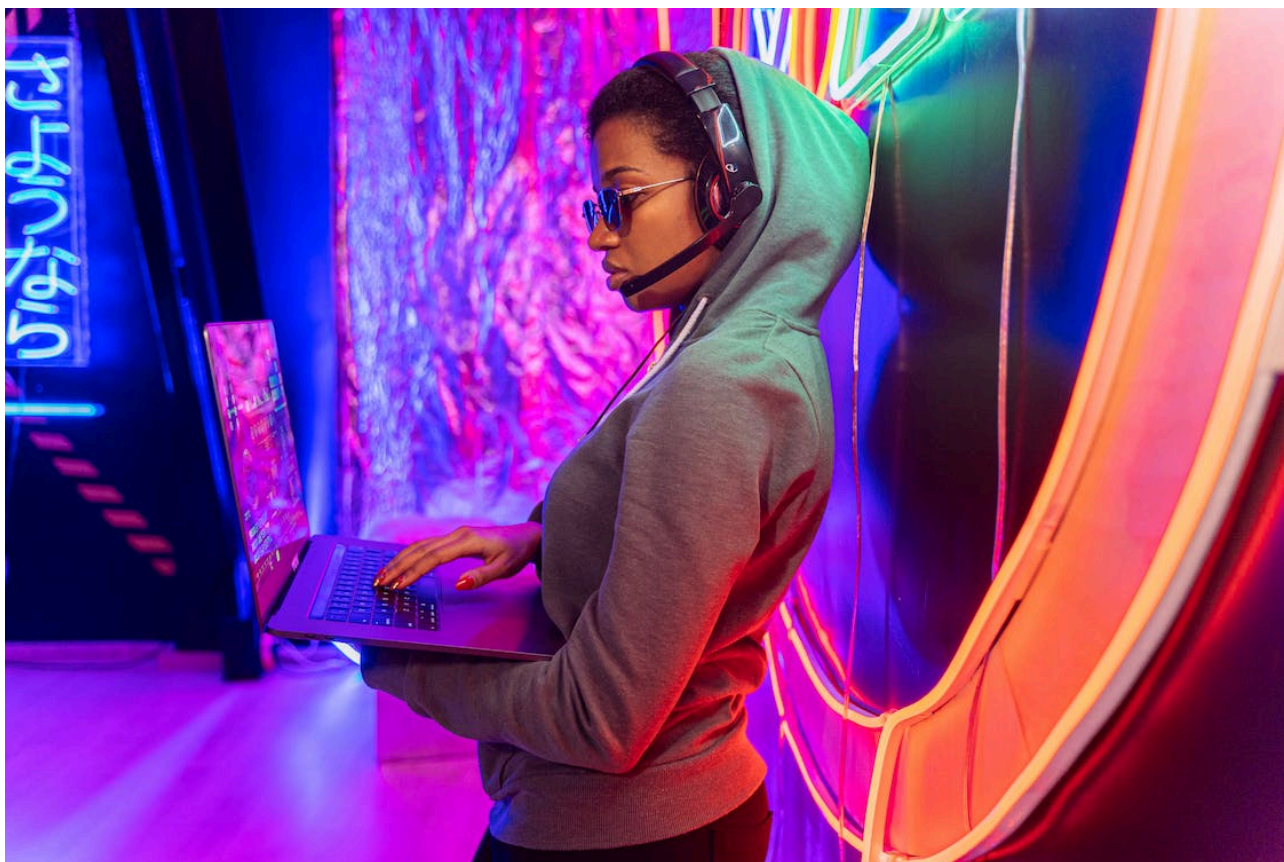


Detecting and Fingerprinting Infostealer Malware-as-a-Service platforms

By BushidoToken

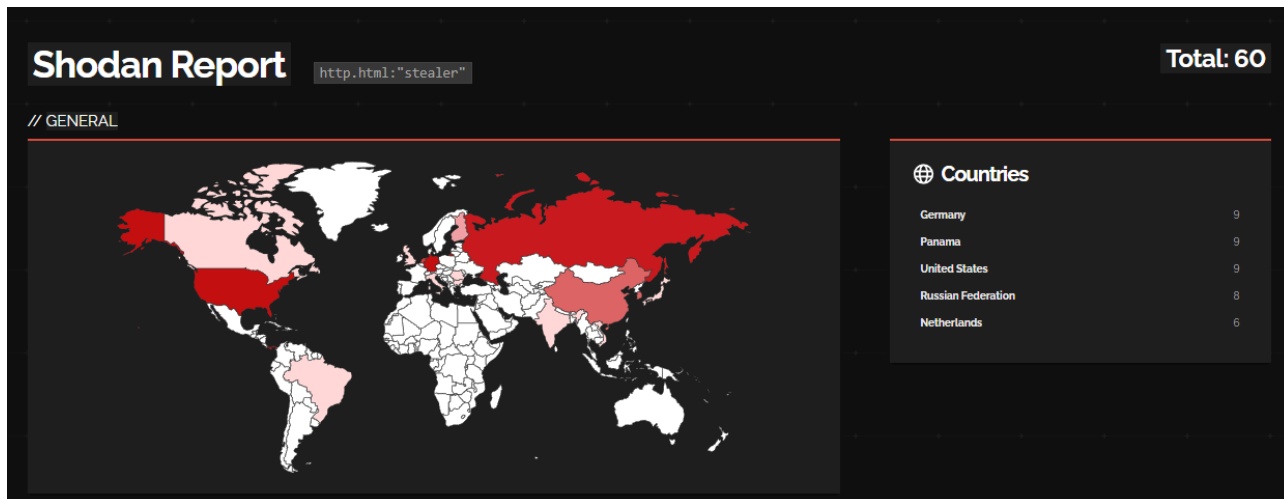
Published: 2022-11-26 · Archived: 2026-04-05 15:14:28 UTC



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.

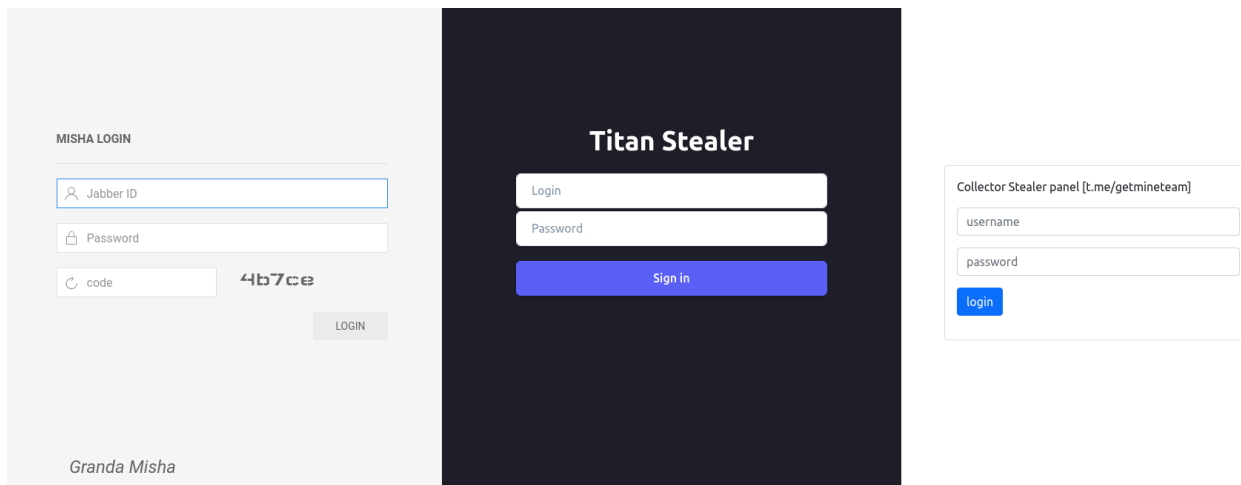
But we can also use Shodan for tracking the adversaries. Through the process of fingerprinting - that is to identify unique attributes of IPs on the internet - we can find command and control (C2) servers and login panels belonging to cybercriminals online. Through this process, I was able to identify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



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.



