ads) - 2,00 €
5. Hulu (Live TV) - 4,00 €
6. Disney+ - 1,00 €
7. --More being added right this second!

Food

1. [USA] McDonald's Account - 1,50 €
2. [USA] Domino's Account + CC - 1,50 €
3. [USA] Domino's Account 60-110 Points - 1,00 €
4. [USA] Domino's Account 120-170 Points - 2,50 €
5. Grubhub Account + CC - 4,00 €

--More accounts and websites are available on my [link]!

Figure 24. Streaming and food service account credentials for sale

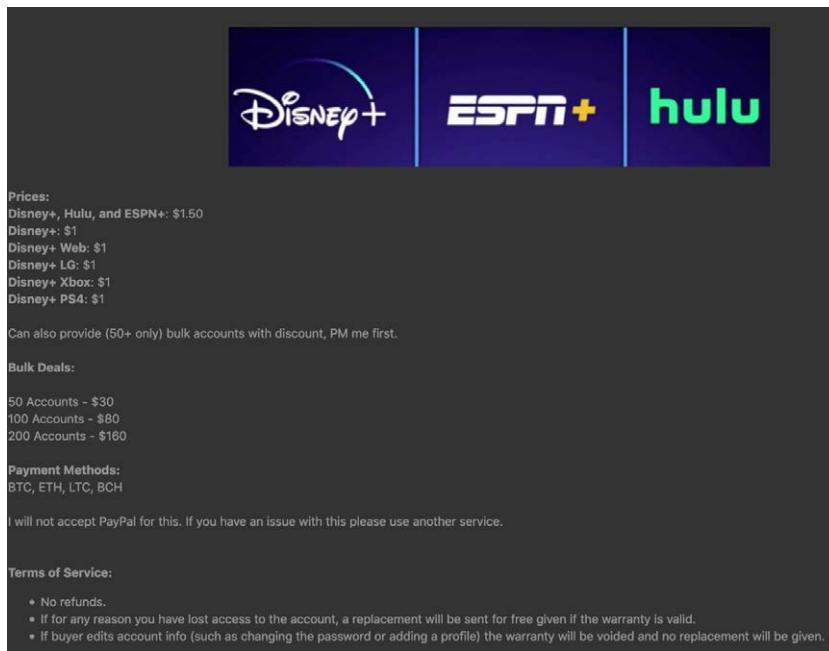


Figure 25. Disney+ account packages starting at US\$1

Name	Included	Last Upload	Refund	Price
Bankofamerica.com	Login:Password only +1	2019-12-30 15:08:37	15 min.	5\$
Bankofamerica.com	Login:Password only +1	2019-12-30 15:03:32	15 min.	5\$
Bankofamerica.com	Login:Password only +1	2019-12-28 23:59:03	15 min.	5\$
Bankofamerica.com	Login:Password only +1	2019-12-20 20:17:22	15 min.	5\$

Figure 26. Banking credentials sold in a carding shop

Online accounts credentials prices	
Netflix	US\$2 and up
Online banking accounts	US\$5 and up
Spotify	US\$3 and up
Disney +	US\$1 and up
McDonalds	US\$1 and up
Domino's	US\$1 and up
Grubhub	US\$3 and up

Credit Card Credentials

The price of stolen credit card numbers, clones, or copies of credit card statements have dropped significantly. This is likely because the underground market has been flooded with these services. Prices for stolen credit card numbers in 2015 started from US\$20 for U.S.-issued cards, but in 2020, most credit cards cost only US\$1. The majority of credit card services are sold in bulk. Premium credit cards that allow large purchases (above US\$5,000) and have been verified to work can cost as much as US\$500 per card.

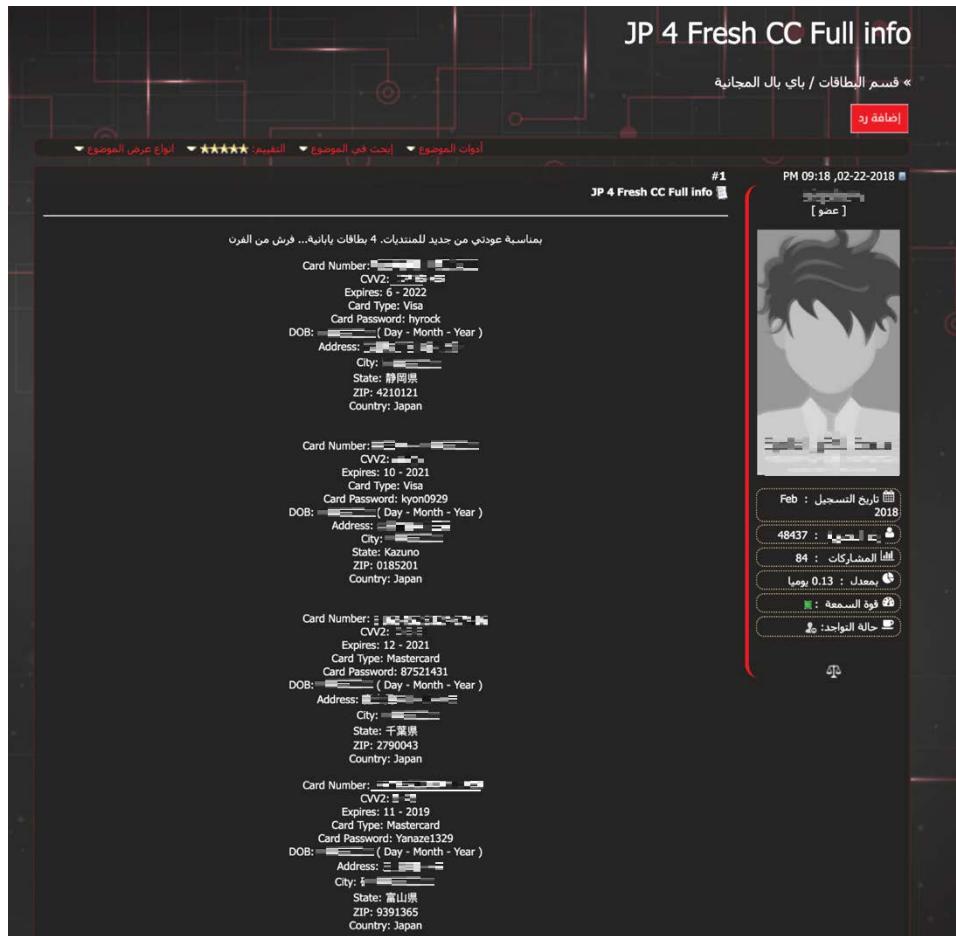


Figure 27. Japanese credit cards offered in an Arabic language forum

Name	Included	Country	Credit card	Last Upload	Refund	Price
Walmart.com	Online	Country: US	Credit card: VISA	2019-12-03 16:06:51	15 min.	3\$
Walmart.com	Online	Country: US	Credit card:	2019-12-03 16:06:51	15 min.	1.5\$
Walmart.com	Online	Country: US	Credit card: MASTERCARD	2019-12-03 16:06:51	15 min.	3\$
Walmart.com	Online	Country: US	Credit card:	2019-12-03 16:06:50	15 min.	1.5\$
Walmart.com	Online	Country: US	Credit card:	2019-12-03 16:06:50	15 min.	1.5\$
Walmart.com	Online	Country: US	Credit card:	2019-12-03 16:06:50	15 min.	1.5\$
Walmart.com	Online	Country: US	Credit card: VISA	2019-12-03 16:06:50	15 min.	3\$
Walmart.com	Online	Country: US	Credit card: VISA	2019-12-03 16:06:50	15 min.	3\$
Walmart.com	Online	Country: US	Credit card:	2019-12-03 16:06:50	15 min.	1.5\$
Walmart.com	Online	Country: US	Credit card:	2019-12-03 16:06:49	15 min.	1.5\$
Walmart.com	Online	Country: US	Credit card:	2019-12-03 16:06:49	15 min.	1.5\$
Walmart.com	Online	Country: US	Credit card:	2019-12-03 16:06:49	15 min.	1.5\$
Walmart.com	Online	Country: US	Credit card:	2019-12-03 16:06:49	15 min.	1.5\$

Figure 28. Walmart credentials with credit card numbers for sale starting at US\$1.50 per account

=====SELLING FRESH VALID WITH GOOD HIGHLY BALANCE CREDIT CARD ALL COUNTRY=====

- I'm looking for a good customer to buy CREDIT CARD everyday and long-term
- I will discount or bonus if you order bulk
- My CVV is good and fresh live 100%
- All my CREDIT CARD are inspected before sale... i will replace if CREDIT CARD DIE !

CREDIT CARD Us :

Us (visa/master) = \$10
Us (amex/disco) = \$12
Us (fullz info) = \$30

CREDIT CARD Uk :

Uk (visa/master) = \$252
Uk (bin/dob) = \$30
Uk (fullz info) = \$35

CREDIT CARD Ca :

Ca (visa/master) = \$15
Ca (bin/dob) = \$22
Ca (fullz info) = \$35

CREDIT CARD Au :

Au (visa/master) = \$15
Au (bin/dob) = \$25
Au (fullz info) = \$35

CREDIT CARD Eu...

France = \$20 (fullz info = \$40)
Germany = \$20 (fullz info = \$40)
Italy = \$20 (fullz info = \$40)
Sweden = \$20 (fullz info = \$40)
Spain = \$20 (fullz info = \$40)
Denmark = \$25 (fullz info = \$40)
Ireland = \$20 (fullz info = \$40)
Mexico = \$15 (fullz info = \$35)
Asia = \$15 (fullz info = \$35)

* And many countries other in stock 95% valid rate and high balance...
* Let me know if have i will sell for you

Figure 29. Worldwide credit cards from US\$10 each

```

=====
<<SELL BANK LOGIN ACCOUNT<<=====

- Bank Login : Username + Password Number (full info)
- Account : Email Address + Password (full info)
- Have all details for login and i can transfer balance to your account (Bank Login if you want)

* Price for Bank Login !!!
- BankLogin US: (Bank of America, Chase, Wells Fargo...)
$200 = Balance $3000
$400 = Balance $5000
$600 = Balance $9000
$1000 = Balance $15000

*Price for UK Bank login !!!
- Bank Login UK: (LLOYDS, TSB, BARCLAYS, Standard Chartered, HSBC...)
$250 = Balance 4000 GBP
$400 = Balance 9000 GBP
$500 = Balance 15000 GBP
$8000 = Balance 20000 GBP

```

Figure 30. High balance credit cards offered from US\$200 and up

Credit card credential prices	
Store credentials with credit cards	US\$1.50 and up
High balance credit cards	US\$100
Bulk credit cards	US\$1 each
Verified credit cards	US\$10 and up

Identity and Document Services

Undocumented immigrants and criminals flock to underground forums in search of identity and document services. These include documents for supporting citizenship claims or other applications, obtaining lines of credit to put up a business, opening untraceable bank accounts, proving residence status, committing insurance fraud, purchasing illicit items, and others.

There have been no significant changes in pricing since 2015; scanned document services such as copies of driver licenses, passports, and bill statements continue to sell for US\$5 and up. Registered passport services cost around US\$2,500. Legitimate-looking counterfeit passports were popular in 2015, but the increase in the number of global immigrants¹¹ and the adoption of e-passports¹² have since affected the type of goods in demand. Underground services shifted to create “legal or registered” passports that can pass a series of authentication tests.

The U.S. opioid crisis has also had an effect on underground goods and services. Opioid prescription has gone down,¹³ thus making the drugs more difficult to obtain. This resulted in an increased demand for forged prescriptions pads. Medical professionals have also started to move to e-prescriptions, which may impact the market further.¹⁴ Forged prescription labels continue to be found in dark web marketplaces for around US\$60.

Registered EU Passports, DL, ID, Visas, and More

Quality rate: ★★★★★

Type: **Physical**

Offers: • 2500 \$ per units, for at least 1 product

Coins: **BTC**

Left/Sold: 16 units / 0 units

Delivery method: Express - 7 days - 50 \$ (1 - 1 units)

Pay with Coin: **BTC**

Purchase type: **Normal Escrow**

Amount: 1 Add to cart Add to wishlist

Details Payment rules Feedback Delivery

Registered EU Passports, DL, ID, Visas, and More

We provide Registered and Authentic documentation for EU countries now. This is a life changer, contact us immediately and get your new document within a week or two.

Passports
driver license
id card
work permit
health card
permanent resident
residency permit

Figure 31. Service that offer registered pasports sold in a dark web marketplace

31/5/18

First post updated !!!

Selling documents.

Prices:

- Scan / photo (Full spread) Passport - \$ 10
- Scan / photo (Bottom) Passport - \$ 5
- (Germany, Norway, Sweden, Switzerland, Argentina, Mexico, Finland, Cameroon, Indonesia, Thailand, Austria) all for \$ 10
- Scan / photo (2 sides) ID / DL - \$ 10
- Scan / photo (1st side) ID / DL - \$ 5

RF Abroad and CIS:

- Scan / photo (Full spread) Passport - \$ 7
- Scan / photo (Bottom) Passport - \$ 5

- Utility bill, Phone bill, Bank statement \$ 10

- order possible.

Kits:

- Passport / ID / DL + Utility bill or Bank statement (Argentina, Poland, France, Czech Republic, Bulgaria) \$ 20
- Passport + ID / DL (Italy, France, Poland, Chile, Norway, Czech Republic, Bulgaria, Nepal) \$ 20
- Passport / ID + Utility bill, Phone bill, Bank statement (France, Poland, Czech Republic) \$ 30
- Passport + ID + DL (Poland) \$ 30
- Passport + ID (2 sides) + DL (2 sides) + Utility bill or Bank statement \$ 40
- ID + CC (Czech Republic) \$ 20

Sets with Selfies (PhotoID).

1. ID (2 sides) + selfie with it (Italy) \$ 25
- 2 ID (2 sides) + selfie with it (Bulgaria) \$ 60
3. Passport (Lower half) + selfie with it (Poland) \$ 40
4. ID (1st party) + selfie with it and a white sheet + address (Bulgaria) \$ 25

At the moment, only these kits with selfie

Set England

1. Passport + National Insurance number \$ 12
2. Passport + National Insurance number + address \$ 15

Figure 32. Russian-based forum selling identity kits

Forged Rowland Pharmacy Prescription Rx Labels - 1 Year Supply

Quality rate:

Type: Physical

Offers: • 120 \$ per Units, for at least 1 product

Coin: BTC

Left/Sold: 999 Units / 0 Units

Delivery method: Priority Domestic - 2-4 Days - 8 \$ (1)

Pay with Coin: BTC

Purchase type: Normal Escrow

Amount: 1

Forged Walgreens Prescription Rx Labels

Quality rate:

Type: Physical

Offers: • 60 \$ per Units, for at least 1 product

Coin: BTC

Left/Sold: 999 Units / 0 Units

Delivery method: Priority Domestic - 2-4 Days - 8 \$

Pay with Coin: BTC

Purchase type: Normal Escrow

Amount: 1

Details **Payment rules** **Feedback** **Delivery**

This listing is a one year supply of the Forged Rowland Pharmacy Prescription Rx Labels, which normally come in a set of only 3 labels not 12 labels. This listing provides a bulk buy discount making it an excellent value amongst the offered forgeries.

-Description- PLEASE READ THIS ENTIRE LISTING BEFORE YOU ASK QUESTIONS OR ORDER

----- Rx LABEL FORGERIES ARE COMPLEX AND THERE IS MUCH INFO TO LEARN

This listing is for forged prescription Rx labels. These labels are identical to the real ones. I have been selling forged prescription labels on the darknet since 2012 and have never had a single one fail. The labels have many purposes. First being so one may carry and possess prescription drugs which are not prescribed to them, such as through airports or across borders. Another use is to pass a drug test for employment, court, probation, parole or other means. In addition these labels can be used to have felony drug charges in court dropped. If one is arrested for use or possession of prescription drugs one may order these labels and have them back dated to a date prior to the arrest and the charges will be dropped. These labels are the ideal way to carry and use your prescription drug of your choice worry free.

