Detecting and Fingerprinting Infostealer Malware-as-a-Service platforms

blog.bushidotoken.net/2022/11/detecting-and-fingerprinting.html

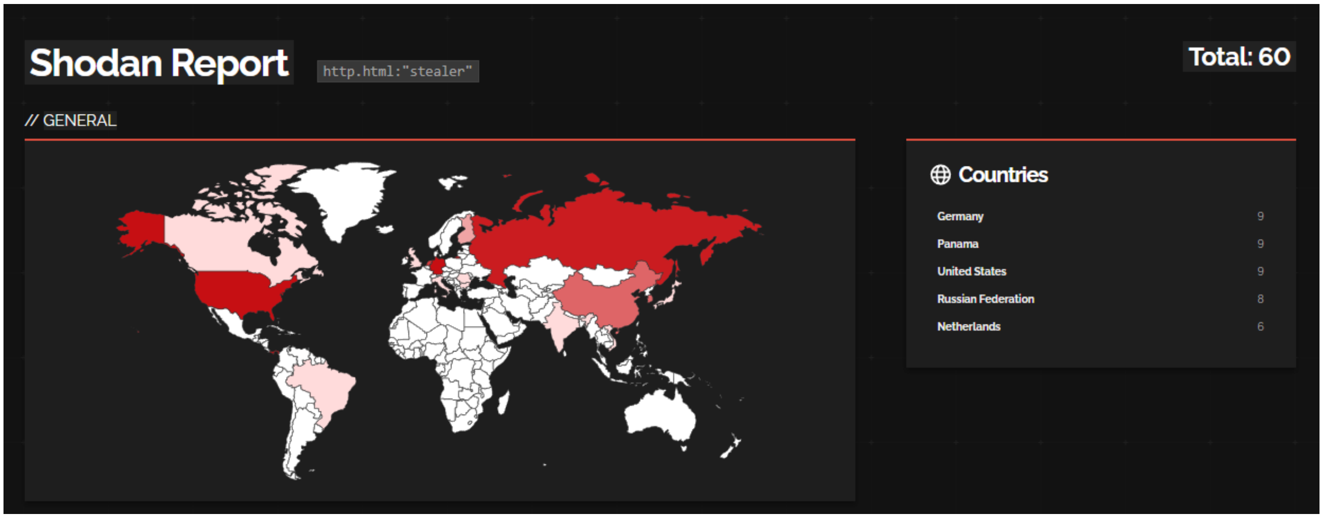
BushidoToken

Cyber threat intelligence largely involves the tracking and studying of the adversaries outside of your network. Gaining counterintelligence about your adversaries' capabilities and weaponry is one of the final building blocks for managing a strong cyber defense. In the pursuit of performing this duty, I have been studying how to discover adversary infrastructure on the internet. One good way of doing this has been via leveraging the scan data available through the popular Shodan search engine. If you've not used it before, Shodan periodically scans the entire internet and makes it available for users to query through. It is often used to monitor networks, look for vulnerabilities, and ensure the security of an organization's perimeter.

But we can also use Shodan for tracking the adversaries. Through the process of fingerprinting - that is to identify unique attributes of IPs on the internet - we can find command and control (C2) servers and login panels belonging to cybercriminals online.

Through this process, I was able to identify dozens of infostealer control panel login pages, as well as three infostealer malware families, called Titan Stealer, Patriot Stealer, and Raxnet Stealer, that have not yet been reported elsewhere online (as far as I could tell).

It all started by searching http.html:"stealer" in Shodan. This revealed several login pages for known and unknown infostealer malware. I have since created a page on my GitHub repo to share some Shodan dorks that help reveal adversary infrastructure.



