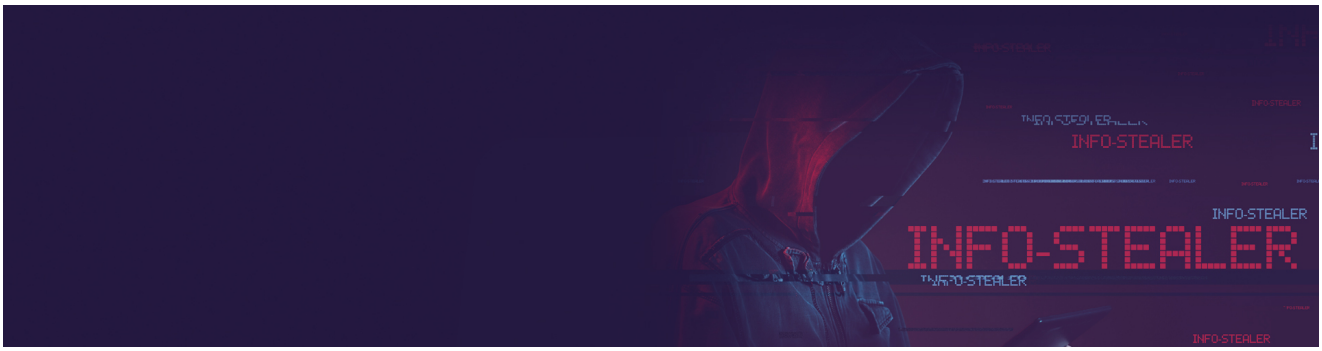
Uncovering the “Easy Stealer” Infostealer

bridewell.com/insights/blogs/detail/uncovering-the-easy-stealer-infostealer



The information stealer is being sold on the underground, advertising a variety of information stealer capabilities, such as the ability to target crypto wallets and passwords. We’ve conducted an analysis of this stealer and are publishing initial findings to share with the wider security community.

The information stealer appears to be linked with a number of recent infection chains including possible connections with Wasabi Seed, used by Proofpoint’s TA866 in a recent Screentime campaign. As we continue to analyse the malware and threat actors behind it, we will update this blog with more information.

Figure 1. EasyStealer advert

Overview

On July 23rd, the first advertisement for “Easy Stealer” appeared on the Russian criminal forum, XSS.is. The post was created by the alias “EasyStealer”, claiming to be “one of the best products on the market, supported by an experienced team”. The advertisement details a “User-friendly panel”, custom File Grabber, and Dynamic Loader.

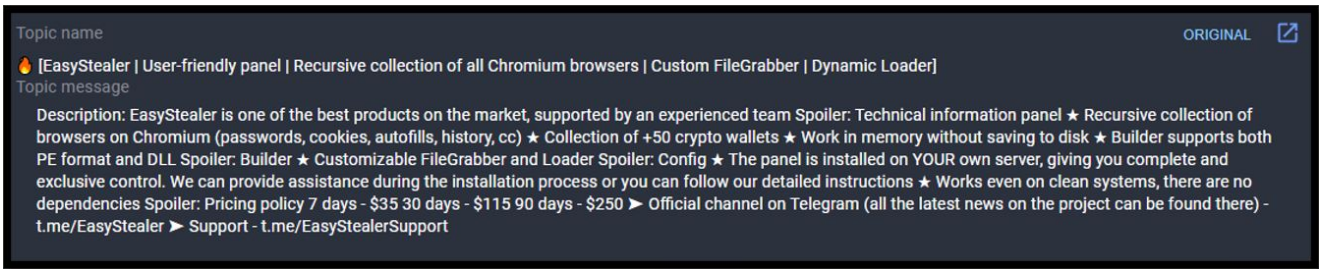


Figure 2. EasyStealer marketplace description (Group-IB threat intelligence platform)

Key features of the information stealer include:

- Technical Information Panel
- Recursive collection of browsers on Chromium (passwords, cookies, autofill history, CC)
- Collection of +50 crypto wallets
- Working in memory
- Supports PE and DLL formats
- Written in Golang

The panel for the stealer is installed on the buyer's own infrastructure, allowing for exclusive control, whilst also providing setup support. The stated pricing models are:

- $35 for 7 days,
- $115 for 30 days
- $250 for 90 days

The developers also advise two Telegram Channels, one for latest news and the other for support:

- t.me/EasyStealer (currently inactive at the time of writing this report)
- t.me/EasyStealerSupport

EasyStealer Timeline

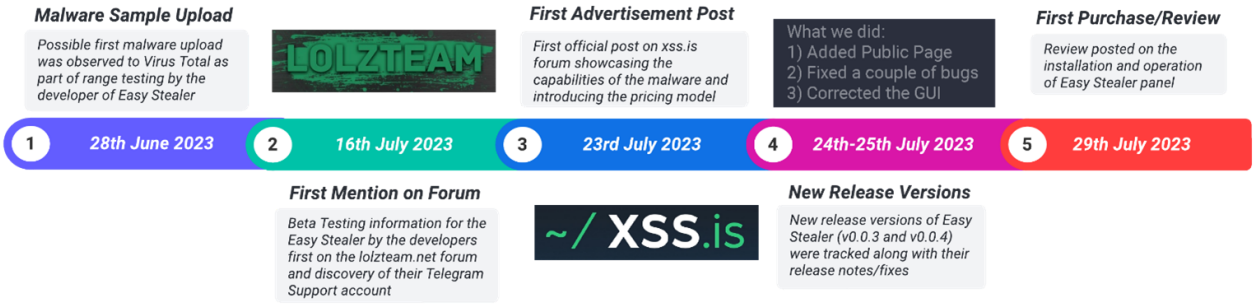


Figure 3. Easy Stealer development timeline

Based on samples submitted to VirusTotal, **it can be observed** that the first possible samples created by the developer, were uploaded on 16th June 2023. This was most likely for the purpose of range testing. The first mention of Easy Stealer was on the “Lolzteam” forum requesting beta testers by the developers on the 16th of July 2023. In the subsequent days following the first advertised post for Easy Stealer on the 23rd of July, the developers pushed out new versions of the stealer, v0.0.3 and v0.0.4.

On the 29th of July the first review of Easy Stealer was posted on the installation and operation of the Easy Stealer Panel.