----- Description- PLEASE READ THIS ENTIRE LISTING BEFORE YOU ASK QUESTIONS OR ORDER

----- Rx LABEL FORGERIES ARE COMPLEX AND THERE IS MUCH INFO TO LEARN

This is a listing for forged Walgreens Pharmacy prescription labels. These are the label that is on the prescription bottle that your pills are in when you have a prescription filled. By law you can only have and carry prescription pills that you have a valid prescription for and must carry them in the prescription bottle as required by federal law. If you do not have a prescription or a bottle with valid label then you are committing a felony. If you obtain prescription drugs whether it be from an online anonymous marketplace, your dealer, a friend or other means you are committing a felony. This means if you are pulled over by police and you consent to a search, or they have probable cause to search you, once they find your prescription pills you will be arrested and charged with a felony. Another situation may be that you are drug tested for employment, drug tested for probation or parole, or searched

Figure 33. Forged U.S. and U.K. Pharmacy prescription Rx labels offered in a dark web marketplace

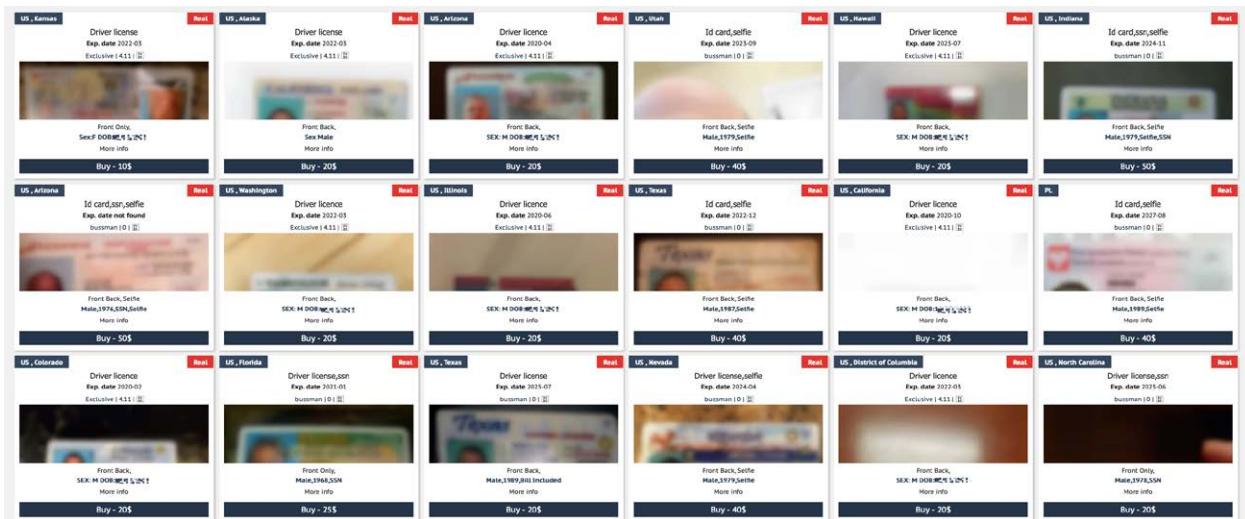


Figure 34. A dark web marketplace selling U.S. driver's license pictures from US\$10 and up

Fake Documents prices	
Fake credit card statement	US\$25
Registered passport service	US\$2,500
Scanned copies of real passports	US\$1 and up per copy
Forged pharmacy Rx labels	US\$60 and up
Identity kits	US\$20 and up
Driver's license scans	US\$10 and up

The Present State of Underground Forums and Marketplaces

Migration of Cybercrime E-commerce to Surface Web Platforms

Over the past 18 months, we noticed that cybercriminals are increasingly using surface e-commerce shopping platforms. Sellers on underground forums post links to their online digital goods stores. One platform in particular has online stores selling malicious digital tools from Arabic, Russian, and English language-based forums. Spanish and Brazilian language-based forums have not adopted this trend.

The specific online platform involved is an all-in-one payment processing and e-commerce solution registered to a company located in the Middle East. Anyone can sign up for an account to sell digital goods on the site. Also, the interface is easy to navigate and use fees are low. In December 2019, the site was ranked in the top 15,000 sites worldwide and 5,000 in the U.S., according to Alexa analytics. Alexa also showed that over half of traffic to the site came from cracked[.]to, a cybercriminal underground forum. The traffic data also showed a significant audience overlap with Nulled[.]to (another forum). This is unsurprising since the About information for Nulled[.]to refers users to the site, claiming that it is connected to one of the forum's administrators.

The e-commerce site's terms and agreements state that it should only be used for lawful purposes. This implies that stores hosted on the site should be banned from selling illegal material. However, when we checked underground forum posts that linked to stores on the site offering illegal goods and services, they were up and running. The fact that the owner participates in underground forums may signal to others in the underground that this particular e-commerce platform can be trusted more than its competitors, and it is likely the reason why bans are uncommon.

Forum users have mentioned being banned from e-commerce platforms for Digital Millennium Copyright Act issues brought on by major companies like Riot and Disney. Other notable e-commerce platforms are also used for cybercriminal transactions. While these platforms are legitimately registered businesses, cybercriminals also heavily use them.

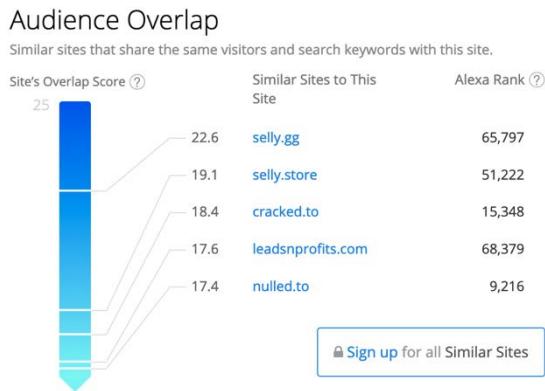


Figure 35. Overlap of visitors to the e-commerce site with two cybercriminal forums, Cracked[.]to and Nulled[.]to

The platform allows users to accept payments through PayPal or in digital currencies like Bitcoin, Ethereum, Stripe, and Litecoin. It offers two options for digital sellers: pay as you go without a monthly fee, or pay for an enterprise account. Items sold on the site are similar to goods and services offered in popular cybercriminal underground forums. However, the e-commerce platform is significantly more convenient for criminals because the seller can showcase various goods or services in one place instead of having to create multiple threads for each individual offering in an underground forum.

Our research found that stores on the site offered stolen accounts, databases, streaming services, carding, VPNs, crypters, banking malware, ransomware, and Mirai variants. The most expensive item we observed was a banking malware sold for US\$2,000. We also found rare limited edition Fortnite skin accounts being sold for US\$999.99.¹⁵ Similar to underground forums, Mirai botnet setups on this platform start at US\$10. Online streaming accounts such as Hulu, HBO, Netflix can also be bought from US\$3 and up. Prices for Android-based RATs start at around US\$50.