Shodan Report `http.html:"stealer"`

Total: 60

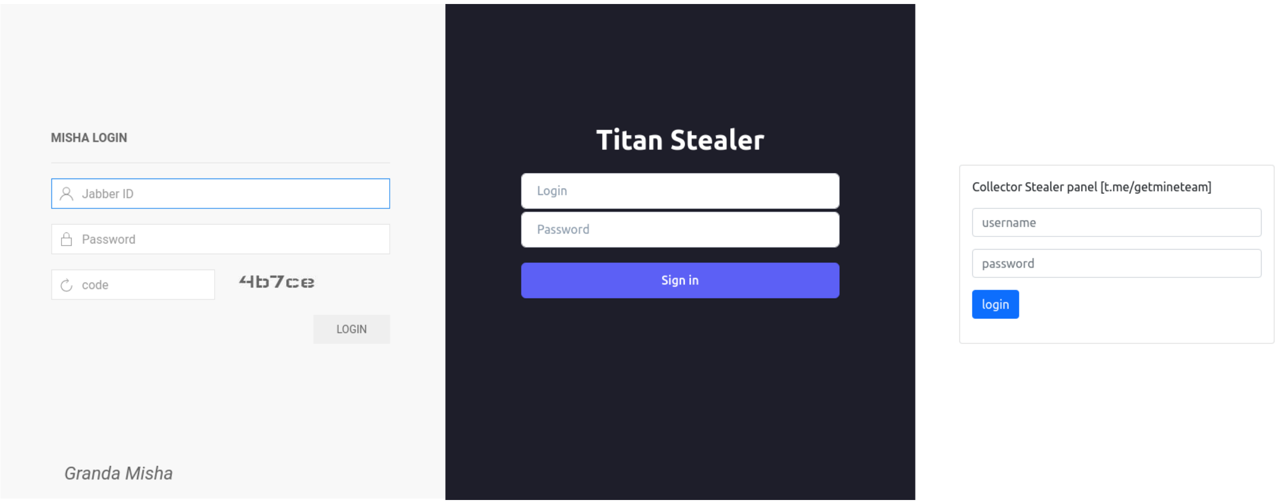
// GENERAL

Countries

Germany	9
Panama	9
United States	9
Russian Federation	8
Netherlands	6

Misha, Collector, and Titan Stealer

The above Shodan dork revealed dozens of IPs, which if investigated were found to be login panels for infostealer malware families. Misha Stealer and Collector Stealer are two semi well-known malware families. The "Titan Stealer" panel appears to be new with apparently no references online, vendor reports, or social media mentions by other researchers. Looks like one we should track in my books.



MISHA LOGIN

Granda Misha

Titan Stealer

Collector Stealer panel [t.me/getmineteam]

Grand Misha (aka Misha Stealer)

- Shodan Dork

    http.title:"misha" http.component:"UIKit"

- URLscan Query
    - https://urlscan.io/search/#filename:%22misha.css%22
    - https://urlscan.io/search/#task.tags:%22misha%22

Collector Stealer

- Shodan Dork
    - http.html:"Collector Stealer"
    - http.html:"getmineteam"
- URLscan Query

    https://urlscan.io/search/#task.tags:%22collector%22

Titan Stealer

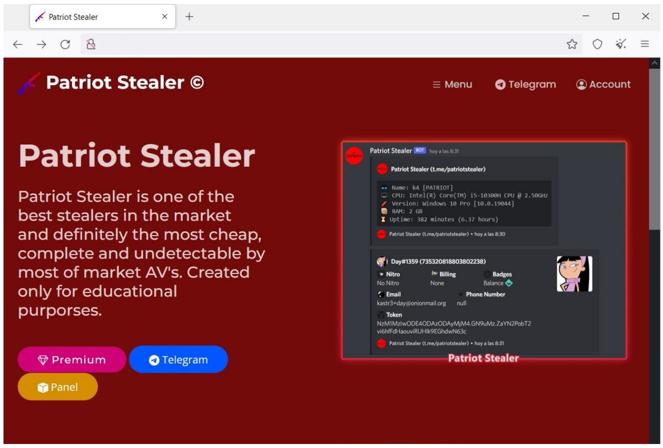
- Shodan Dork

    http.html:"Titan Stealer"
- URLscan Query

    https://urlscan.io/result/daca0fcd-bbc9-48c8-810d-89fee466b639

Patriot Stealer

The same Shodan Dork http.html:"stealer" also revealed an unreported and new Malware-as-a-Service (MaaS) platform marketing itself as "Patriot Stealer". The paid version of the infostealer malware is reportedly capable of stealing "passwords, cookies, Autofilldata, Telegram session, Persistence" and if you want to buy it you should speak to "@kastr3" on Telegram. Interestingly, the malware leverages Discord webhooks to report to the operator when a victim has been infected and data has successfully been stolen.



Patriot Stealer

Patriot Stealer is one of the best stealers in the market and definitely the most cheap, complete and undetectable by most of market AV's. Created only for educational purposes.

Patriot Stealer BOT hoy a las 8:31

Patriot Stealer (t.me/patriotstealer)

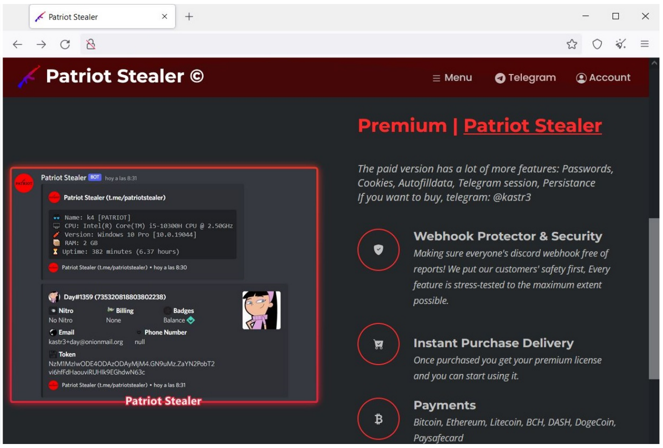
```
Name: k4 [PATRIOT]
CPU: Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz
Version: Windows 10 Pro [10.0.19044]
RAM: 2 GB
Uptime: 382 minutes (6.37 hours)
```