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

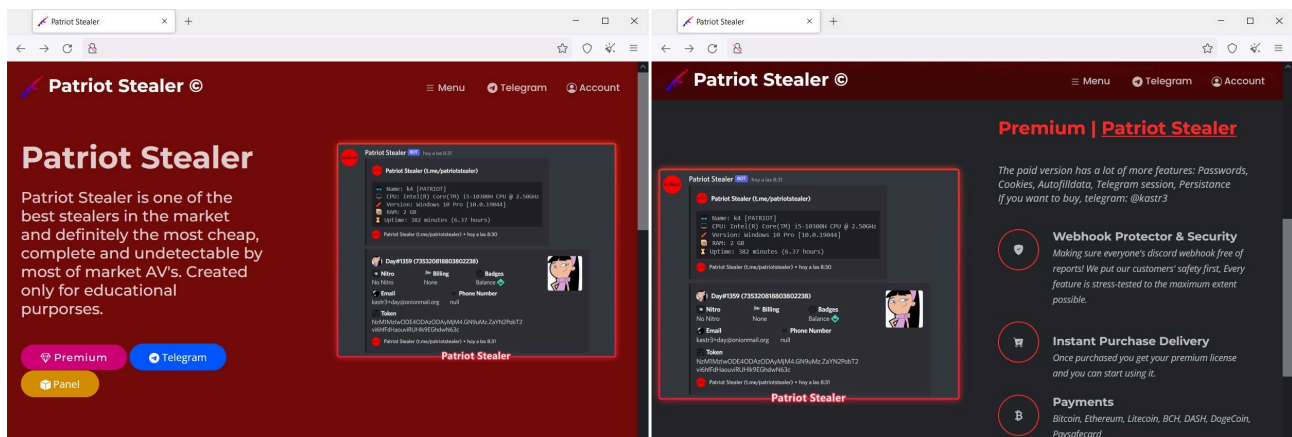
- Shodan Dork
 - `http.html:"Collector Stealer"`
 - `http.html:"getmineteam"`
- URLscan Query
 - `https://urlscan.io/search/#task.tags:%22collector%22`

Titan Stealer

- Shodan Dork
 - `http.html:"Titan Stealer"`
- URLscan Query
 - `https://urlscan.io/result/daca0fcd-bbc9-48c8-810d-89fee466b639`