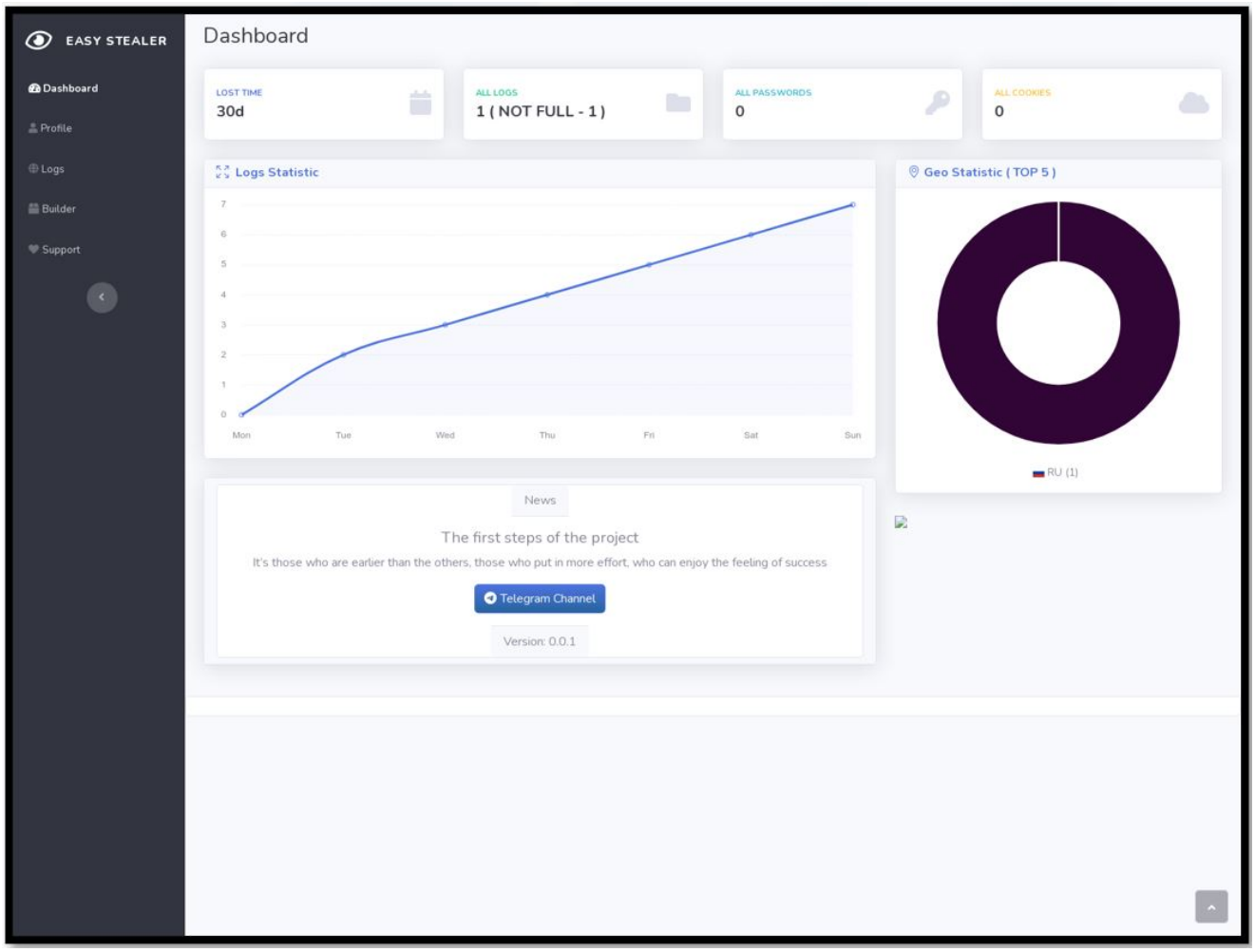


Figure 4. Easy Stealer Dashboard Panel

Infrastructure Discovery & Analysis

We utilised open-source tooling to identify an initial IP address belonging to Easy Stealer: **91.103.252[.]210.** This IP address is hosted on Shetler LLC and the Dashboard panel can be accessed on port 3000.