Patriot Stealer (t.me/patriotstealer) • hoy a las 8:30

Day#1359 (735320818803802238)

Nitro: No Nitro
Billing: None
Badges: Balance
Email: kastr3+day@onionmail.org
Phone Number: null
Token: NzM1MzlwODE4ODAzODAyMjM4.GN9uMz.ZaYN2PobT2vi6hfFdHaouviRUHIk9EGhdwN63c

Patriot Stealer (t.me/patriotstealer) • hoy a las 8:31



Patriot Stealer BOT hoy a las 8:31

Patriot Stealer (t.me/patriotstealer)

Name: k4 [PATRIOT]
CPU: Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz
Version: Windows 10 Pro [10.0.19044]
RAM: 2 GB
Uptime: 382 minutes (6.37 hours)

Patriot Stealer (t.me/patriotstealer) • hoy a las 8:30

Day#1359 (735320818803802238)

Nitro: No Nitro
Billing: None
Badges: Balance
Email: kastr3+day@onionmail.org
Phone Number: null
Token: NzM1MzlwODE4ODAzODAyMjM4.GN9uMz.ZaYN2PobT2vi6hfFdHaouviRUHIk9EGhdwN63c

Patriot Stealer (t.me/patriotstealer) • hoy a las 8:31

Premium | Patriot Stealer

The paid version has a lot of more features: Passwords, Cookies, Autofilldata, Telegram session, Persistance
If you want to buy, telegram: @kastr3

Webhook Protector & Security

Making sure everyone's discord webhook free of reports! We put our customers' safety first, Every feature is stress-tested to the maximum extent possible.

Instant Purchase Delivery

Once purchased you get your premium license and you can start using it.

Payments

Bitcoin, Ethereum, Litecoin, BCH, DASH, DogeCoin, Paysafecard

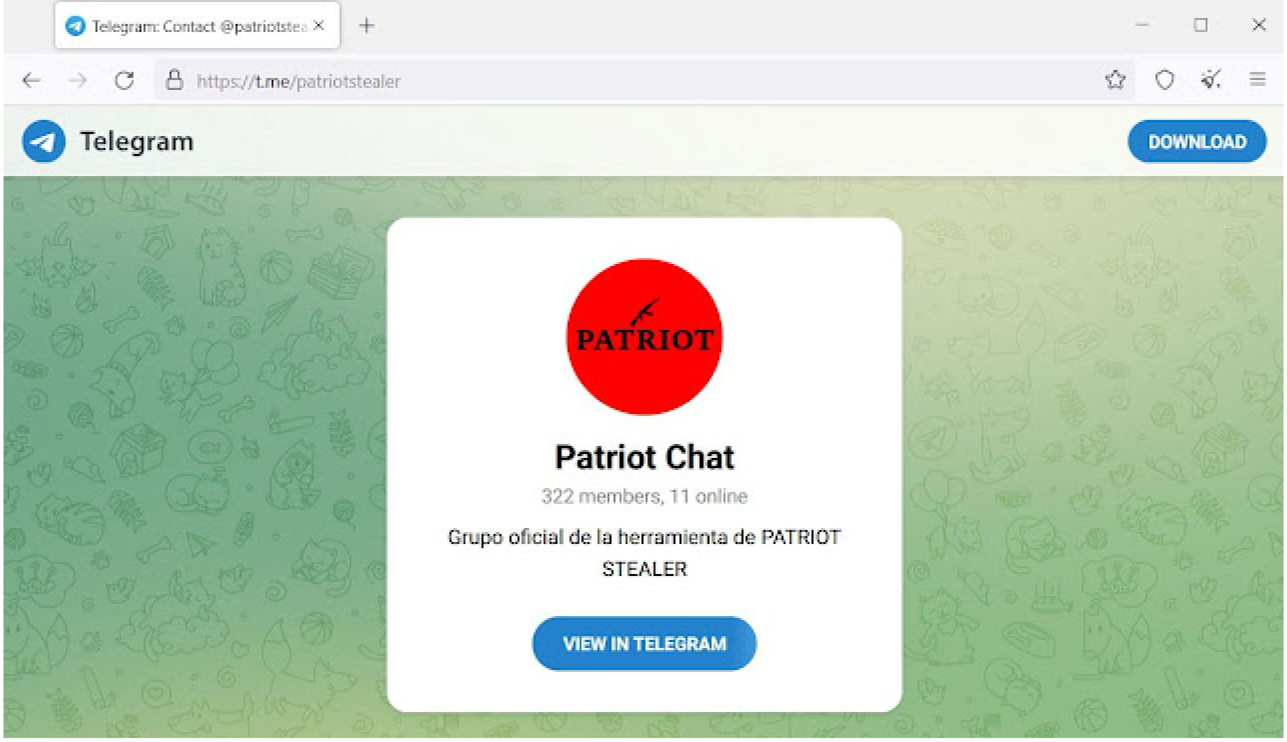
From the Discord language setting in the screenshot on the website and from the description of the group's Telegram channel it appears the developer(s) of the Patriot Stealer are Spanish-speaking threat actors.