Patriot Stealer

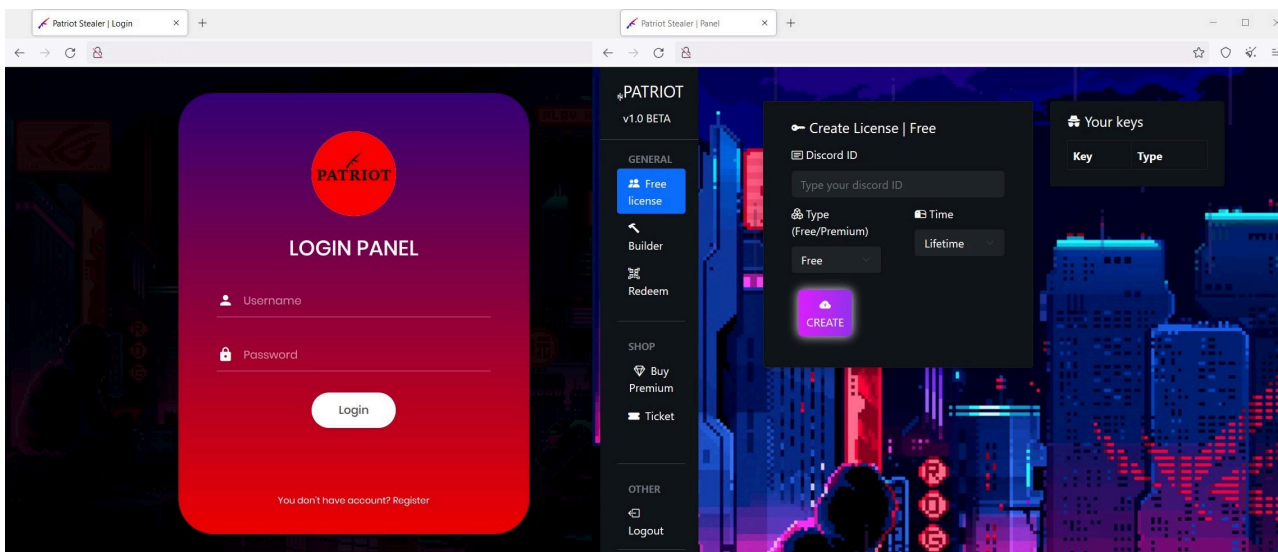
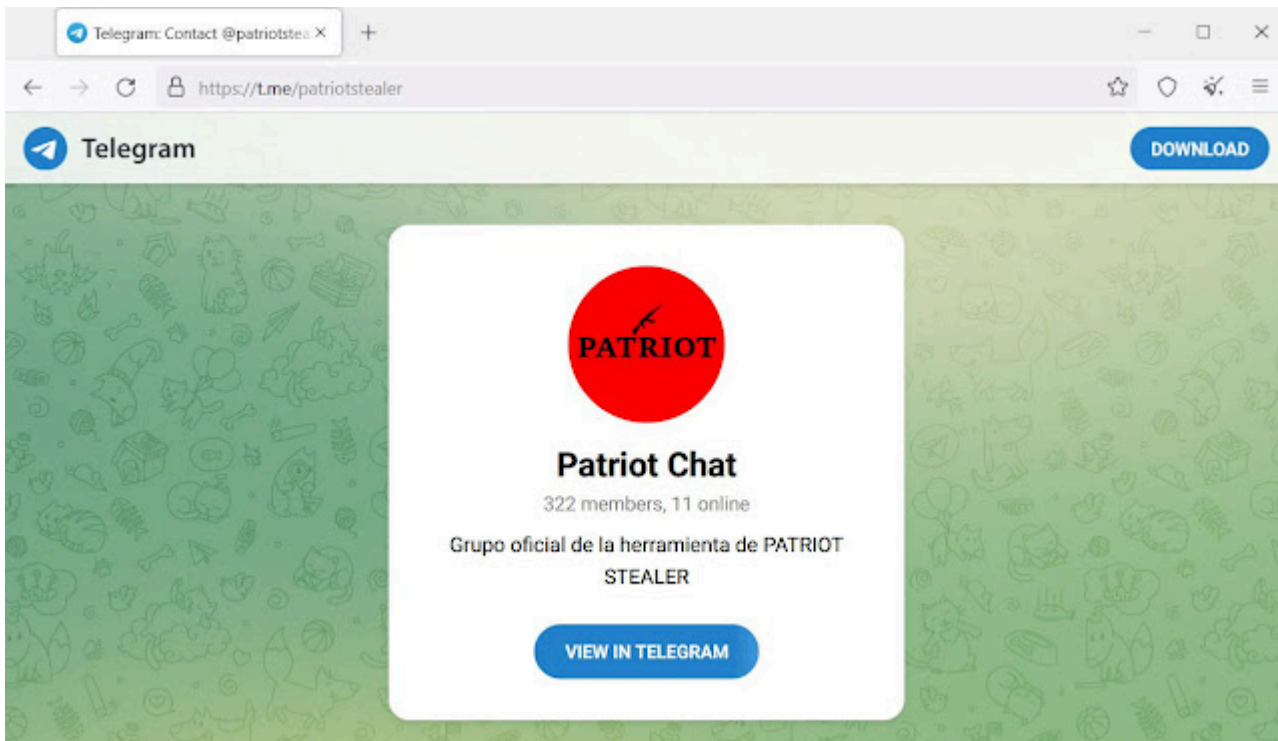
The same Shodan Dork `http.html:"stealer"` also revealed an unreported and new Malware-as-a-Service (MaaS) platform marketing itself as "Patriot Stealer". The paid version of the infostealer malware is reportedly capable of stealing "passwords, cookies, Autofilldata, Telegram session, Persistence" and 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.



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.