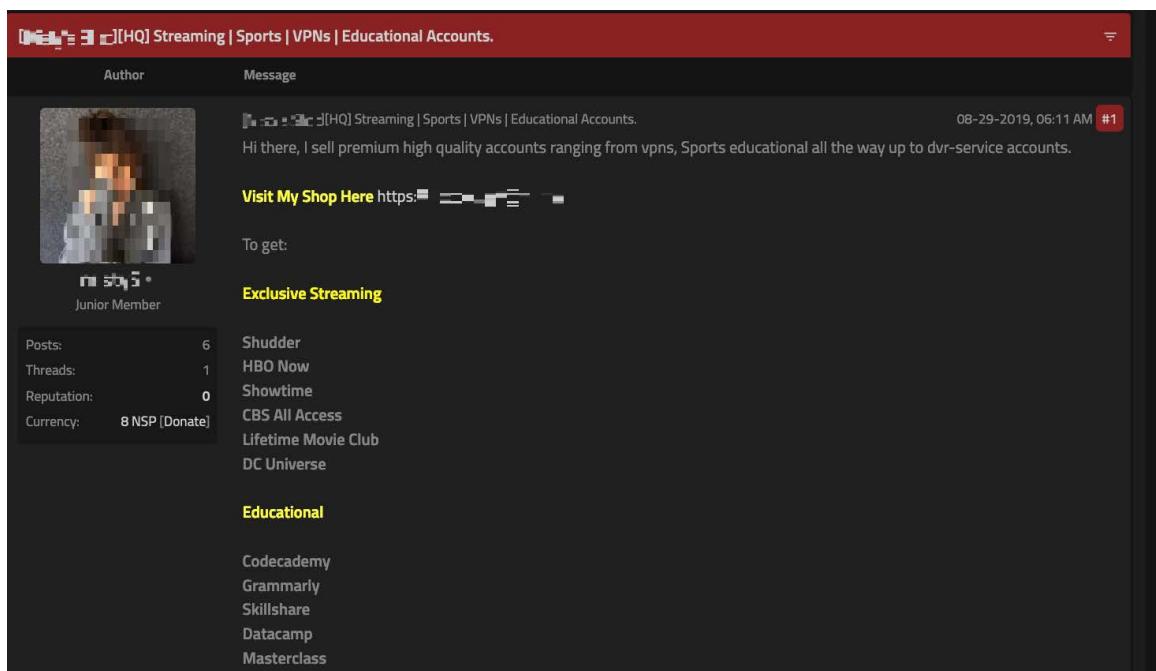


Figure 36. Forum post advertising a store for video streaming services

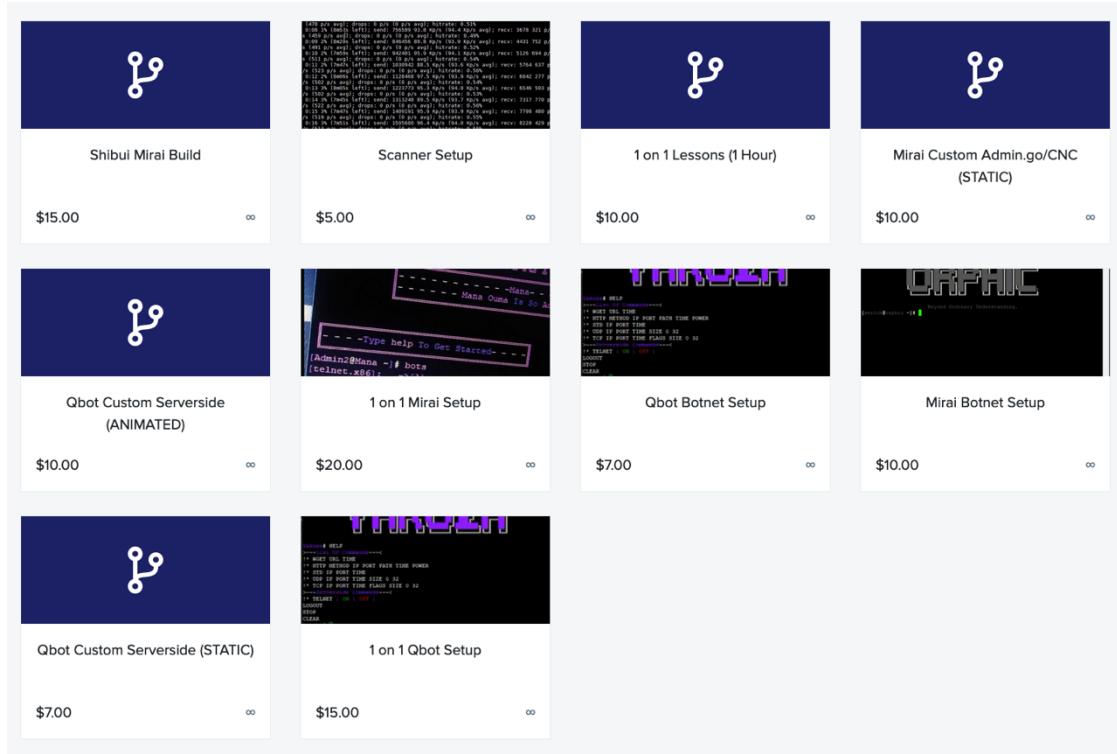


Figure 37. A store on the platform offering services for Qbot and Mirai variants

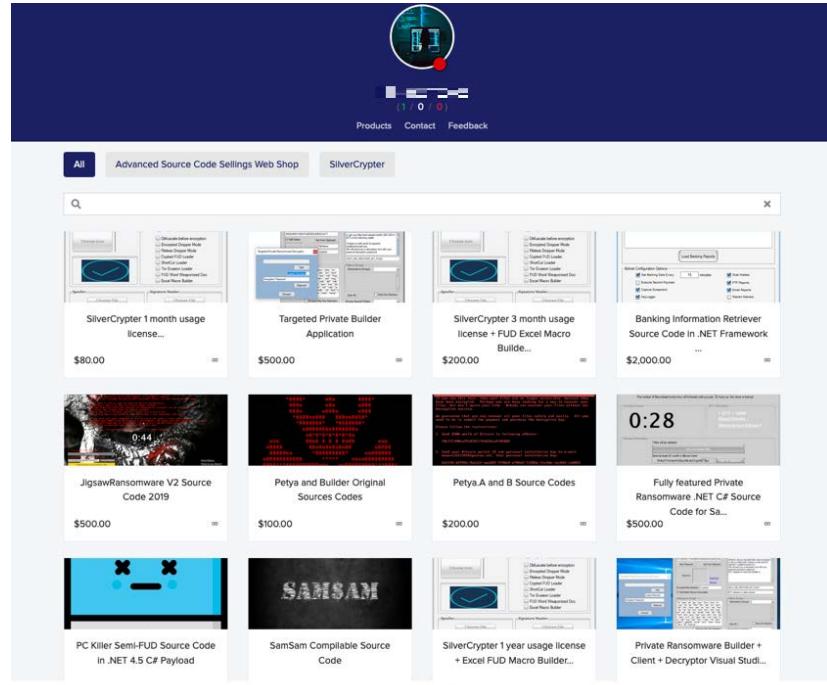


Figure 38. A store offering crypters and ransomware

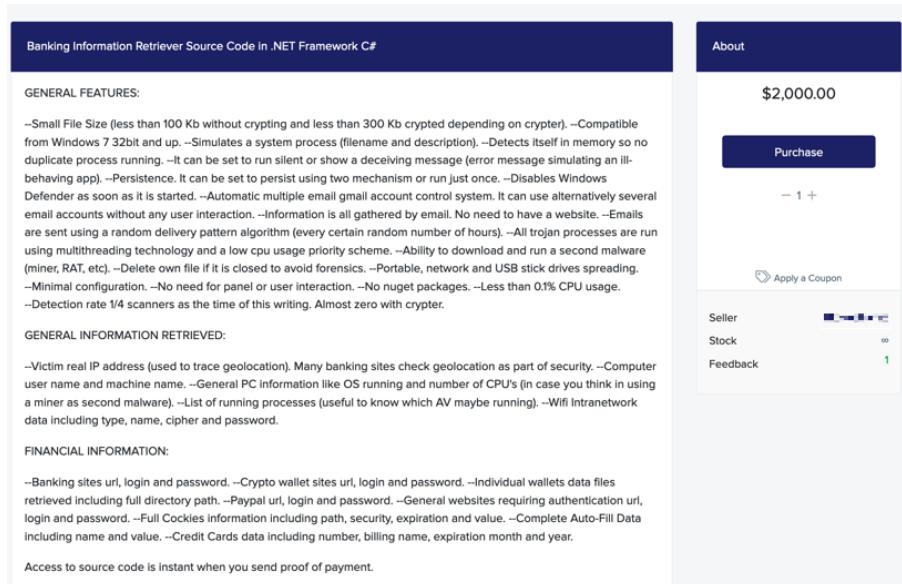


Figure 39. A store offering a banking trojan for US\$2,000

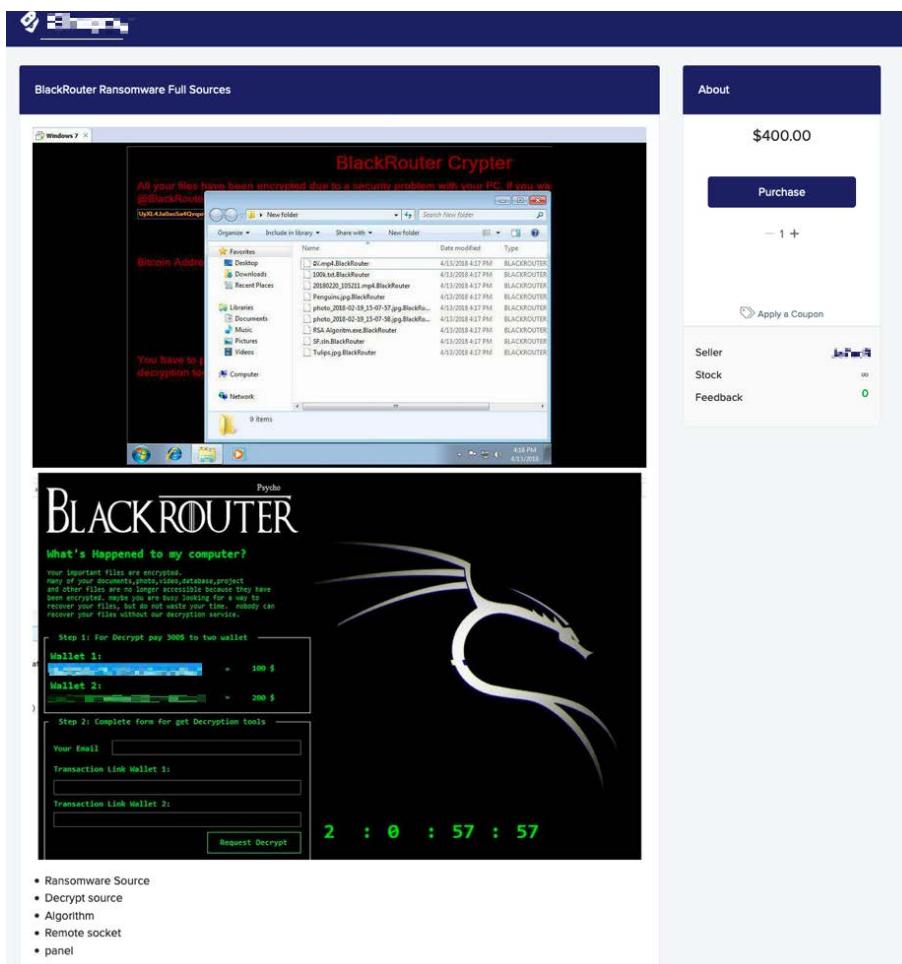


Figure 40. A store offering the ransomware BlackRouter

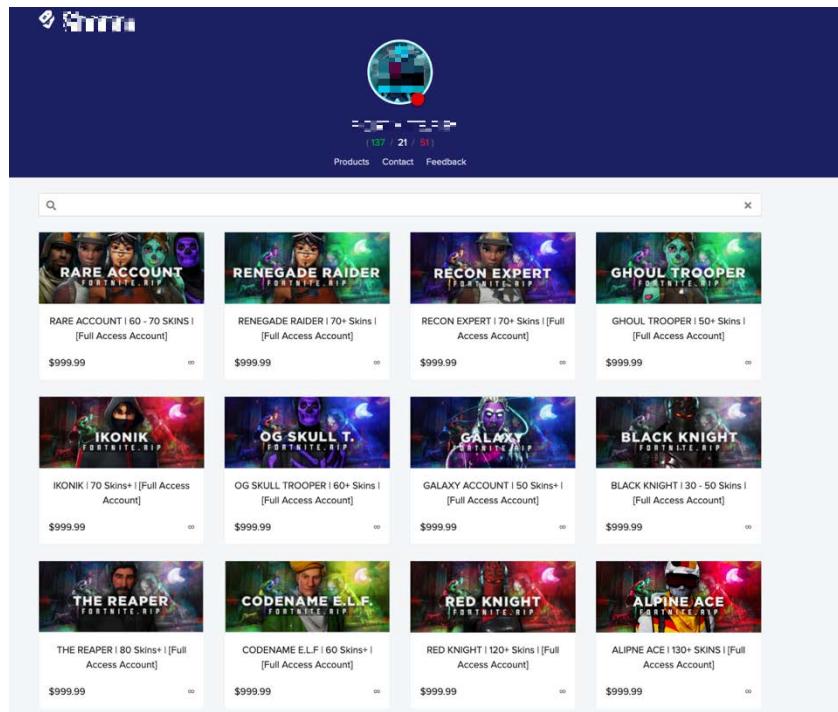


Figure 41. A store of rare Fortnite gaming accounts sold for US\$999.99 each

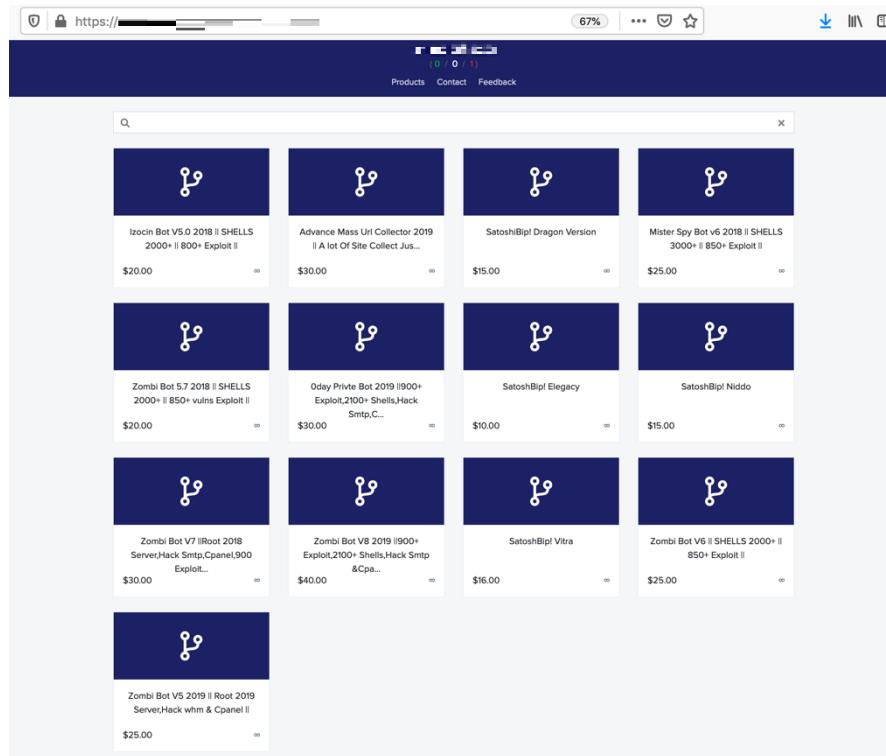


Figure 42. A botnet store

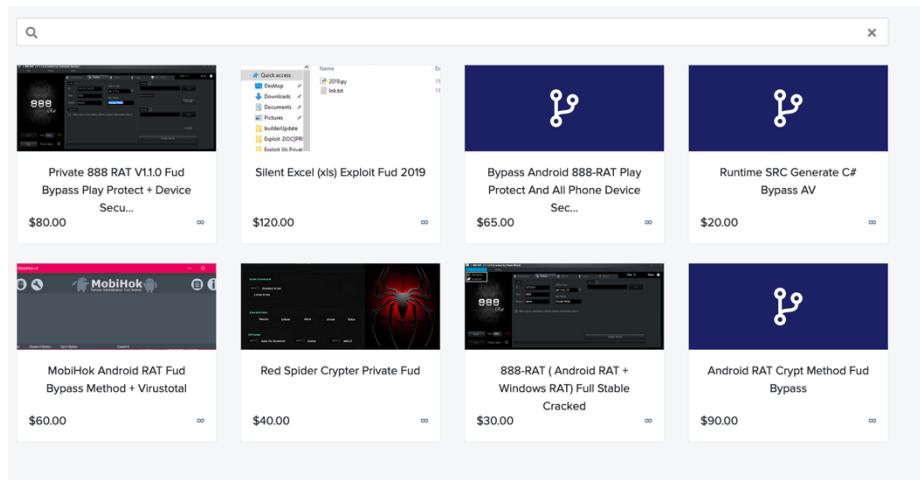


Figure 43. A store that specializes in RATs

Average Store Prices	
Service	Price
Mirai botnet build	US\$10
Ransomware	US\$400 and up
Custom bank trojan	US\$2000 and up
Crypters	US\$50
RATs	US\$30
Android-based RAT	US\$50
Rare Fortnite gaming accounts	US\$999
Botnet rentals	US\$10 and up
Hulu Premium	US\$3
Netflix	US\$5
NordVPN/TunnelBear	US\$3
Grammarly	US\$3
Spotify Family	US\$3
U.S. VISA/AMEX/Mastercard	US\$10
Japan VISA/AMEX/Mastercard	US\$15

Fake News and Cyber Propaganda Tools Gain Popularity

In our 2017 paper, *Fake News and Cyber Propaganda: The Use and Abuse of Social Media*,¹⁶ we discussed services that threat actors used to spread fake news and steer public opinion. These manipulations served various motives, ranging from personal and financial to political. In 2019, these services became more prominent in cybercriminal underground forums. They offer a cost-effective alternative to traditional advertising and promotional efforts, often by manipulating social networks.

Social media-related services, such as large scale social media promotions, the creation of fake comments, and crafting YouTube likes, are sold at very reasonable prices. For these manipulations, cybercriminals generally use autonomous bots, real people, or crowdsourcing programs. Prices start as low as US\$1 for 10,000 likes. The Russian underground maintains the lowest-priced fake news services among the other forums, and prices have remained steady since 2017.

In the era of fake news and cyber propaganda, outdated voter databases are often shared for free while more current databases are available for buyers. We noted an individual U.S. state database going for US\$9.99, while a 2019 Turkish voter database costs US\$400. One underground forum had over 300 database links containing 5 billion entries with information such as PII, credit card information, social security numbers, emails, and passwords. All this information came from data breaches that occurred between 2015 and 2019. Compromised voter databases combined with other data available in underground forums can help malicious actors create very effective cyber propaganda campaigns. For example, key data points can be used to create a target profile for a specific country's electorate.

Voter information is collected through various means, from outright hacking and stolen or lost devices, to unprotected or misconfigured servers, among others. The collected information is usually put up for sale in underground forums.

Several breaches have affected voters across the globe over the past few years. In 2017, an exposed and unsecured Amazon S3 storage server owned by the data analytics firm Deep Root Analytics was discovered by the security firm UpGuard. It contained 1.1 terabytes of data (birthdates, home addresses, telephone numbers, and political views) of nearly 62% of the entire U.S. population.¹⁷ In March 2016, the Anonymous Philippines hacker collective and LulzSecPilipinas compromised the Philippines Commission on Elections (Comelec) database containing the information of 54.36 million registered voters for the 2016 elections. The compromised Philippine Comelec information and exposed Turkish 2016 voter databases are commonly found in cybercriminal underground forums.¹⁸

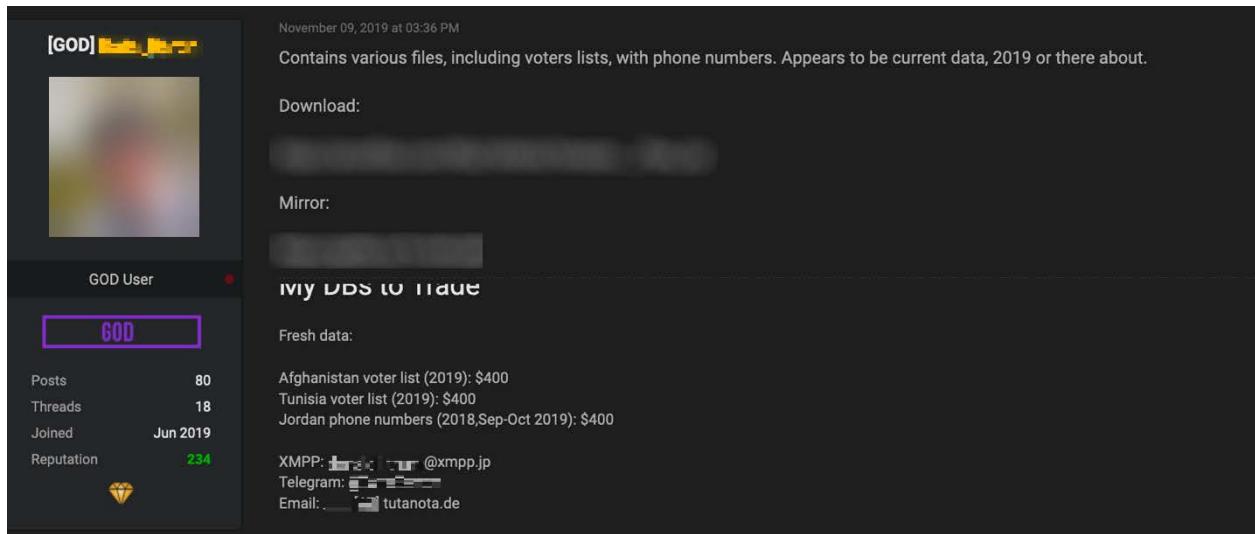


Figure 44. An English language forum selling voter databases for Afghanistan and Tunisia at US\$400 each

The image displays a dark web marketplace listing for various voter databases. Each entry includes the database name, voter count, payment methods (Bitcoin, Bitcoin Multisig, Monero), digital autopilot listing, escrow, and auto shop options. The seller has 20 positive feedbacks, 100% positive feedback, and is a member since 2019-04-22. The level is Level 1 and verified.

- Alabama Voter Database 132788 Voters**: 9.99 USD/Each, 0.00133895 BTC/Each. Order Now.
- Pennsylvania Voter Database 620201 Voters**: 9.99 USD/Each, 0.00133895 BTC/Each. Order Now.
- Arkansas Voter Database 1.7 Million Voters**: 9.99 USD/Each, 0.00133895 BTC/Each. Order Now.
- Rhode Island Voter Database 740049 Voters**: 9.99 USD/Each, 0.00133895 BTC/Each. Order Now.
- Washington DC Voter Database 493000 Voters**: 9.99 USD/Each, 0.00133895 BTC/Each. Order Now.
- Oregon Voter Database 3.1 Million Voters**: 9.99 USD/Each, 0.00133895 BTC/Each. Order Now.
- Missouri Voter Database 4.1 Million Voters**: 9.99 USD/Each, 0.00133895 BTC/Each. Order Now.
- USA Voter Database Pack (27 States)**: 9.99 USD/Each, 0.01340165 BTC/Each. Order Now.
- Ohio Voter Database 7509310 Voters**: 9.99 USD/Each, 0.00133895 BTC/Each. Order Now.
- Philippine Voter Database 70 Million Voters**: 9.99 USD/Each, 0.00133895 BTC/Each. Order Now.

Figure 45. A dark web marketplace offering voter databases for US\$9.99 each (as of Nov 12, 2019) from a seller with 100% feedback

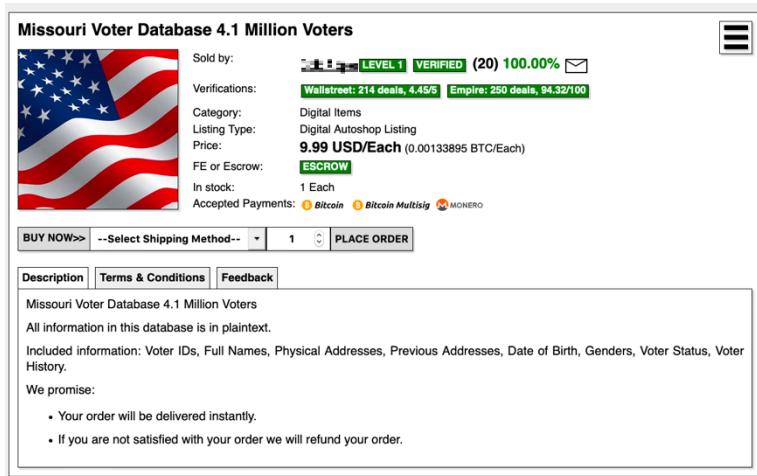


Figure 46. Details of the voter database contents, which includes dates of birth, voter history, addresses, and voter IDs

Services for increasing social media likes are common in the underground, across all languages. Some of these services guarantee the quality of these manipulations and also specify the use of automated bots or humans. Most of these types of tools are used to drive political agendas, but they can also be used for social engineering.

We saw services that offer 1,000 Instagram likes for as low as 15 cents. We also saw offers for Facebook and Instagram likes that cost US\$3 for 1,000. Twitch likes start from 50 cents for 50 likes. Bot tools for increasing likes or visitors cost US\$25. In Arabic language-based forums, Russian actors occasionally post offerings for VkTarget projects. VkTarget is a service for people who want to make money through crowdsourcing. Users can advertise small tasks (like creating traffic for sites and liking social media accounts) for others to complete.