Patriot Stealer

- Shodan Dork
  - http.favicon.hash:274603478
  - http.html:"patriotstealer"
- URLscan Query

  https://urlscan.io/result/43a51776-e283-4522-ab29-ea5c7efc174a/
- Telegram Channel

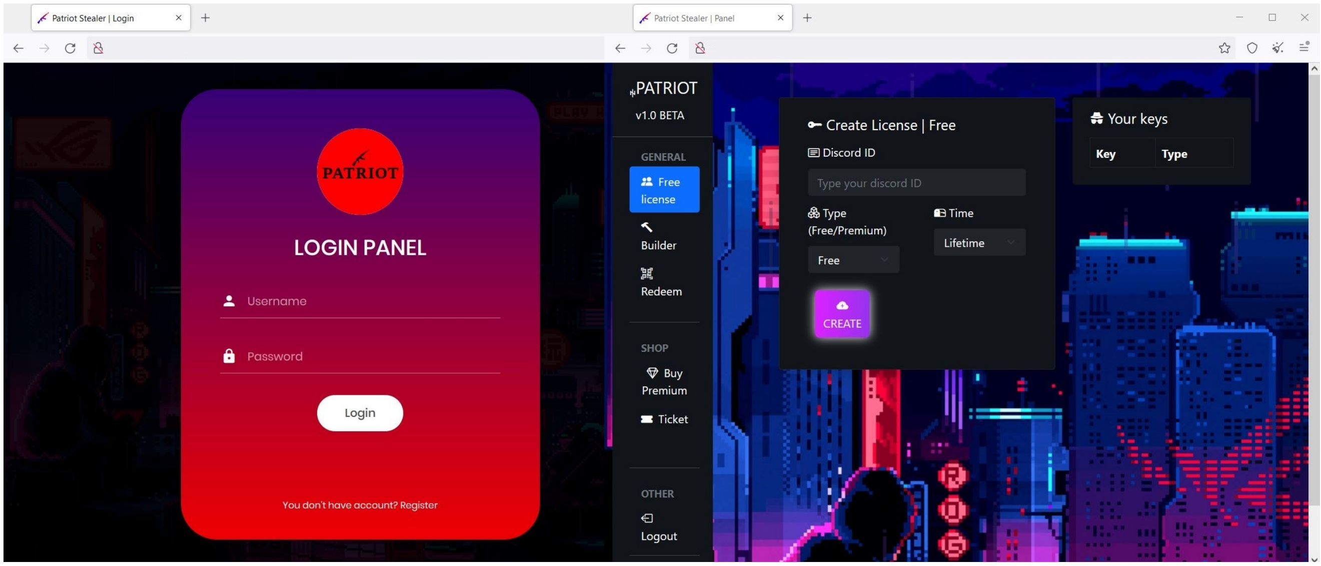
  hxxps://t.me/patriotstealer



Patriot Chat

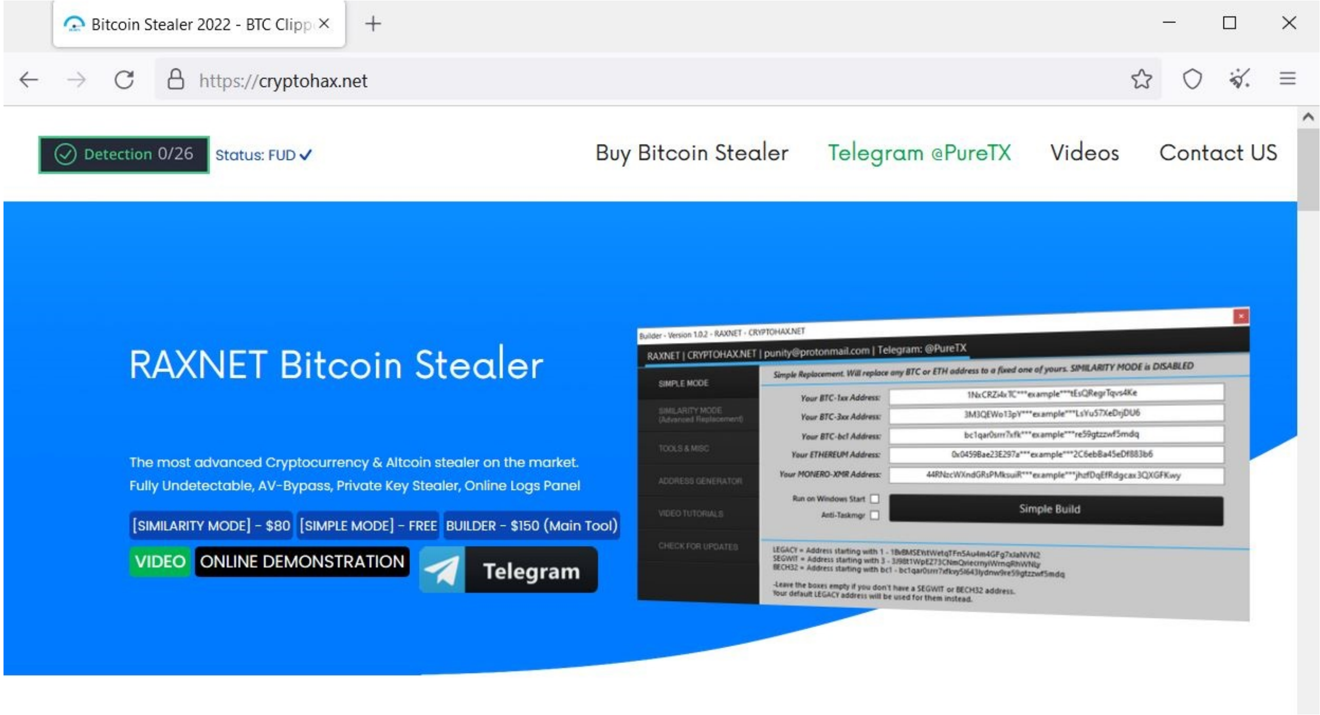
322 members, 11 online

Grupo oficial de la herramienta de PATRIOT STEALER



RAXNET Bitcoin Stealer

Again, the trusty Shodan Dork http.html:"stealer" uncovered another new and unreported infostealer malware called "RAXNET Bitcoin Stealer" that targets cryptocurrency users by replacing destination wallet addresses with the cybercriminal's own wallet addresses. The main features of this Malware-as-a-Service (MaaS) allegedly includes "Fully Undetectable, AV-bypass, Private Key Stealer, Online Logs Panel" and has several pricing models from $80 to $150, including "similarity mode" and the "builder" of the malware. The MaaS operators also offer "spreading methods" for $75. Other notable services related to this MaaS were "resell rights", "full video tutorials", "24/7 support", and a "refund policy."



RAXNET Bitcoin Stealer

The most advanced Cryptocurrency & Altcoin stealer on the market.
Fully Undetectable, AV-Bypass, Private Key Stealer, Online Logs Panel