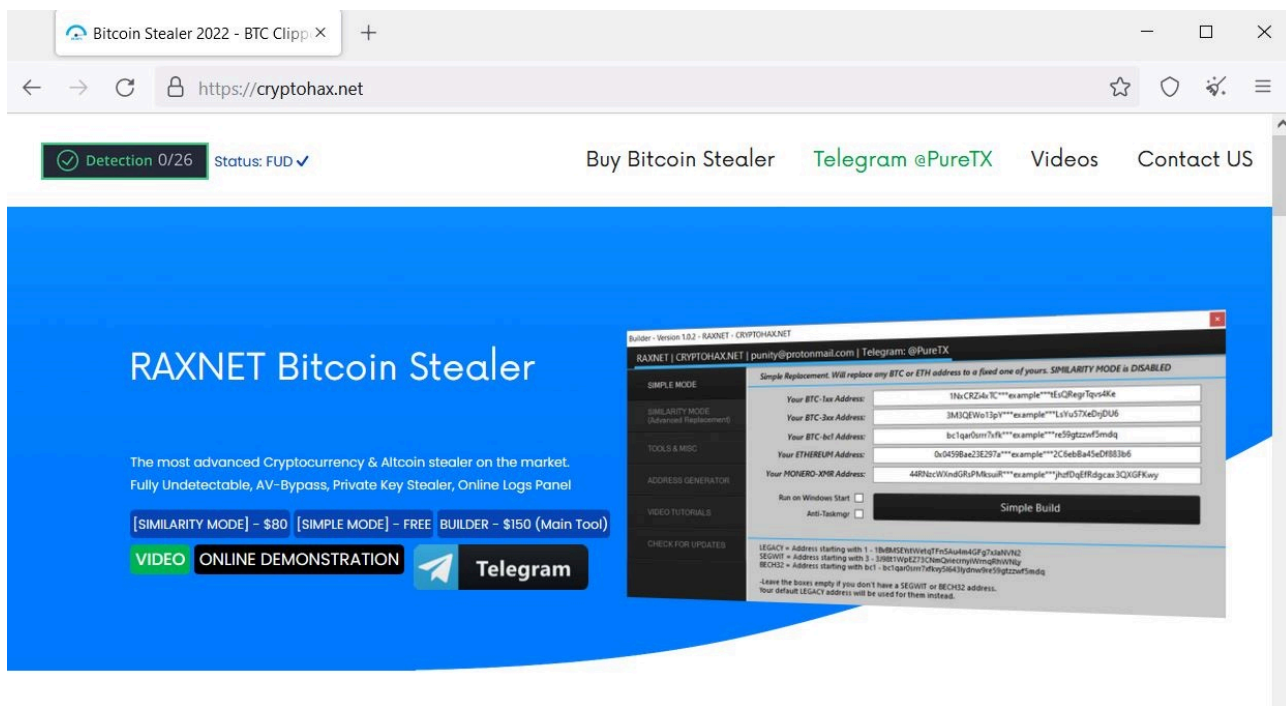
Patriot Stealer

- 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`



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

- Shodan Dork
 - [http.favicon.hash:-1236243965](http://favicon.hash:-1236243965)
- URLscan Query
 - <https://urlscan.io/result/c4f7f543-46f5-4051-b3cb-3699d4b99c5c/>
- Domain
 - [cryptohax\[.\]net](https://cryptohax[.]net)
- Telegram
 - [@PureTX \(hxxps://t.me/PureTX\)](https://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)



✔ Detection 0/26 Status: FUD ✔

Buy Bitcoin Stealer Telegram @PureTX Videos Contact US

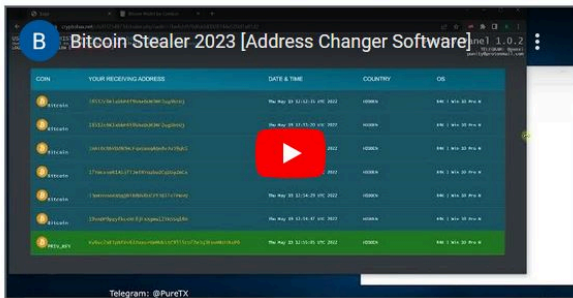
\$150

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.



The screenshot shows the website <https://cryptohax.net>. At the top, there is a navigation bar with links for "Buy Bitcoin Stealer", "Telegram @PureTX", "Videos", and "Contact US". A status bar indicates "Detection 0/26" and "Status: FUD". The main content is divided into three columns, each with a circular icon and a checkmark:

- Spread the file**: Includes instructions to upload the virus and a button for "\$75 - Buy SPREADING METHODS".
- Wait for transactions**: Explains that the stealer will replace a victim's BTC address with the user's.
- Check your Online Logs Panel**: Describes how to check for replaced addresses in the online logs panel.

The screenshot shows a Telegram contact card for the user **PureTX** (@puretx). The card features a Bitcoin logo as a profile picture and a blue "SEND MESSAGE" button. A "DOWNLOAD" button is visible in the top right corner of the contact area.

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.

Source: <https://blog.bushidotoken.net/2022/11/detecting-and-fingerprinting.html>