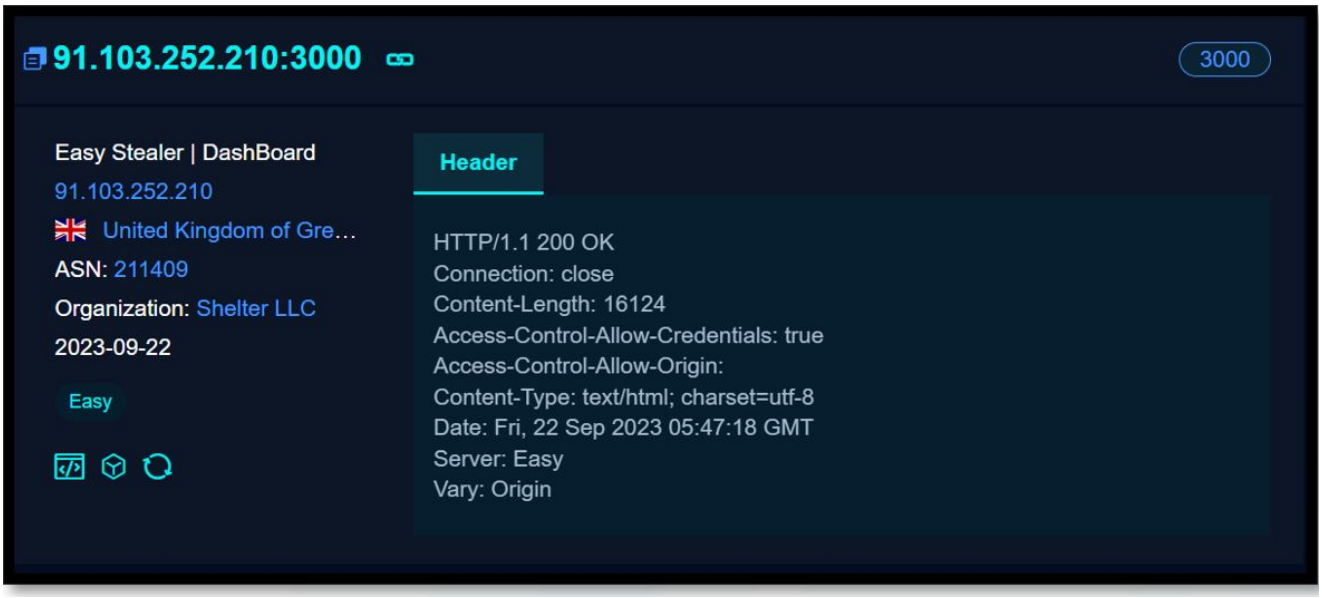


Figure 5. Easy Stealer FOFA search result

Interestingly, the developer has failed to place any access control mechanisms on the server making it readily accessible to anyone who stumbles across it. We were able to analyse the server to identify that it's currently running a v0.0.1 build, which is known to be behind recent versions. When accessing the logs tab, we observed that there is only a single IP address listed: 194.154.78[.]251.

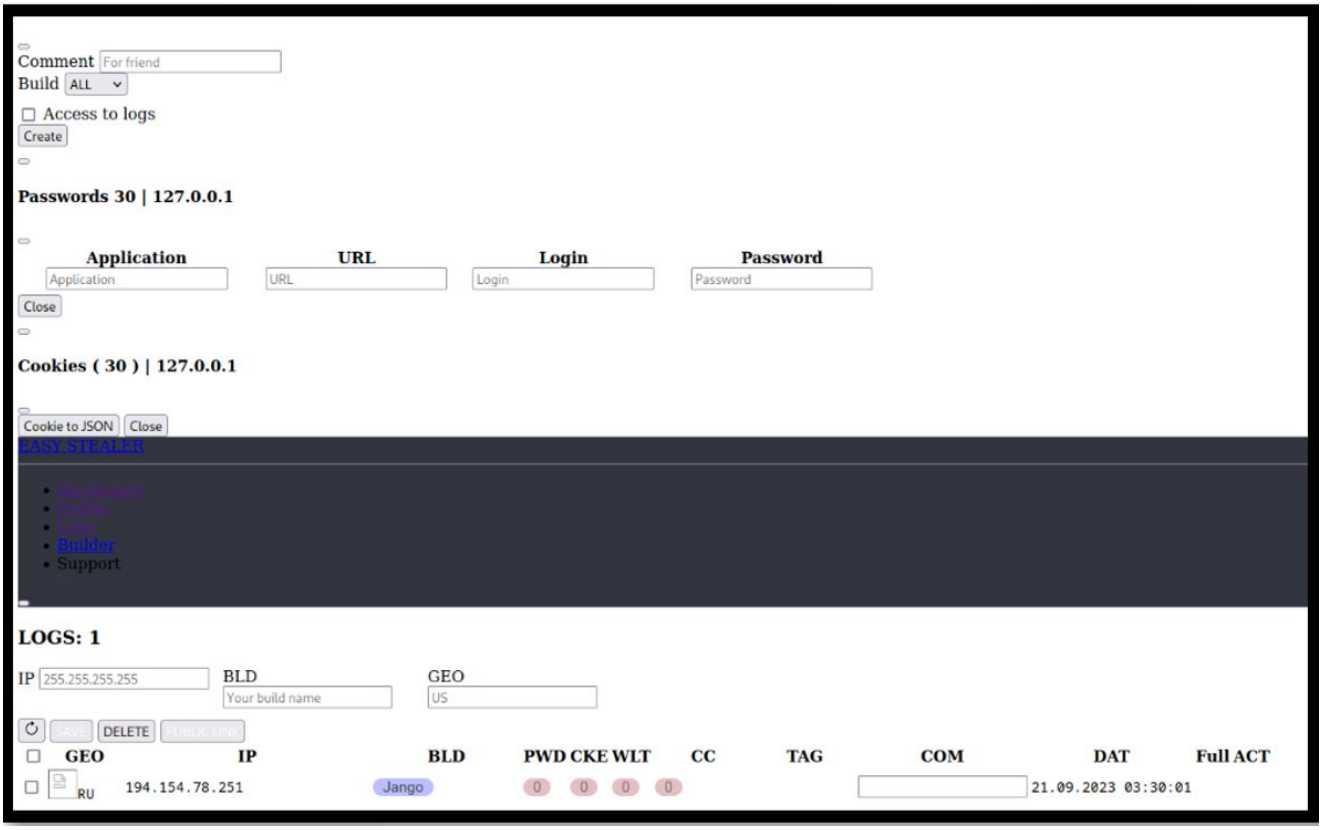
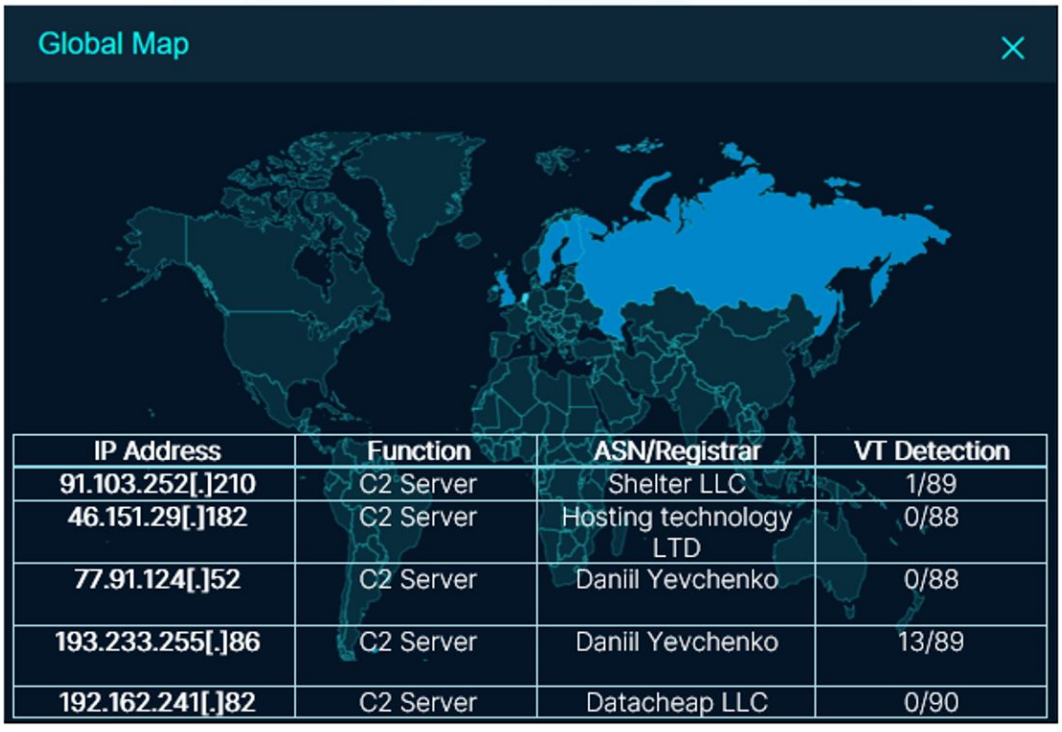