[SIMILARITY MODE] - $80 [SIMPLE MODE] - FREE BUILDER - $150 (Main Tool)

VIDEO
ONLINE DEMONSTRATION
Telegram
Builder - Version 1.0.2 - RAXNET - CRYPTOHAX.NET
RAXNET | CRYPTOHAX.NET | punity@protonmail.com | Telegram: @PureTX
SIMPLE MODE
SIMILARITY MODE (Advanced Replacement)
TOOLS & MISC
ADDRESS GENERATOR
VIDEO TUTORIALS
CHECK FOR UPDATES
Simple Build

Simple Replacement. Will replace any BTC or ETH address to a fixed one of yours. SIMILARITY MODE is DISABLED

Your BTC-1xx Address: 1NxCRZi4xTC***example***tEsQRegrTqvs4Ke
Your BTC-3xx Address: 3M3QEWo13pY***example***LsYu57XeDrjDU6
Your BTC-bc1 Address: bc1qar0srrr7xfk***example***re59gtzzwf5mdq
Your ETHEREUM Address: 0x0459Bae23E297a***example***2C6ebBa45eDf883b6
Your MONERO-XMR Address: 44RNzcWXndGRsPMksuiR***example***jhzfDqEfRdgcax3QXGFKwy

Run on Windows Start □
Anti-Taskmgr □

LEGACY = Address starting with 1 - 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2
SEGWIT = Address starting with 3 - 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy
BECH32 = Address starting with bc1 - bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq

-Leave the boxes empty if you don't have a SEGWIT or BECH32 address.
Your default LEGACY address will be used for them instead.