Figure 47.Underground forum post advertising an exploit to increase Instagram likes

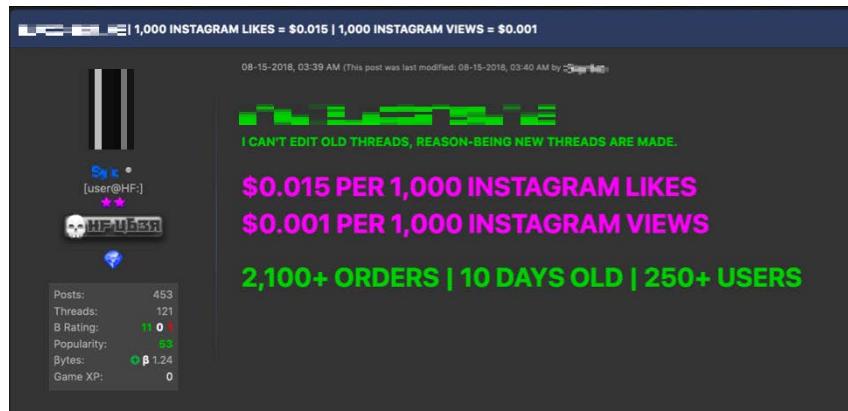


Figure 48. Advertisement selling Instagram likes

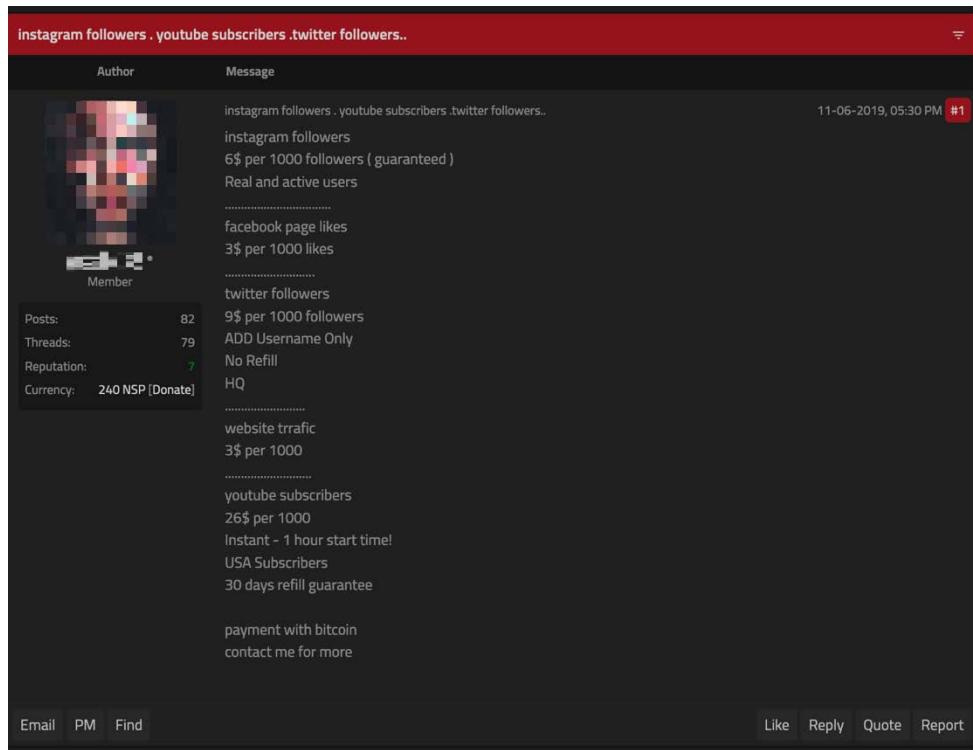
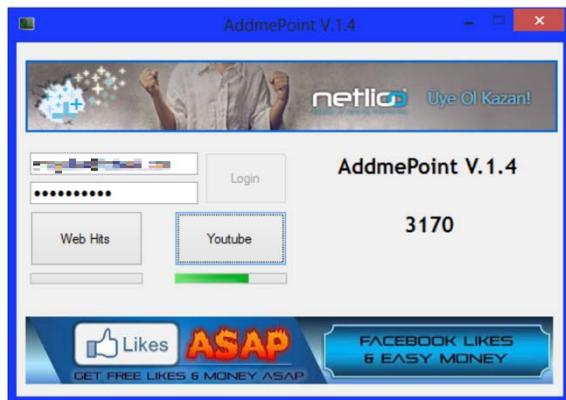


Figure 49. A forum post offering to purchase social media followers



[رابط تحميل الاداة : رابط الاول](#)

Download 1 Link

[رابط تحميل الاداة : رابط الثاني](#)

Download 2 Link

Figure 50. Free bot tool for adding likes to YouTube, Instagram, Twitter, and Facebook offered in an Arabic language forum

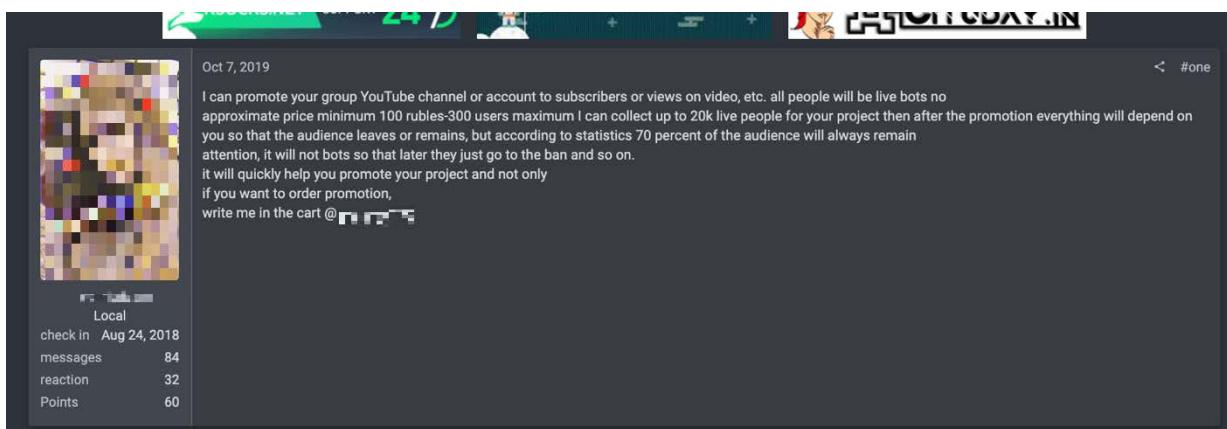


Figure 51. A Russian language forum post offering YouTube likes

Fake news and cyber propaganda prices	
Service	Price
United States voter databases	Free to US\$9.99
Non U.S.voter databases	US\$9.99-US\$400
1,000 Facebook likes	US\$3 and up
1,000 Instagram likes	US\$0.15 and up
50 Twitch likes	US\$0.50 and up
Social media bot	US\$25 and up

Fake news and cyber propaganda prices	
Service	Price
1,000 YouTube likes	US\$26 and up
20,000 New visitor hits	US\$5 and up

Interest in Deepfake Scams Increase

Deepfake technology is an AI-generated technology that creates fake videos, images, or audio recordings that look and sound genuine. Users in underground forums have expressed interest in finding ways to monetize this technology. Deepfake services already exist in underground forums, but most posts involve inquiries and exchanges of information. Forum users often discuss how AI technology can be used for “eWhoring,” also known as sextortion, and for bypassing photo verification requirements on dating sites.

In the past, sextortion was mostly about social engineering and reputation attacks.¹⁹ Criminals would send emails threatening to expose a damaging or embarrassing recording to friends or family and demanding money in exchange for keeping quiet.

People would be more likely to pay the extortion amount if cybercriminals started attaching or sending links of realistic Deepfake images of their victim. A real image or video would be unnecessary. Virtually blackmailing individuals is more efficient because cybercriminals wouldn’t need to socially engineer someone into a compromising position. Deepfake videos can also be used to undermine the reputation of a political candidate or senior executive.

A new emerging threat we expect to take off is the use of Deepfakes for extortion-based ransomware. Here is a likely scenario: The attacker starts with an incriminating Deepfake video, created from videos of the victim’s face and samples of their voice collected from social media accounts or publicly available websites. To further pressure the victim, the attacker could start a countdown clock (24-48 hours is common for ransomware) and include a link to a fake video. They would also likely include a Bitcoin address to receive payment. If the victim does not pay before the deadline, all contacts in their address books will receive the link. Although we have not seen this type of attack, it seems like a likely threat given the direction of Deepfake queries in underground forums.

In March 2019, an executive of an unnamed U.K.-based energy company conversed with on the phone with someone he thought was his boss (the CEO of the organization’s parent company). This person asked him to urgently transfer €220,000 (US\$243,000) to a Hungarian supplier. It turned out that the executive was talking to a scammer that used Deepfake voice technology to impersonate his boss.²⁰

Aquí van 7 tecnologías emergentes que representan amenazas para la ciberseguridad moderna.

Los audios y vídeos "deepfake" generados mediante IA pueden ayudar a los piratas informáticos a estafar a las personas.

La tecnología "deepfake", que permite a la gente manipular vídeos y audio haciendo que el resultado sea muy real, ha dado pasos agigantados en los últimos años. De hecho, cualquiera que esté familiarizado con los filtros de intercambio de caras en Snapchat o Instagram ha sido testigo de primera mano de una versión rudimentaria de la tecnología deepfake.

A medida que los deepfakes son cada vez más sofisticados y difíciles de distinguir de la realidad, los expertos en ciberseguridad temen que los hackers puedan utilizar la tecnología para estafas en las que les sea fácil hacerse pasar por otra persona y conseguir así que las víctimas entreguen información privada.

Algunas empresas están trabajando en crear un software basado en IA que detecte los deepfakes pero, por el momento, estos avances se encuentran aún en las primeras fases de desarrollo.

Figure 52. A Spanish underground forum discussing seven emerging threats in 2019 that includes a section on Deepfakes

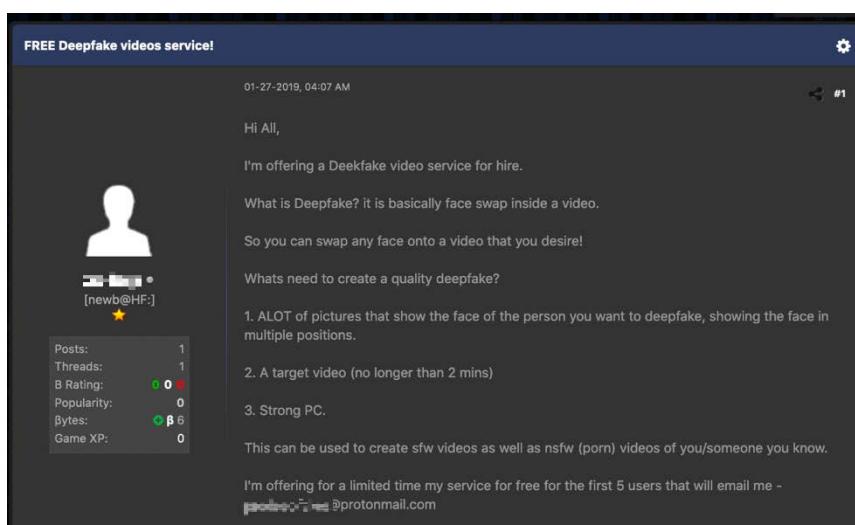


Figure 53. Seller offering five users free Deepfake video services to start their business

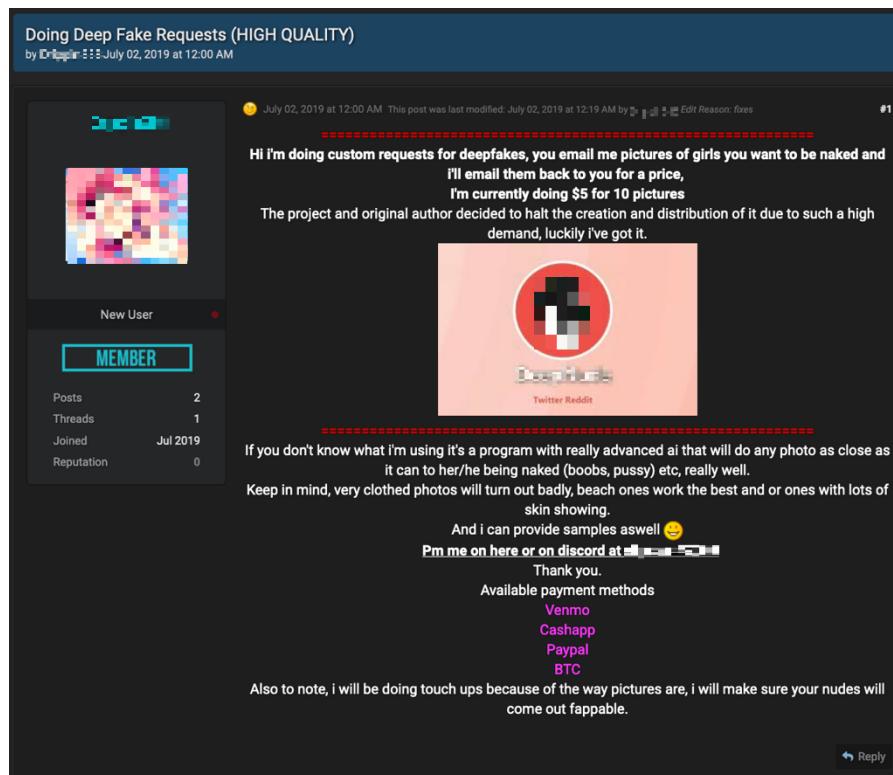


Figure 54. A Deepfake still image service

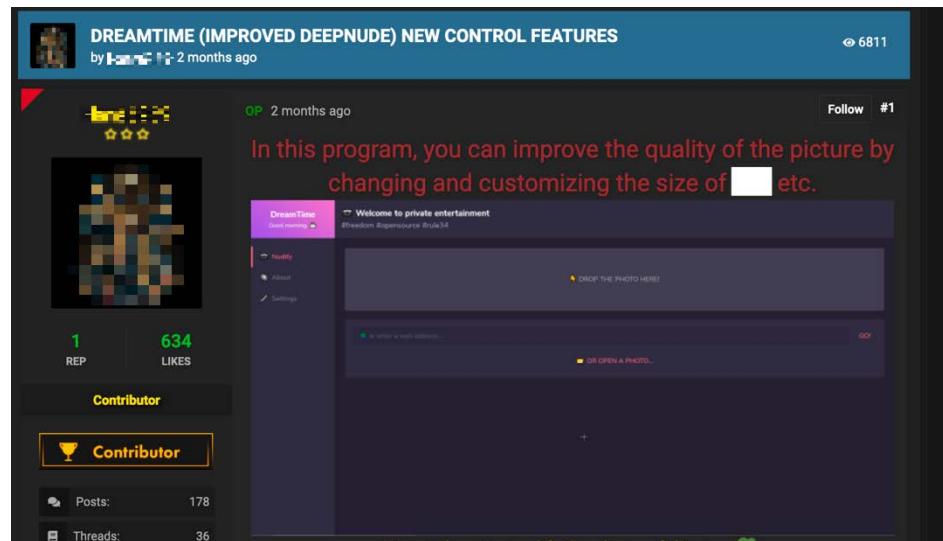


Figure 55. Software to create nude Deepfake images by customizing the person's measurements and features



Figure 56. Deepfake services for nude pictures and videos offered through Dread

Deepfake prices	
Service	Price
Deepfake videos	From US\$50
Deepfake still images	From US\$2.50 each
Software to create deepfakes	From US\$25

Exploring Advanced AI and Using Current Services for Gambling

As AI capabilities become more powerful, we expect cybercriminals to use AI technology to increase targeting and improve malware infection rates in the future. However, the underground market discussions currently revolve around information and inquiries about the AI technology itself rather than actual criminal services. We found multiple listings of AI college books offered for sale and sometimes shared for free.

Most goods or services we encountered were related to the gambling sector. Advertisements for gambling bot services mentioned the use of “advanced AI engines” and start at around US\$80 for a basic one-month subscription. One gambling bot, called Luckybot, uses AI to predict dice roll patterns. Another advertisement we observed was the use of AI to solve complex Roblox CAPTCHA.

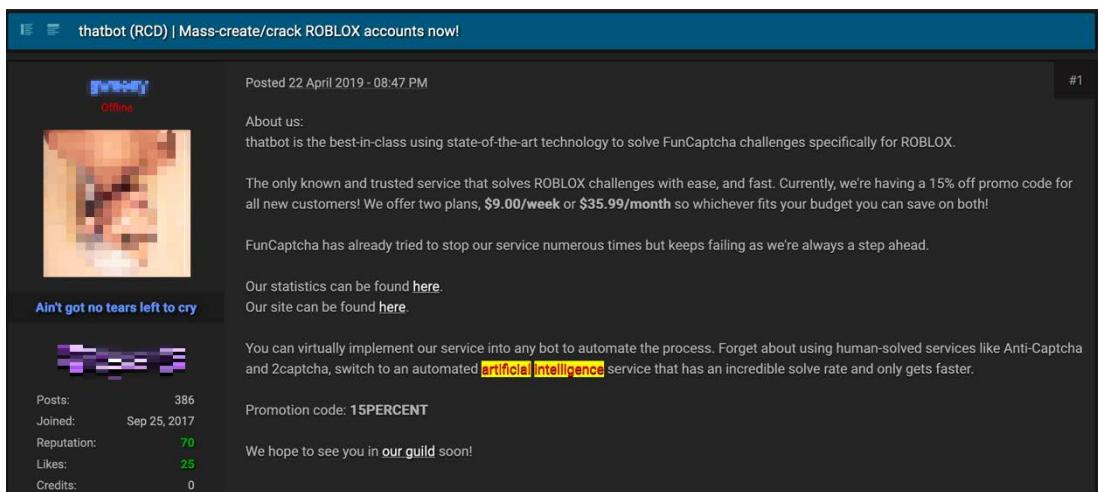


Figure 57. AI-enabled bot for solving Roblox captchas

Figure 58. AI-enabled gambling tool for predicting dice roll patterns

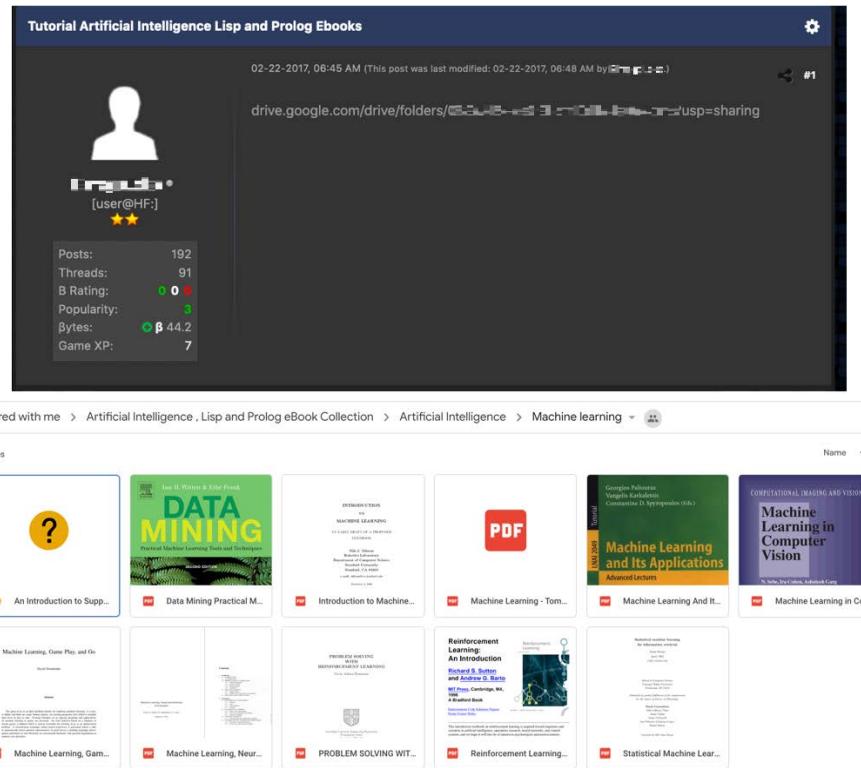


Figure 59. Free AI books shared in an English language forum

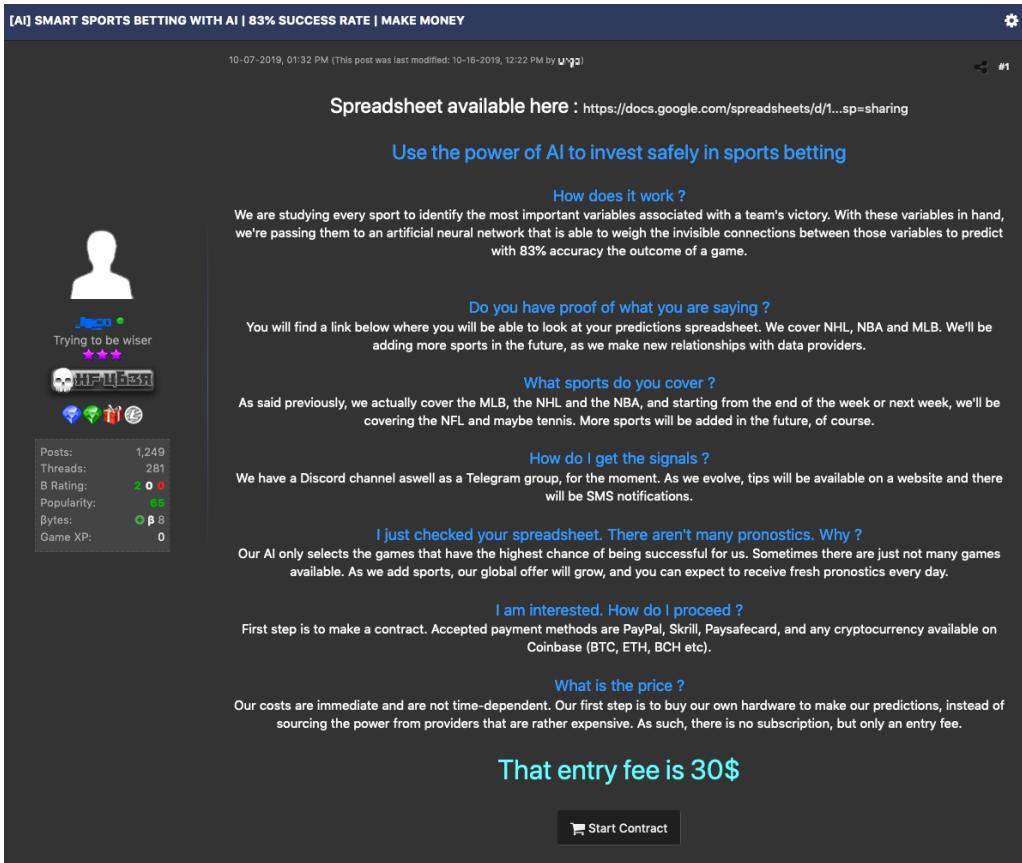


Figure 60. Sports betting service using AI

AI prices	
Service	Price
Roblox	From US\$36
Gambling Bot	From US\$75
Sports Betting AI	From US\$30

Access-as-a-Service Becomes Popular

Access-as-a-service has evolved from remote desktop protocol (RDP) offerings to selling access to hacked devices and corporate networks. While it has been around for years, there was an increase in offerings in the last year. Access to different organizations and companies were obtained through ransomware, credential-stealing malware, and botnets. We found multiple levels of access sold: executive-level credentials, remote desktop access, administrative panels, cloud storage, email accounts, and even full company network access.

Many of these offerings are found on the Russian forum Exploit[.]in. One actor was selling access to an American insurance company for US\$1,999, and a European software company for US\$2,999. Prices for Fortune 500 companies can reach up to US\$10,000. Some offerings include access with read and write privileges.

The screenshot shows a forum post on the website Exploit[.]in. The title of the post is "[SELL] network + remote desktop access from uk, and another companies for sale". The post is authored by a user named "Junior Member" who has 7 posts, 1 thread, and 0 reputation. The user's currency is 9 NSP [Donate]. The message content details the offer: "[SELL] network + remote desktop access from uk, and another companies for sale", "remote desktop access from uk companies for sale", "+600 gig data (with edit access)", "one good from another country with 4terabyte + read and write data (edit files)", "+ escrow welcome", and "if u have any good idea tell me ,".

Figure 61. Network access to a U.K. company

Cloud Log Access (0/10)

01/10/2020

The screenshot shows a forum post from a user named "HDD drive" (User). The post was made on 01/10/2020. The user has no avatar and is a Junior Member. Their profile includes registration on 04/05/2019, 21 messages, 0 reactions, and 1 point. The post content discusses selling access to a cloud of logs (approx. 160GB) from the beginning of 2018 to the fall of 2019. It specifies a global geo (USA and EU), mentions the cloud is no longer replenished, and notes a limit of 10 accesses. The price is \$150, payment is via Bitcoin or forum guarantor, and contact information is provided via telegram and jabber.

Figure 62. Actor selling access to cloud logs

The screenshot shows a forum post titled "A Fortune 500 US Based Company Network Access". The author is "Junior Member" (Junior Member). The post was made on 06-08-2019, 12:20 AM. The user has 26 posts, 3 threads, 0 reputation, and 32 NSP (Donate). The post content details a large corporation with annual profits of \$2.5B, operating in insurance, shipping, and other sectors. It offers network login information for a fee negotiable in crypto currency. The post includes several paragraphs of text describing the company's operations and the nature of the data being offered.

Figure 63. Selling Fortune 500 network access

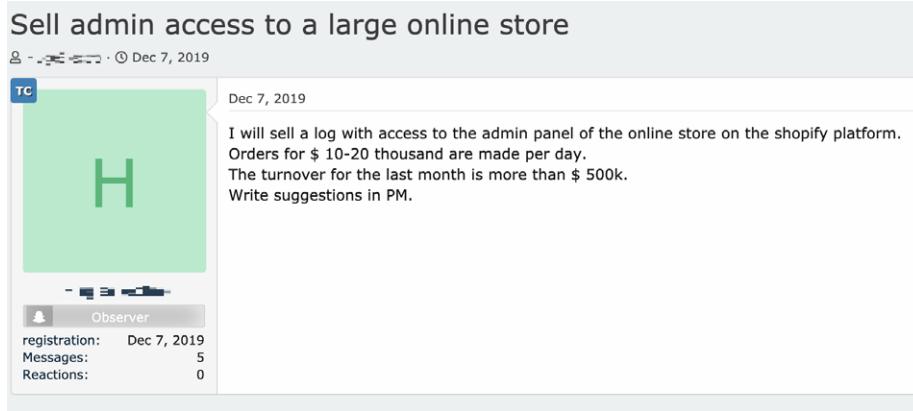


Figure 64. Advertisement for admin access to a profitable online store

Wearable Trackers Targeted

In multiple English language-based forums, we found numerous advertisements for Fitbit user accounts and for the actual wearable device itself. Fitbits are priced in the U.S. between US\$69.95 to US\$279 and include a one-year warranty. Users can purchase an additional year of warranty for a fee. Fitbits sold in the EU can range from €79.97 to €299.95²¹ and include a two-year warranty.²² Underground prices for account information such as usernames and passwords are frequently available, but we have also found advertisements selling the devices' captured data such as steps and GPS locations.

Cybercriminals who purchase Fitbit user accounts are usually running a warranty scam, where they modify the email and address and then request a replacement device under the one or two-year warranty. These Fitbits are then sold in underground forums for a large discount. The Fitbit Iconic goes for US\$249 in the U.S., but it can be purchased in the underground for US\$40. We cannot confirm what cybercriminals are using the captured step data for, but we speculate it may be used to receive the special offers and discounts given after a certain amount of step activity. We even found an advertisement offering a class on how to social engineer customer service to obtain a replacement Fitbit for US\$100 on an English language-based forum.

A screenshot of a forum post on the /b/ board. The title is "Fitbit email changed without my authorization". The post was made by a user named "Jogger" on April 19, 2019, at 19:16, last edited on April 20, 2019, at 11:02. The content of the post is:

I received an email that my email address was changed. This email is not mine and I never made the change. I chatted online right away with a Fitbit support rep and he said he opened a ticket but after reading through other people's complaints about the same exact issue, I'm a bit concerned. I don't understand why this person, whoever they are, would hack my Fitbit data. It's of absolute no value to them! I just want access to my data again that I've accumulated for the last year! Does anyone know if I can expect to gain access to my account again? I've used the same email since I got my Fitbit a year ago so this is just ridiculous if Fitbit can't fix this, they should've never allowed the email change in the first place without me confirming it.

Moderator edit: Removed personal info

Below the post are two buttons: "1 Vote" and "Reply".

Figure 65. A Fitbit user complaining their account information was changed

A screenshot of a forum post on the /b/ board. The title is "1.9k Fitbit Accounts - Device Capture - Cracked [3/22/18]". The post was made by a user named "f00t" on March 22, 2018, at 11:05 PM. The content of the post is:

Cracked all these accounts on my own.
:Sample:
[Device - One] [Type - HADRON] [Battery - High]

[Device - Blaze] [Type - ELECTRON] [Battery - Empty]

[Device - Alta] [Type - LEPTON] [Battery - High]

[Device - Alta HR] [Type - ATOM] [Battery - High]

Enjoy.

The sidebar on the left shows the user's profile: "Banned", "Posts: 232", "Threads: 45", "Joined: Oct 2017", "Reputation: 264", and "2 YEARS OF SERVICE".

Figure 66. Fitbit captured accounts for sale

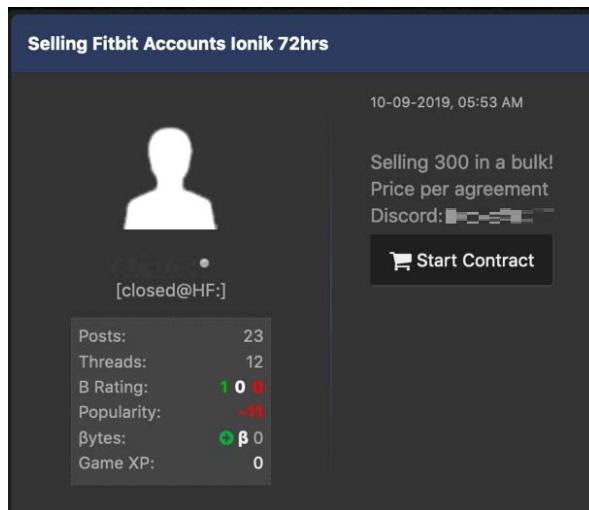


Figure 67. Fitbits sold in bulk

250+ a day Full Fitbit SE Method [24/7 SUPPORT] - [SCREENSHARE MENTORING] -

09-30-2019, 01:13 PM #1

I'm selling fitbit proces method,replist and the method to get a form for 100\$ BTC/Paypal/Cashapp

You will be able to get fitbits and sell them.

I will send a text document and mentor the method through screenshare if that's needed.

Contact me on discord for any questions or proof: [REDACTED]

Ebook Seller / Web hosting Seller ★

Posts: 31
Threads: 15
B Rating: 5 0 0
Popularity: 5
Bytes: 0 216.26
Game XP: 0

Included:

- Method to get form
- Method to process it
- 1 on 1 monitoring through discord
- Textdocument with the methods
- Replist
- apk for fitbit chat so no need to login
- account suppliers for you to buy accounts

Proof I can show over discord before paying but won't show the method 70+ orders I did personally

Start Contract

Figure 68. A class on social engineering, teaching others how to obtain Fitbits and sell them

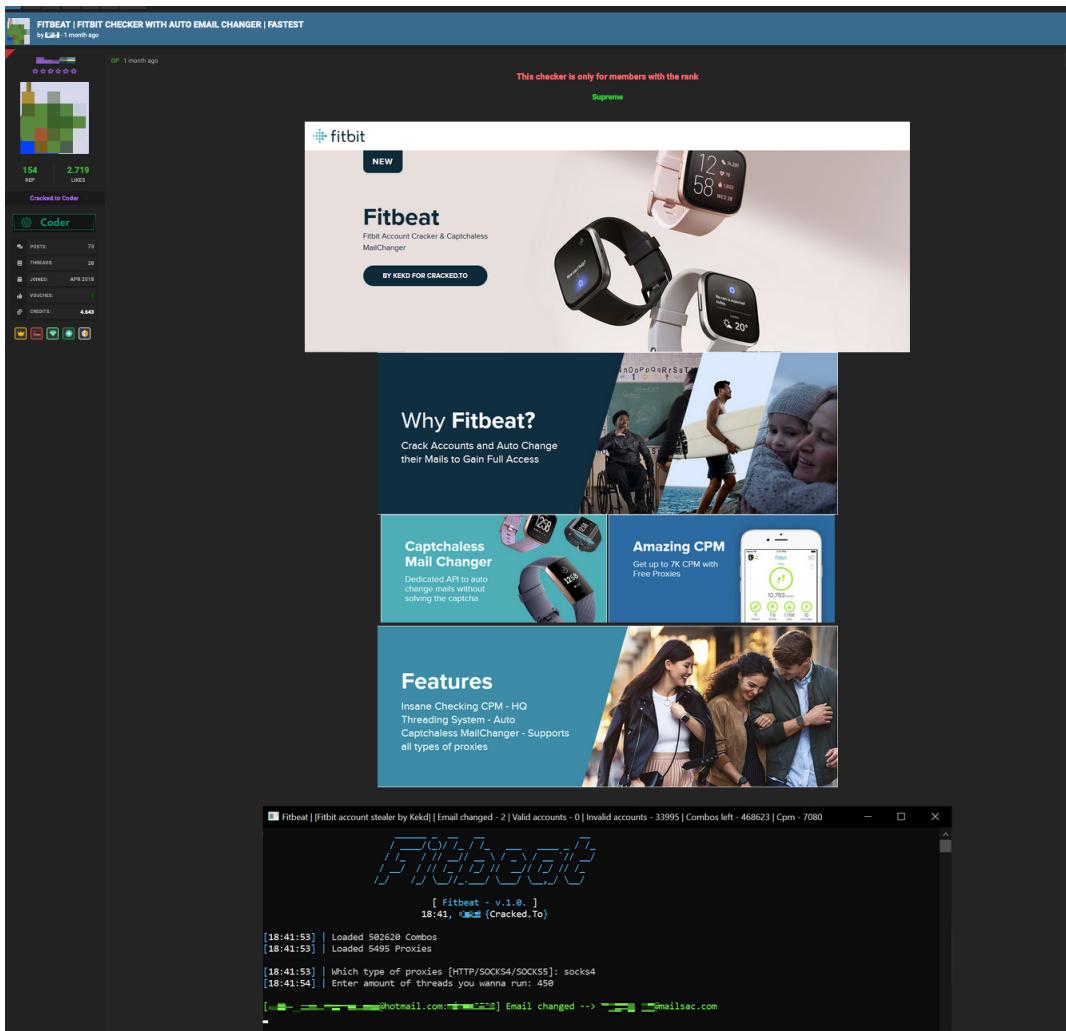


Figure 69. An advertisement for a Fitbit account validation service

Fitbit prices	
Service	Price
Fitbit social engineering course	From US\$100
Fitbit Ionic	From US\$40
Fitbit Versa	From US\$35

IoT Botnets are the New Norm

IoT botnets are now commonly found across underground forums. As IoT device use becomes commonplace in households, enterprises, and the public sphere, Mirai and its variants continue to evolve and adapt. They remain the dominant IoT threat, particularly because of landscape changes like the adoption of 5G. Our recent IoT paper, *The Internet of Things in the Criminal Underground*,²³ covered data and active monetization schemes focused on consumer devices.