RAXNET Bitcoin Stealer

- Shodan Dork

  http.favicon.hash:-1236243965

- URLscan Query

  https://urlscan.io/result/c4f7f543-46f5-4051-b3cb-3699d4b99c5c/

- Domain

  cryptohax[.]net

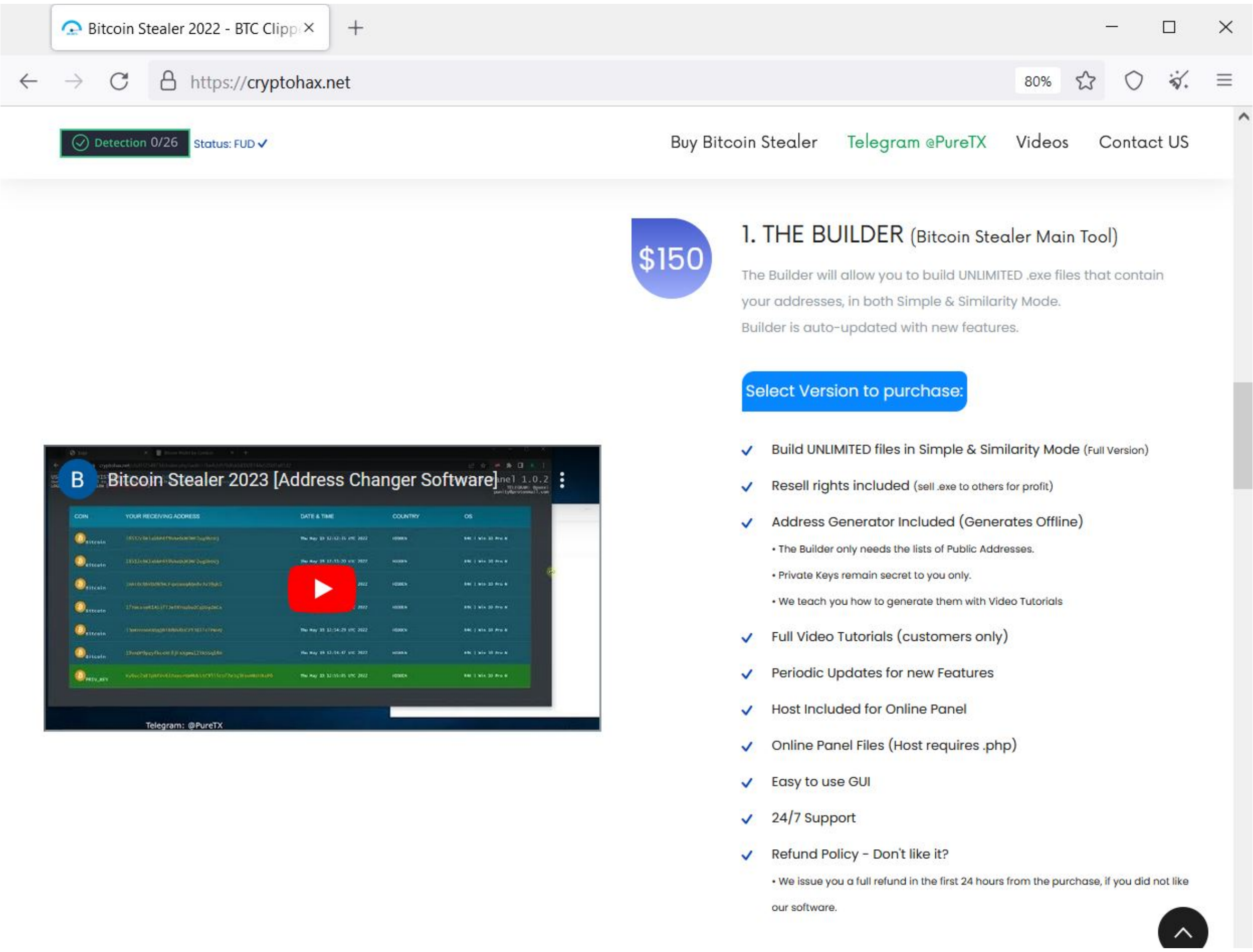
- Telegram

  @PureTX (hxxps://t.me/PureTX)

- E-mail

  punity@protonmail.com

- YouTube
  - https://www.youtube.com/@bitstorm101 (Joined 17 Nov 2022)
  - https://www.youtube.com/@punxi49 (Joined 21 Jun 2020)
  - https://www.youtube.com/watch?v=oNGIubac9sk (video tutorial)
  - https://www.youtube.com/watch?v=D9iT4VJev28 (video tutorial)