Most IoT botnets found in underground forums are either based on the same leaked source code from the Mirai malware, other similarly behaving malware, or a variant. We found multiple forum users asking for links to the original Mirai source code or information on how to troubleshoot their own Mirai code. Older Mirai variants are commonly shared for free. Newer undetected variants can go for up to US\$5,000 when first released.

Mirai botnet rentals start at just US\$10. Low-cost rentals mean that this type of botnet is readily available to all levels of cybercriminals, even those that may not have the skills to build and run their own botnets. We also noticed that some of these Mirai botnet rentals come with bulletproof hosting as part of the service. The predominant model for earning with these botnets is still distributed denial of service (DDOS), however, we do expect criminals to innovate more over time.

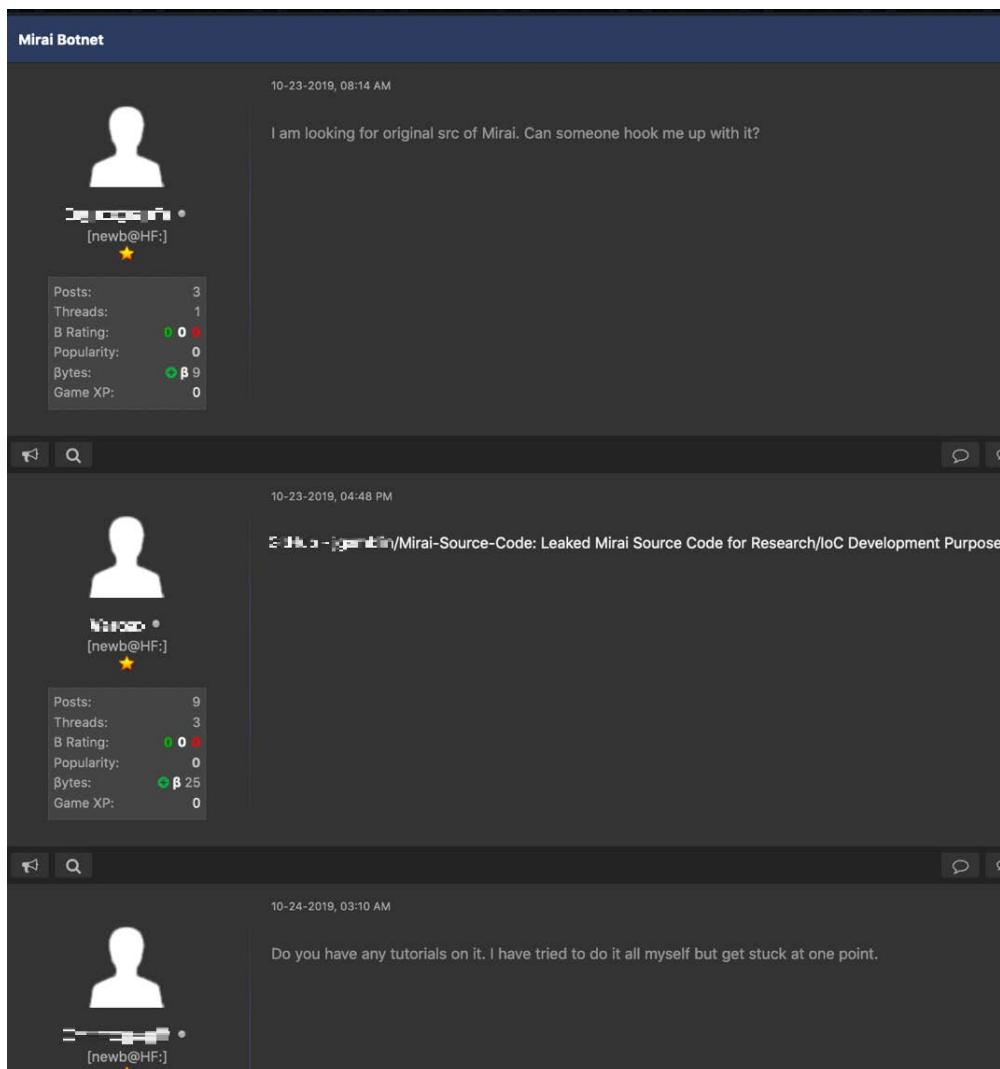


Figure 70. Forum user asking for the Mirai source code

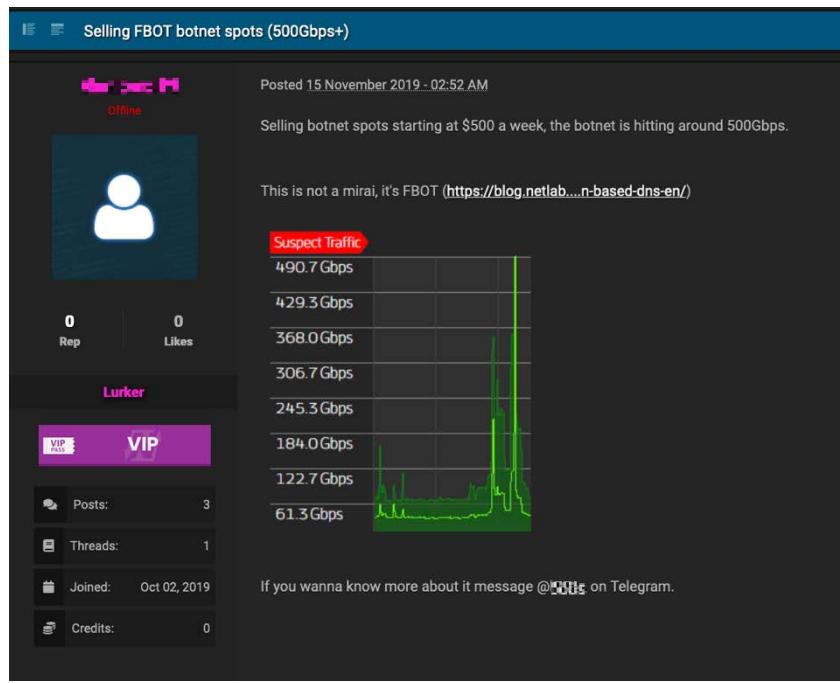


Figure 71. Fbot botnet spots for sale using Satori, a Mirai variant²⁴

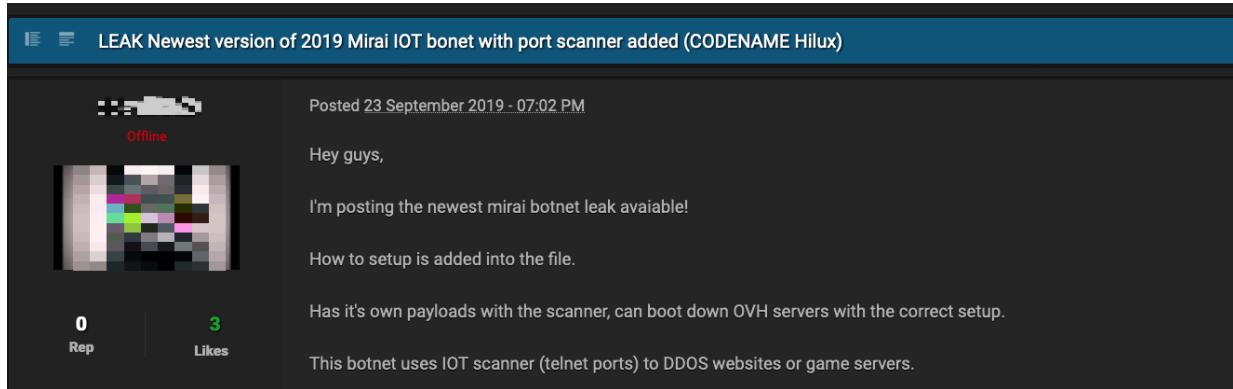


Figure 72. Free Hilux Mirai variant download

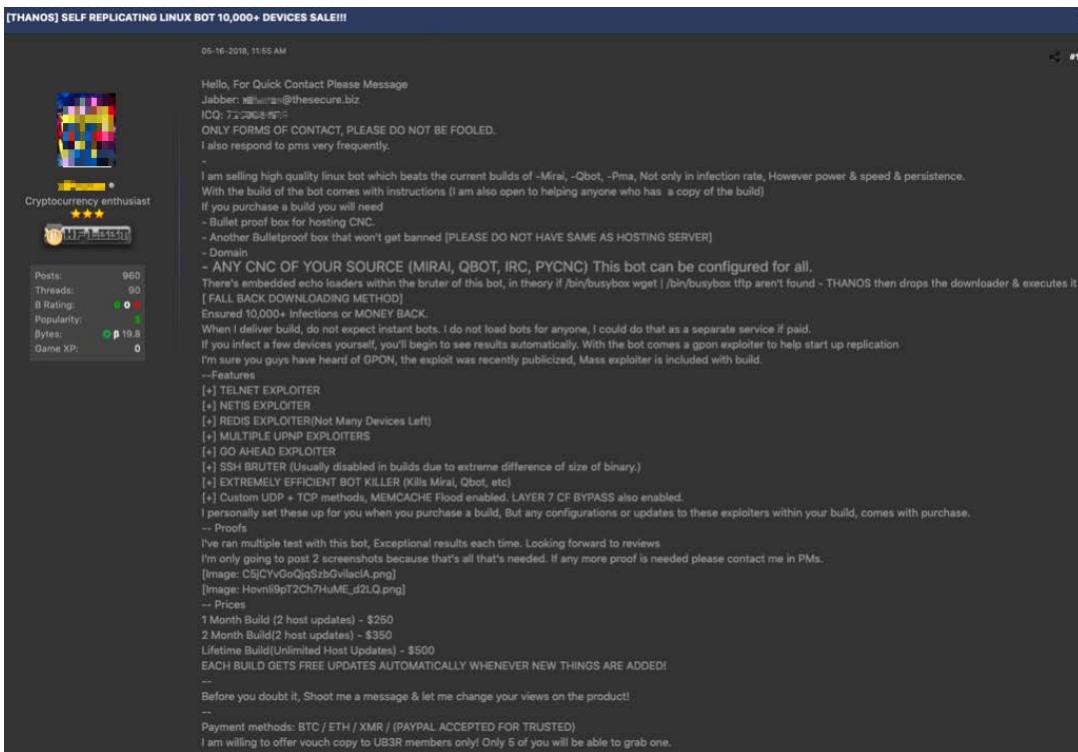


Figure 73. A Mirai botnet variant rental service starting at US\$250 a month

Figure 74. A Mirai botnet stressor service

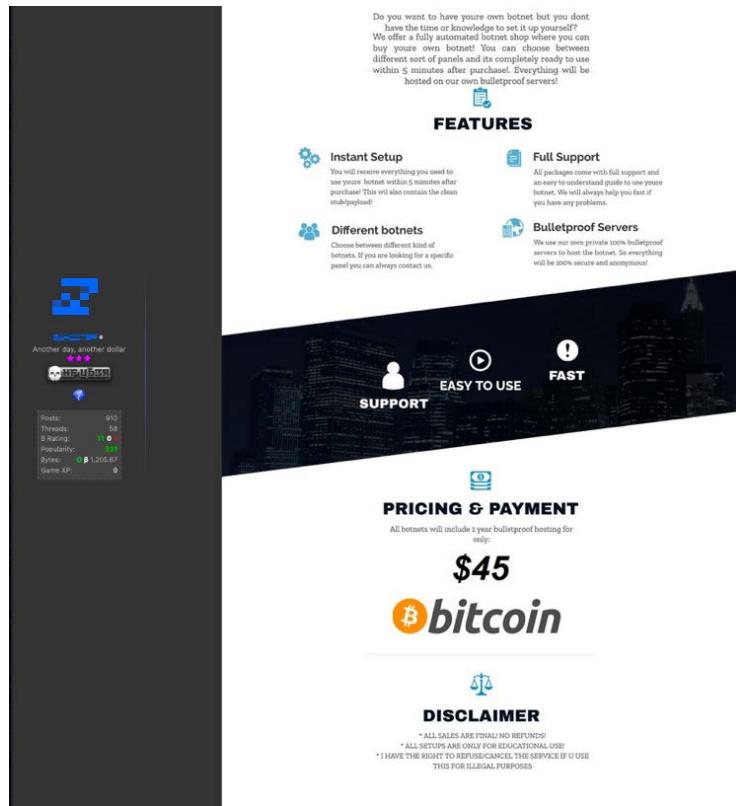


Figure 75. IoT botnet setup service with Bulletproof servers

IOT Botnet prices	
Service	Price
Mirai botnet rentals	US\$10 and up
Original Mirai source code	Free
Mirai based stressor	US\$20 and up
Fbot Mirai variant rental	US\$500 a week

Dark Web Marketplace Users Lose Trust

In March 2019, the dark web marketplace Dream Market announced that it was shutting down in April to transfer its services to a partner company. Shortly after, Wall Street Market, Valhalla, and DeepDotweb became part of the long list of marketplaces that law enforcement took down in May 2019. Wall Street Market administrators were planning an exit scam using money held in escrow for current transactions when law enforcement arrested them.²⁵

After a major marketplace shuts down, the dark web community usually migrates to other coexisting markets. However, because of current volatility within the landscape, there is no dominant and stable marketplace.

We observed multiple chats on Dread discussing slow sales after the May 2019 takedowns. Users frequently posted about fears of exit scams and law enforcement involvement. Sites like Empire, which became one of the top markets in the wake of the takedowns, are consistently battling login problems and DDoS attacks. Forum users on Torum and Dread regularly express frustration at marketplaces because of these issues (Torum is a crypto-driven, multi-functional, self-governing forum). The source of the DDoS activity is rumored to be law enforcement. In November 2019, it was reported that the Berlusconi Market was taken down by the Italian police, which discouraged dark web users even more.²⁶

Re: Why markets like Empire have so many mirrors and most of them are offline most of the time?

by [u/CallioLogix](#) » 29 Nov 2019

The direct answer is: Empire is the largest dark market nowadays, and one of the most trusted. There has been news that the German high tech federal people have been attacking it and other sites with heavy DDoS attacks that is slowing the whole onion network down and hitting the reliable sources such as Dread and Empire.

In all cases, as long as there are links that work it is a good sign. But we should always stay alert and not take anything for granted.

Dread was gone for long days and it is now back with a better system, as they claim, to handle the attacks.

Another theory is that Empire is preparing for an exit scam. For me I don't understand why not just do it without "preparation" which will make users stay away and not deposit.

Re: Why markets like Empire have so many mirrors and most of them are offline most of the time?

by [u/CallioLogix](#) » 29 Nov 2019

Be careful new links are great, but make sure you authenticate them through the site itself if you don't you will wind up getting phished just from the sheer volume of links around.

I think LE like to phish as well, when they can't knock the servers offline as they hope for that once in a life time nibble from a target of value.

Annoying but if the site you go to is any good you should be able to verify the links, a lot don't bother and they get phished as well because they just grab the links but never authenticate.

Figure 76.Torum post discussing why the Empire marketplace is frequently offline

Empire FORUM

by [u/CallioLogix](#) • 6 hours ago in [/d/Empire](#)

Will it ever be working again?
If not maybe there are forums like that?
Thanks!

4 comments

Comments

Sort comments by [Top](#)

[u/CallioLogix](#) 2 points 5 hours ago
was wondering the same thing

[u/CallioLogix](#) 2 points 4 hours ago
There are no functioning forums other than this. During previous downtimes I visited and immediately left thehub/envoy because of their lack of content. Scrolling through sections gives you last post date of 3 weeks ago. With recent downtime there was more content but they both failed the test big time. Neither is worthy of being a replacement. Perhaps people will flock there during next downtime but it will never be solid the way it is and people will leave when there is no more necessity to be there. Thehub has more content, larger posts but the people still don't know what the fuck they're talking about. Envoy is just few people talking to themselves. It really shows that it is just the drainage of people that are banned on normal places to be, instead of actually trying to be an alternative for everyone.

[u/CallioLogix](#) 1 points 3 hours ago
Yep i got the same feeling when visiting the ones you mention.
I so much liked the empire forum because you could read and then check the vendor on the market to see his feedback and listings.. Was very convenient! :)
Found some forums on the clearnet but they seem like a total scam.. Seems there is nothing like empire forum has been... And it is sad..

If anyone knows any news regarding Empire Forum or places like it please write it here! Thanks!

Figure 77. Empire users are worried an exit scam is inevitable

WHO CAN YOU TRUST?!

[Post Reply](#)

WHO CAN YOU TRUST?!

by [/u/thisisnotme](#) • 27 Nov 2019

i am sick of getting scammed! seems like you can't trust a damn soul on here. Why can't there be just ONE GOOD TRUSTWORTHY MARKET with a real honest reviews and plenty of people to vouch. All anybody wants to do is take your damn money. Can someone please help find trustworthy sites????

Re: WHO CAN YOU TRUST?!

by [/u/FireFox](#) • 27 Nov 2019

use the forum to find vouched for vendors and then buy from them..

Re: WHO CAN YOU TRUST?!

by [/u/thisisnotme](#) • 27 Nov 2019

thats what i've been trying to do.. but i can't find any posts with multiple vouches its only one person recommending a site.. that one person could be a scammer to all i know.. its hard to trust people on here. especially after being scammed 3 damn times

Re: WHO CAN YOU TRUST?!

by [/u/FireFox](#) • 27 Nov 2019

what are you looking for? trust no marketplace man!!!

Re: WHO CAN YOU TRUST?!

by [/u/thisisnotme](#) • 27 Nov 2019

just a reliable TRUSTWORTHY vendor that sells cc's with pins. Or even paypal transfers. But i dont know who to trust anymore. [/u/thisisnotme](#) is starting to get too risky for me as i can only make online transactions. I just want to hit an atm and be done.

Figure 78.Torum post discussing distrust in the marketplace community

WE NEED TO STOP THIS CYCLE OF EXIT SCAMMING MARKETS

3 by [/u/thisisnotme](#) • 6 months ago* in [/d/exit_scams](#)

with the problems over at empire about withdrawing (see post/129c79e32430e0e4f4f9) everything is coming to a head. even if they resolve it and its just a technical issue, this happens way too much.

wsm got off with millions (until they got busted for being fuckin stupid), dream went balls up, this happens over and over and fucks over thousands of people. also, LE has shown they can penetrate these sites all the time and even with encryption can find people.

then we got ddos bullshit happening all the fucking time

whats the solution?

1. vendors want FE, but hard to trust only FE. many scammers around, and buyers like the safety of escrow, this isn't going to change
2. nobody uses multisig, its not too difficult, but buyers already struggle to encrypt their addresses, let alone use multisig!
3. centralized markets are a target. they can be ddos'd and make it impossible to use
4. decentralized markets like openbazaar are trickier to use and the search feature is difficult to use

how do we fix this?

some ideas:

1. use an independent onion-based btc and monero / other alt-coin escrow service that is disconnected from the markets. can be used for any escrow service, not just drug markets.
2. have third parties mediate disputes. mediators can get a percentage for helping and be assigned tickets randomly to prevent corruption. all vendors use tracking labels to confirm they shipped something. not perfect, but about the same level of trust as on the markets.
3. independent rating site for vendors. no sales happen on the site itself, low overhead, hard to DDOS (and ratings sites have little in the way of money, how can you blackmail that?). maybe some way to have escrow transactions rated when buyers marked it finalized and being able to import individual ones to the rating site? need to find a way to minimize fake transactions.

some ideas, i kno they need work. thoughts anyone?

Figure 79. Dread discussion on exit scams

The marketplace community has been looking for ways to build trust. A new site called DarkNet Trust was created to verify vendors' reputations by searching through usernames and PGP fingerprints. DarkNet Trust searches over 10,000 profiles from Dream, Empire, Nightmare, Berlusconi, Tochka, Cryptonia, Apollon, Grey Market, and Agora.

New encrypted email services like Sonar and Elude have also suddenly appeared. Former favorite Protonmail was accused of helping law enforcement in the past, prompting dark web users to look for alternative email services.²⁷

Administrators of new marketplaces are also adding new security features, for example: walletless markets, multisignatures on BTC and Monero, and no-javascript policies. Grey Market and BitBazaar are new walletless markets. Monopoly is a walletless market where payment is directly made between buyer to vendor, and the market gets a monthly commission as opposed to transaction fees. The Cryptonia marketplace uses multisignature wallets for transactions.

The screenshot shows the DarkNet Trust website interface. At the top, there is a navigation bar with links for Home, Donate, Login, and Register. Below the navigation is a search bar with placeholder text "Search by username or PGP fingerprint" and a "Search" button. A note below the search bar specifies that letters, numbers "-", and "_" are allowed, with a minimum of 3 characters, and a limit of 12 results per query. The main content area displays several vendor profiles in cards:

- Empire Market**: Member since: July 07, 2018, Last online: Nov 16, 2019, Rating: 89.21%
- CRYPTONIA MARKET**: Member since: 2019-04-29, Last online: -, Rating: 95.35%
- APOLLON**: Member since: Jul 21, 2018, Last online: Oct 23, 2019, Rating: 94%
- Hunter**: Member since: July 07, 2018, Last online: Nov 16, 2019, Deals: 408, Rating: 89.21%, Vendor Level: 3, Trust Level: 2, Reviews: 220, Positive Reviews: 186, Neutral Reviews: 10, Negative Reviews: 24. There is a link to "Register to write a review" and a note that the profile was last updated on 2019-11-16.
- Empire Market**: This card is identical to the one above it, showing the same information for the Empire Market vendor.

Figure 80. A DarkNet Trust search for a specific underground vendor

Sonar

Easily encrypt all your messages

[Login](#) · [Register](#)

About

No logs, no javascript, no tracking, no email, no clearnet.

Sonar is the most secure and private web messaging system available in the Darknet.

Easily encrypt ALL your messages.

Comparison Table

Here you can compare the security and privacy features of several messaging systems.

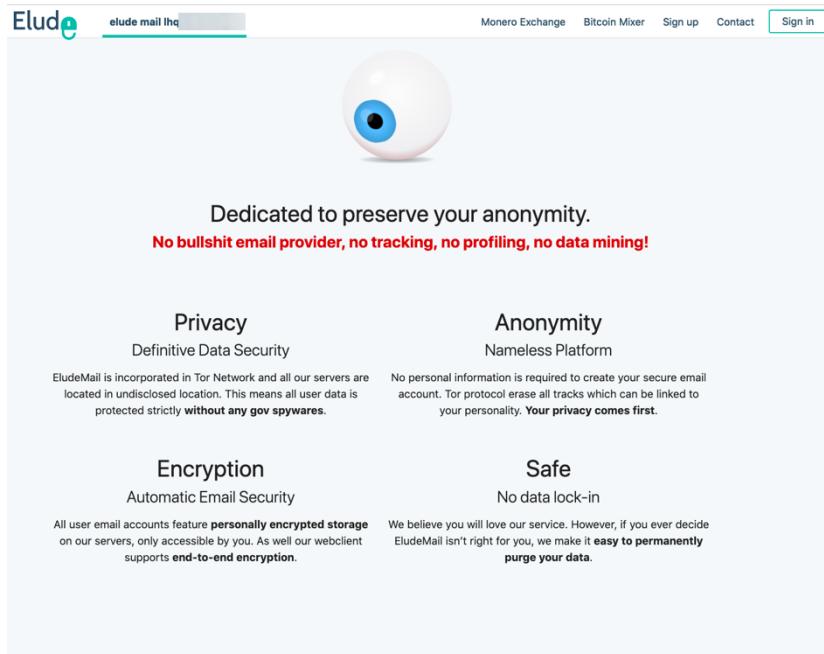
Website	Remove own messages	Remove peer messages	Allows auto-encrypt	Self destruction	Plain text disabled
Empire	x	x	x	x	x
Sonar	Yes	Yes	Yes	In progress	Yes
Dread	Yes	Yes	x	x	x
Apollon	Yes	x	x	Yes	x
Cryptonia	Yes	x	Yes	x	x
Tochka	x	x	x	x	x
Cannazon	x	x	x	x	x
Dream Alt	x	x	x	x	x
Nightmare	x	x	Yes	x	x

Features



Sonar uses Public-key cryptography in order to encrypt every message before it is stored in the server. A private key and public key are generated for every user upon registration.

Figure 81. Sonar, a new email encryption service



The screenshot shows the EludeMail homepage. At the top, there's a navigation bar with links for "Monero Exchange", "Bitcoin Mixer", "Sign up", "Contact", and a "Sign in" button. The main visual is a large white eye icon with a blue iris. Below the eye, the text reads "Dedicated to preserve your anonymity." and "No bullshit email provider, no tracking, no profiling, no data mining!". There are two columns of text: "Privacy" (Definitive Data Security) and "Anonymity" (Nameless Platform). Under "Privacy", it says "EludeMail is incorporated in Tor Network and all our servers are located in undisclosed location. This means all user data is protected strictly without any gov spywares." Under "Anonymity", it says "No personal information is required to create your secure email account. Tor protocol erase all tracks which can be linked to your personality. Your privacy comes first." At the bottom, there are sections for "Encryption" (Automatic Email Security) and "Safe" (No data lock-in). It states that "All user email accounts feature personally encrypted storage on our servers, only accessible by you. As well our webclient supports end-to-end encryption." and "We believe you will love our service. However, if you ever decide EludeMail isn't right for you, we make it easy to permanently purge your data."

Figure 82. Elude, a secure email system

Users on dark web forums also suggested that blockchain technology could host decentralized marketplaces. Sites that are hosted on blockchain are perceived to be less susceptible to law enforcement takedowns and surveillance. One such decentralized blockchain DNS service is Blockchain-DNS, or BDNS, which can access domains such as .bit, .bazar, .coin, .emc, as well as other domain name extensions used by OpenNIC. (This echoes a prediction we made in 2013 that .bit domains are advantageous to cybercriminals and could eventually be used for malicious activity.²⁸) However, the idea of using these types of markets hasn't particularly caught on. Some dark web forum users say decentralized markets are not easy to use, and it is harder to search for products.

So far, a few organizations have experimented with different structures and new features. We noted that a popular carding site, Jokers Stash, moved to a blockchain DNS to avoid law enforcement surveillance. OpenBazaar, an open-source, decentralized P2P market, has an Android and iOS app that allows users to chat privately. It has experienced steady growth over the last three years but has yet to become a top marketplace. Utopia is another new marketplace that was launched in late 2019. It is advertised as a marketplace that can bypass online censorship, firewalls, and surveillance with its built-in use of encrypted text, email, and messages.

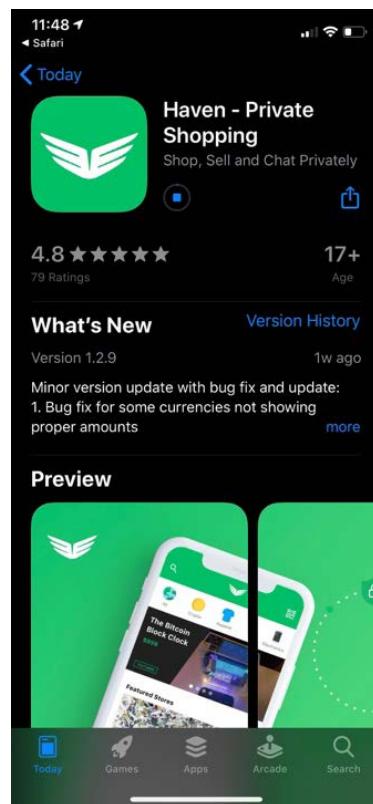


Figure 83. OpenBazaar iOS app

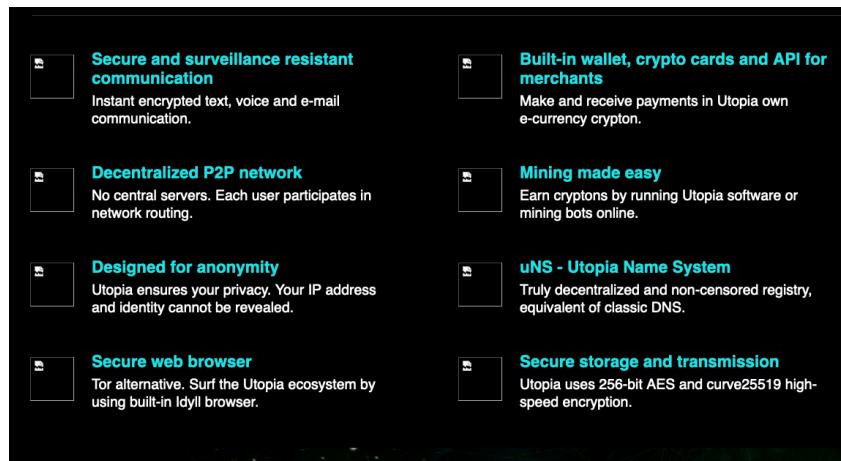


Figure 84. Utopia's security features for gaining the user's trust

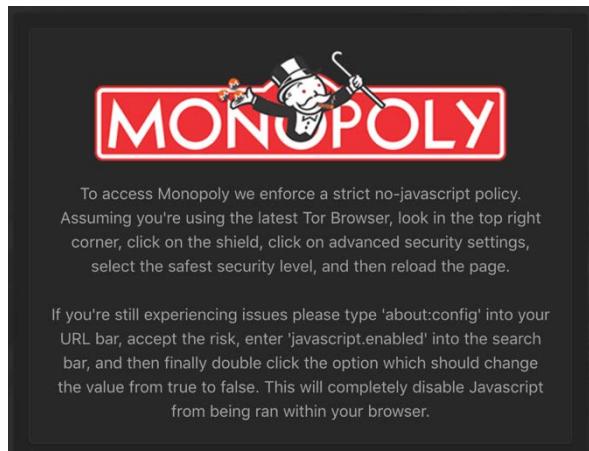


Figure 85. Monopoly's strict no javascript policy

Discord Used for Direct Messaging and Sales

Two years ago, we saw that many cybercriminals used the Telegram messaging app to facilitate their malicious activity. In 2019, cybercriminals moved to Discord, a popular communication platform with more than 250 million users as of May 2019. The platform is viewed as a safe place that allows users some degree of anonymity.

Underground forums and dark web marketplaces have created their own Discord servers. While these channels are not as busy as the forums themselves, we have observed the same goods and services being offered for the same prices.



Figure 86. Discord group for sellers

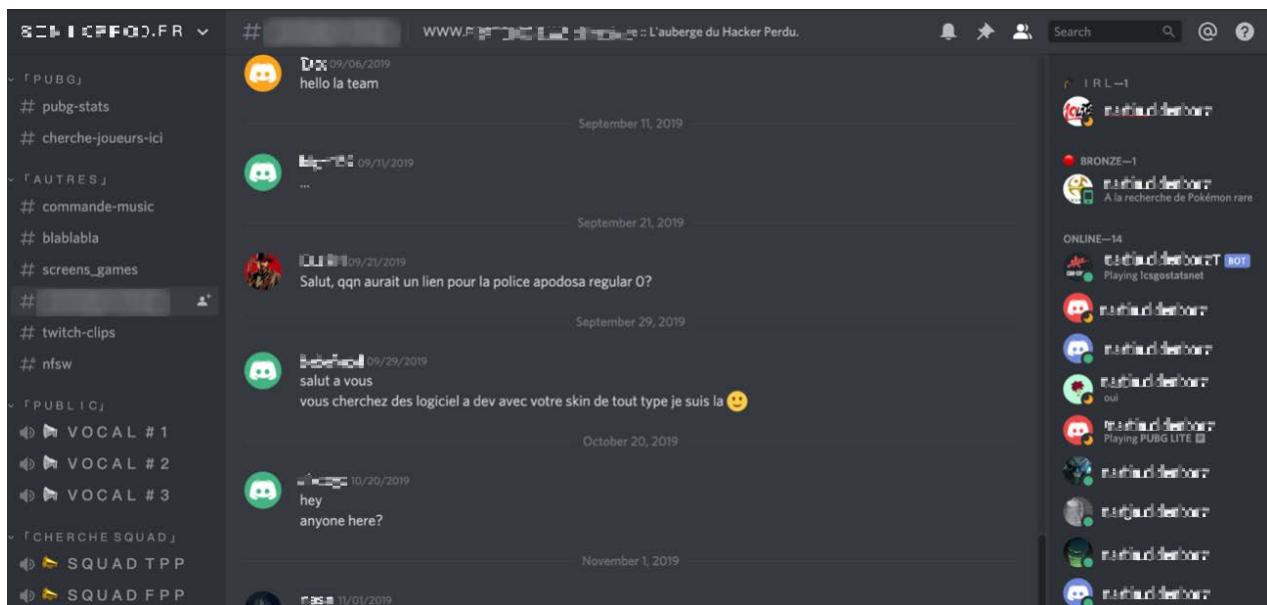


Figure 87. French underground forum Piratologie Discord channel

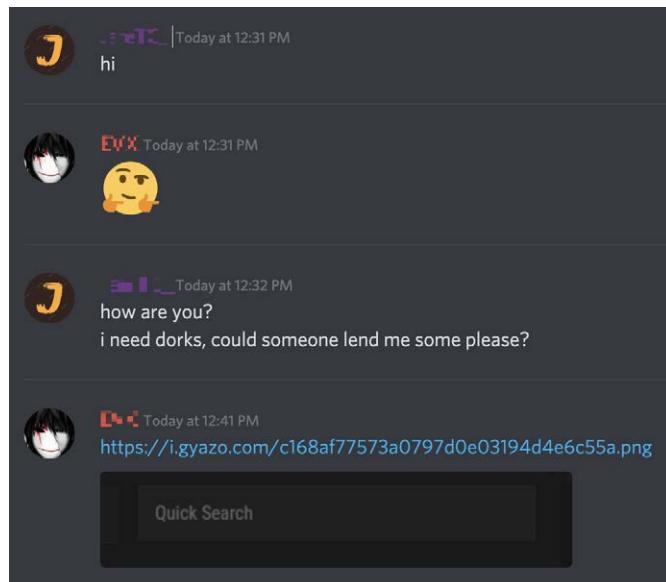


Figure 88. Discord channel for OG forum

African Cybercrime Increases

In our 2017 research paper on the West African underground market²⁹ we predicted that West African cybercriminals would shift to more elaborate crimes, complex operations, and business models. BEC and tax fraud are examples of such activities.