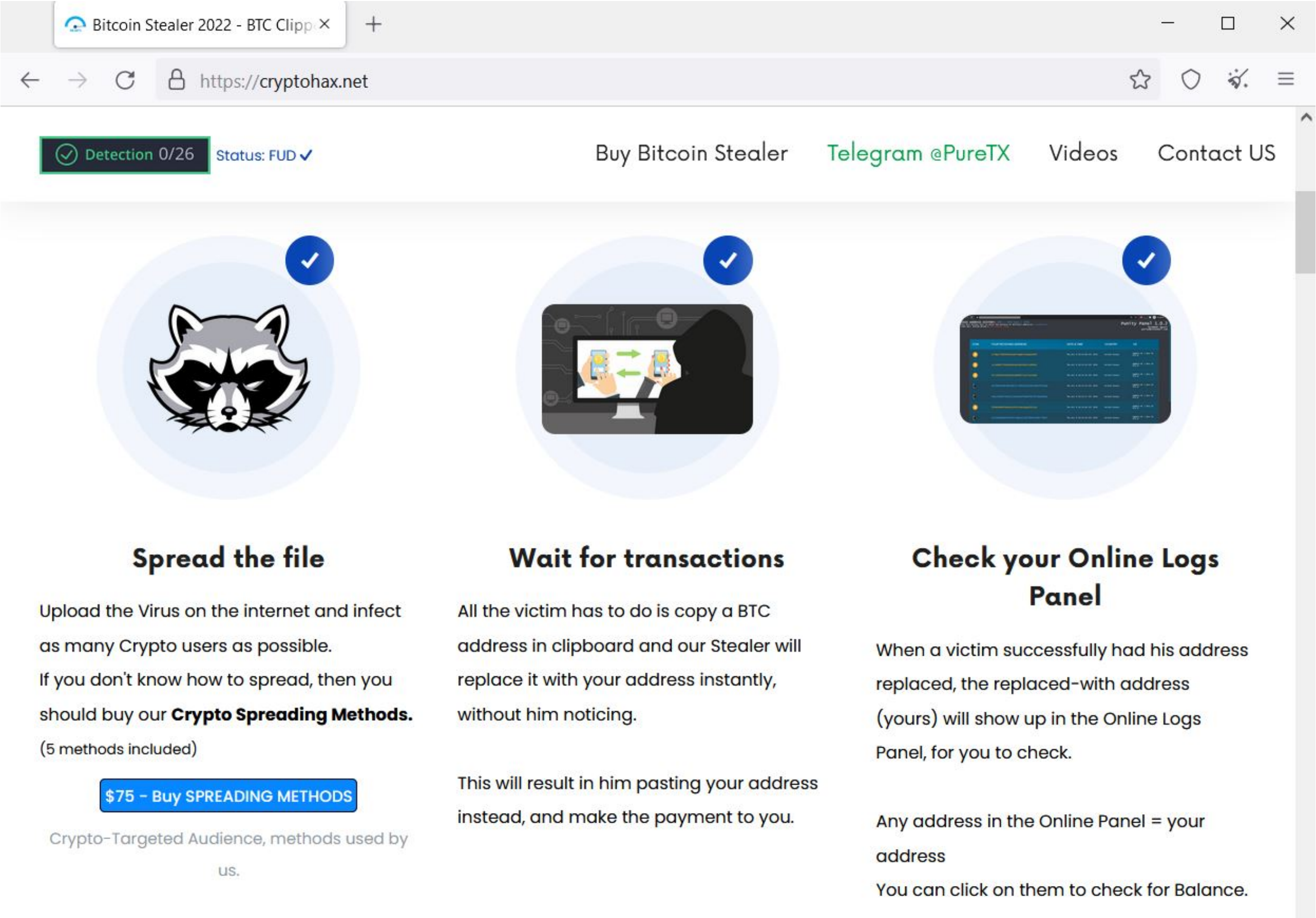
$150

1. THE BUILDER (Bitcoin Stealer Main Tool)

The Builder will allow you to build UNLIMITED .exe files that contain your addresses, in both Simple & Similarity Mode.
Builder is auto-updated with new features.

Select Version to purchase:

- ✓ Build UNLIMITED files in Simple & Similarity Mode (Full Version)
- ✓ Resell rights included (sell .exe to others for profit)
- ✓ Address Generator Included (Generates Offline)
  - The Builder only needs the lists of Public Addresses.
  - Private Keys remain secret to you only.
  - We teach you how to generate them with Video Tutorials
- ✓ Full Video Tutorials (customers only)
- ✓ Periodic Updates for new Features
- ✓ Host Included for Online Panel
- ✓ Online Panel Files (Host requires .php)
- ✓ Easy to use GUI
- ✓ 24/7 Support
- ✓ Refund Policy - Don't like it?
  - We issue you a full refund in the first 24 hours from the purchase, if you did not like our software.