Internet and mobile users have increased in Africa over the last two years, and more people are using online banking, online bill payments, and social media accounts. This, of course, is a ripe environment for cybercriminals. Several hacking groups have already emerged. In 2017, members of the Forkbombo group were arrested for exploiting banking infrastructure loopholes to steal millions from Kenyan banks. SilentCards, a group that supposedly spawned from Forkumbo, reportedly continues to siphon ATMs and target banks.^{30, 31} In West Africa, the group Silent Starling successfully infiltrated more than 500 organizations worldwide with BEC attacks in 2019. The group first started with romance scams.³²

SIM Card Services Popular but Prices Remain Private

SIM swapping and SIM-jacking will be a growing threat that takes advantage of remote employees and everyday users. Since mobile devices are used for enterprise authentication, hijacked SIM cards can give hackers access to a user's enterprise email account as the hardware is "trusted." This means that they will be able to access all manner of corporate data covertly.³³

Underground offerings vary from free tutorials to region-specific SIM card services. Many of the services are offered in Russian language forums. In forums of other languages, they were not so visible. Prices for these services are commonly unlisted and only available through private messages.

Theft of Australian sims! Simswap Australlia!

Posted by [REDACTED] Nov 11, 2019 to Banks and money transfers

M 0
Posted by Nov 11, 2019

Hello everyone, I want to offer you the services of hijacking Australian sim cards. We can steal almost any number, break through the missing info and much more in Australia. Our service opens for you new boundaries of monetization of your logs / botnets, everything that was previously protected by SMS and could not be cashed out, turns into money with us. We will steal the phone number, the account owner, we will receive SMS with the transfer code and voila)

I immediately warn you, I communicate only with the owners of botnets / logs, pioneers of police and others go to ignore.

The first contact PM.

P.S. We merge top banks only with VNC!
P.P.S. Keylogger is desirable.

Figure 89. Russian language forum offering SIM swaps in Australia

sim swap UK hacker needed to join my work

Thread Modes

Registered Member 5★
REGISTERED CARDER

Posts: 1
Threads: 0
Escrow Balance: 0\$

#1

Im Uk based i need help find a good uk hacker it would be will to help or join my team for long term work, the work needed is for sim swap mobile take over.
I would appreciate it if its something you cant do but you know what software they use any info would be great.. love

Q Find Reply

Figure 90. Russian language forum asking for SIM swap hackers

The Future of Seller Spaces

Predicting how underground markets and forums will evolve is complicated, but we can reasonably anticipate certain issues with sufficient data and insight. We have identified several scenarios we expect to see in the cybercriminal underground economy within the next three years.

Deepfake ransomware will be the evolution of sextortion. Deepfakes will move away from creating fake celebrity pornographic videos, and veer into manipulating company employees and teenagers. These tools will demand a higher price than non-sextortion ransomware builds.

More cybercrime will hit Africa in the next three to five years. As more citizens use online platforms for banking and transactions, cybercriminals will develop tools and schemes to take advantage of them. Established hacking groups are already attacking financial institutions, and we predict more will follow.

Cybercriminals will find a scalable business model that takes advantage of the IoT's wide attack surface. Cybercriminals will move away from simple DDoS to data interception or using the machines as long-term infected proxies to make botnets harder to map out. Cybercriminals will hone in on IoT devices for espionage and extortion.

We will see smart contracts in escrow offered in underground forums. Replacing escrow with a blockchain for trust could help guarantee that both parties get what they want out of the deal, without the need to establish trust through reputation.

SIM card hijacking will increase and target high-level executives. Underground forums currently offer services involving the use of social engineering on telecommunication companies to swap SIMs. Many offerings exist for SIM card swaps, usually from a company insider. Gaining access to your account allows hackers to pass 2-step verification process in various platforms.

Appendix of Prices

Past

Generic Android botnet	Up to US\$1,500
Generic DDOS botnet	US\$50 a day
Panel.builder for a form grabber botnet	US\$100
Botnet rentals	US\$5 and up
Generic botnet builds	Free and up
RevengeRAT/NjRAT	Free
Generic Android RATS	US\$1 and up
Source code for a generic RAT	US\$49 and up
Monthly RAT subscriptions	US\$5 and US\$25
Generic ransomware build	US\$5 and up
Ranion ransomware	US\$900 a year
Cryptolocker ransomware	US\$100
Jigsaw ransomware	US\$3,000
Dharma ransomware	US\$100
Generic crypterbuilders	US\$99 and up
Crypteras a service	US\$20 and up
Kronos-based malware	US\$3,000 and up
Generic Android banking malware	US\$100 and up
ATM Malware	US\$2,000 and up
GozNym malware	US\$750
Phone Flooder	US\$50 and up
SMS bulk sender	US\$25 to US\$500
SMS sender monthly	US\$2 and up
Netflix accounts	US\$2 and up
Banking credentials	US\$5 and up
Spotify accounts	US\$3 and up
Disney+ accounts	US\$1 and up
McDonald's accounts	US\$1 and up
Domino's accounts	US\$1 and up
Grubhub accounts	US\$3 and up
Store credentials with credit cards	US\$1.50 and up
High balance credit cards	US\$100
Bulk credit cards	US\$1 each

Verified credit cards	US\$10 and up
Fake credit card statement	US\$25
Registered passport service	US\$2,500
Scan copies of real passports	US\$1 and up per copy
Forged Pharmacy Rx labels	US\$60 and up
Identity kits	US\$20 and up
Driver's license scans	US\$10 and up

Present

United States Voter databases	Free to US\$9.99
Non-U.S. Voter databases	US\$9.99-US\$400
1,000 Facebook likes	US\$3 and up
1,000 Instagram likes	US\$0.15 and up
50 Twitch likes	US\$0.50 and up
Social media bot	US\$25 and up
1,000 YouTube likes	US\$26 and up
20,000 new visitor hits	US\$5 and up
Deepfake videos	From US\$50
Deepfake still images	From US\$2.50 each
Software to create deepfakes	From US\$25
Roblox	From US\$36
Gambling bot	From US\$75
Sports Betting AI	From US\$30
Fitbit Social Engineering course	From US\$100
Fitbit Ionic	From US\$40
Fitbit Versa	From US\$35
Mirai botnet rentals	US\$10 and up
Original Mirai source code	Free
Mirai based stresser	US\$20 and up
FbotMirai variant rental	US\$500 a week

References

- 1 Trend Micro. (n.d.) *Trend Micro Security News*. “Cybercriminal Underground Economy Series.” Last accessed on 26 March 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercriminal-underground-economy-series>.
- 2 Brian O’Connor. (9 May 2018). *Experian*. “Cybercrime: The \$1.5 Trillion Problem.” Last accessed on 28 March 2020 at <https://www.experian.com/blogs/ask-experian/cybercrime-the-1-5-trillion-problem/>.
- 3 Macrotrends. (n.d.) *Macrotrends*. “Apple Revenue 2006-2019 AAPL.” Last accessed on 26 March 2020 at <https://www.macrotrends.net/stocks/charts/AAPL/apple/revenue>.
- 4 Reuters. (12 July 2019). *Reuters*. “Saudi Aramco reports 2018 net income of \$111.1 billion”. Last accessed on 26 March 2020 at <https://www.reuters.com/article/us-saudi-oil-aramco-idUSKCN1TD12O>.
- 5 Zak Stambor. (30 January 2020). *Digital Commerce 360*. “Amazon’s 2019 sales rise 20.5%.” Last accessed on 26 March 2020 at <https://www.digitalcommerce360.com/article/amazon-sales/>.
- 6 Max Goncharov. (28 July 2015). *Trend Micro Security News*. “The Russian Underground Today: Automated Infrastructure, Sophisticated Tools.” Last accessed on 26 March 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/russian-underground-automized-infrastructure-services-sophisticated-tools>.
- 7 Juliana De Groot. (24 October 2019). *Digital Guardian*. “A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time.” Last accessed on 26 March 2020 at <https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time>.
- 8 Kyle Wilhoit and Stephen Hilt. (7 December 2015). *Trend Micro Security News*. “North American Underground: The Glass Tank.” Last accessed 26 March 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/north-american-underground-the-glass-tank>.
- 9 Numaan Huq, Vladimir Kropotov, Mayra Rosario, David Sancho, and Fyodor Yarochkin. (28 June 2019). *Trend Micro Security News*. “Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground.” Last accessed on 26 March 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crimeware-for-sale-the-commoditization-of-atm-malware-in-the-cybercriminal-underground>.
- 10 Jane Wakefield. (16 May 2019). *BBC*. “GozNym cyber-crime gang which stole millions busted.” Last accessed on 26 March 2020 at <https://www.bbc.com/news/technology-48294788>.
- 11 United Nations Department of Economic and Social Affairs. (17 Septemebr 2019). *United Nations*. “The number of international migrants reaches 272 million, continuing an upward trend in all world regions, says UN.” Last accessed on 26 March 2020 at <https://www.un.org/development/desa/en/news/population/international-migrant-stock-2019.html>.
- 12 Rachita Rake. (n.d.) *Allied Market Research*. “E-Passport Market Expected to Reach \$57,061 Million, Globally, by 2023.” Last accessed on 26 March 2020 at <https://www.alliedmarketresearch.com/press-release/E-passport-market.html>.
- 13 Brian Owens. (13 May 2019). *The National Center for Biotechnology Information*. “Opioid prescriptions down but some patients fear doctors now too strict.” Last accessed on 26 March 2020 at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6520068/>.
- 14 Paul Uhrig. (1 July 2019). *Surescripts*. “It’s Official: Hla fo All States Will Soon Require E- Perscrivbing to Combat the Opioid Epidemic.” Last accessed on 26 March 2020 at <https://surescripts.com/news-center/intelligence-in-action/opioids/it-s-official-half-of-all-states-will-soon-require-e-prescribing-to-combat-the-opioid-epidemic/>.
- 15 Best Fortnite. (April 2019). *Best Gaming Settings*. “25 Best Fortnite Skins—the Rarest Skins Ever!” Last accessed on 26 March 2020 at <https://bestfortnitesettings.com/best-fortnite-skins/>.
- 16 Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin. (13 June 2017). *Trend Micro Security News*. “Fake News and Cyber Propaganda: The Use and Abuse of Social Media.” Last accessed on 26 March 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media>.
- 17 BBC Technology. (19 June 2017). *BBC*. “Personal details of nearly 200 million US citizens exposed.” Last accessed on 26 March 2020 on <https://www.bbc.com/news/technology-40331215>.
- 18 Alex Hern. (11 April 2016). *The Guardian*. “Philippine electoral records breached in ‘largest ever’ government hack.” Last accessed on 31 March 2020 at <https://www.theguardian.com/technology/2016/apr/11/philippine-electoral-records-breached-government-hack>.
- 19 Trend Micro. (24 April 2019). *Trend Micro Security News*. “New Sextortion Scheme Demands Payment in Bitcoin Cash.” Last accessed on 26 March 2020 at <https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/new>-

- sextortion-scheme-demands-payment-in-bitcoin-cash.
- 20 Panda Security. (2 October 2019). *Panda Security*. “Fraud with a deepfake: the dark side of artificial intelligence.” Last accessed on 26 March 2020 at <https://www.pandasecurity.com/mediacenter/news/deepfake-voice-fraud/>.
- 21 Fitbit. (n.d.) *Fitbit*. “Products.” Last accessed on 26 March 2020 at <https://www.fitbit.com/de/store>.
- 22 Fitbit. (n.d.) *Fitbit*. “Fitbit Limited Warranty.” Last accessed on 26 March 2020 at <https://www.fitbit.com/legal/returns-and-warranty>.
- 23 Stephen Hilt, Vladimir Kropotov, Fernando Merces, Mayra Rosario, and David Sancho. (10 September 2019). “Uncovering IoT Threats in the Cybercrime Underground.” Last accessed on 31 March 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-internet-of-things-in-the-cybercrime-underground>.
- 24 Hui Wang. (14 September 2018). *Netlab*. “Fbot, A Satori Related Botnet Using Block-chain DNS System.” Last accessed on 26 March 2020 at <https://blog.netlab.360.com/threat-alert-a-new-worm-fbot-cleaning-adbminer-is-using-a-blockchain-based-dns-en/>.
- 25 Adi Robertson. (3 May 2019). *The Verge*. “Police just took down a massive dark web marketplace in Germany.” Last accessed on 26 March 2020 at <https://www.theverge.com/2019/5/3/18528211/wall-street-market-silkkitie-valhalla-dark-web-takedown-police-germany>.
- 26 Pierluigi Paganini. (8 November 2019). *Security Affairs*. “Italian police shut down dark web Berlusconi market and arrested admins.” Last accessed on 26 March 2020 at <https://securityaffairs.co/wordpress/93603/cyber-crime/berlusconi-market-darkweb.html,2019>.
- 27 Eduard Kovacs. (30 May 2019). *Security Week*. “ProtonMail Accused of Voluntarily Helping Police Spy on Users.” Last accessed on 26 March 2020 at <https://www.securityweek.com/protonmail-accused-voluntarily-helping-police-spy-users>.
- 28 Robert McArdle and David Sancho. (19 November 2013). *Trend Micro Security News*. “.Bit Domain Used To Deliver Malware and other Threats.” Last accessed on 26 March 2020 at <https://www.trendmicro.com/vinfo/au/security/news/cybercrime-and-digital-threats/bit-domain-deliver-malware-and-other-threats>.
- 29 Trend Micro and INTERPOL. (9 March 2017). *Trend Micro Security News*. “Is There a Budding West African Underground Market?” Last accessed on 26 March 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/west-african-underground?>.
- 30 Victor Amadala. (2 May 2019). *The Star*. “Revealed: Here are hacker groups looting banks in Kenya.” Last accessed on 26 March 2020 at <https://www.the-star.co.ke/business/2019-05-02-revealed-here-are-hacker-groups-looting-banks-in-kenya/>.
- 31 Eddy Mwanza. (2 May 2019). *Kenyans*. “Hacker Group That Siphoned Ksh400 Million From Local Bank.” Last accessed on 26 March 2020 at <https://www.kenyans.co.ke/news/39309-hacker-group-siphoned-ksh400-million-local-bank>.
- 32 Luke Christou. (n.d.). *Verdict 3ncrypt*. “Silent Starling: Pioneering Vendor Email Compromise, 2020’s ‘Biggest Financial Threat’.” Last accessed on 31 March 2020 at https://verdict-encrypt.nridigital.com/verdict_encrypt_winter19/silent_starling_vendor_email_compromise.
- 33 Craig Gibson. (15 November 2019). *Trend Micro Security News*. “From SIMjacking to Bad Decisions 5G Security Threats to Non-Public Networks.” Last accessed on 31 March 2020 at <https://www.trendmicro.com/vinfo/hk/security/news/internet-of-things/from-esim-jacking-to-fake-news-threats-to-5g-and-security-recommendations>.



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