Spread the file

Upload the Virus on the internet and infect as many Crypto users as possible.
If you don't know how to spread, then you should buy our **Crypto Spreading Methods.**
(5 methods included)

$75 - Buy SPREADING METHODS

Crypto-Targeted Audience, methods used by us.

Wait for transactions

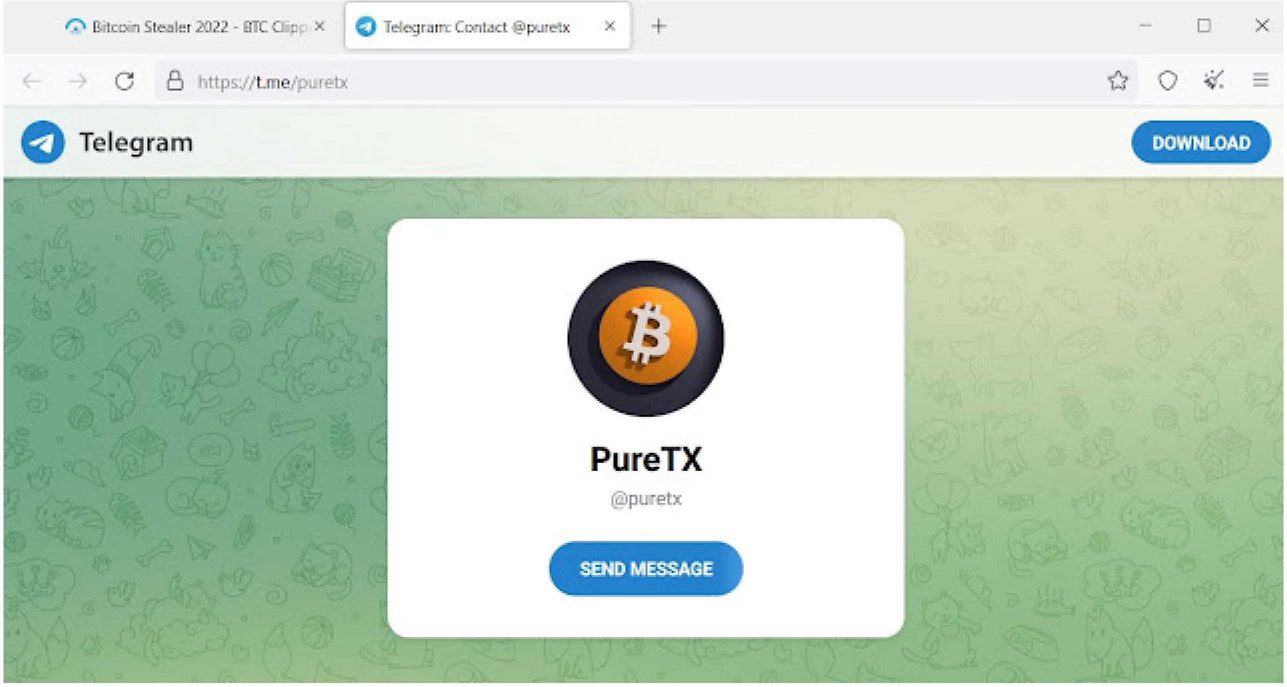
All the victim has to do is copy a BTC address in clipboard and our Stealer will replace it with your address instantly, without him noticing.

This will result in him pasting your address instead, and make the payment to you.

Check your Online Logs Panel

When a victim successfully had his address replaced, the replaced-with address (yours) will show up in the Online Logs Panel, for you to check.

Any address in the Online Panel = your address
You can click on them to check for Balance.



Analysis

The cybercriminal underground continues to evolve, and Malware-as-a-Service (MaaS) offerings have been a significant contributing factor for an increase in cybercrime. Aspiring cybercriminals no longer require the technical skills to perform such attacks, but as little as

$150 dollars to run a malware campaign with a multi-featured cybercrime tool allegedly with "24/7 support" from English- and Spanish-speaking malware developers as part of the as-a-Service business model.

This research also highlights that the infrastructure of cybercriminals often includes several common denominators, such as email addresses and Telegram channels to communicate with customers, websites and YouTube channels to advertise products, as well as cryptocurrency wallets to receive payments.

Stealing credentials on a wide scale can be useful for a plethora of attacks. The threat actor who actually stole the credentials is also not always going to be the one who leverages them. This is due to the growing popularity of selling stolen credentials on cybercrime forums and marketplaces.

Lessons from the Conti Leaks

Overview of Russian GRU and SVR Cyberespionage Campaigns 1H 2022

Gamer Cheater Hacker Spy