Figure 6. Easy Stealer logs

This information helps make some initial assumptions; that this server is used for testing and development, and that the IP address could be an indication as to the location of the developer. When analysing the IP address, it can be seen that it places it in Moscow, Russia and is assigned to a Telecommunications company called “PJSC Vimplecom”.

Figure 7. Possible Easy Stealer developer IP address

Using tools such as FOFA, we were able to fingerprint and identify an additional five servers linked to Easy Stealer. Based on information provided by Virus Total, there is currently a very low/ no detection at all for the servers hosting Easy Stealer likely due to its early stage of development and lack of known campaigns that are associated with it. IP address 193.233.255[.]86 has higher detections due to historical association with other information stealer campaigns.



IP Address	Function	ASN/Registrar	VT Detection
91.103.252[.]210	C2 Server	Shelter LLC	1/89
46.151.29[.]182	C2 Server	Hosting technology LTD	0/88
77.91.124[.]52	C2 Server	Daniil Yevchenko	0/88
193.233.255[.]86	C2 Server	Daniil Yevchenko	13/89
192.162.241[.]82	C2 Server	Datacheap LLC	0/90

Figure 8. Easy Stealer C2 global distribution

A number of the C2 servers are either historical or still active but more secure. IP address 46.151.29[.]182 is completely clean in VirusTotal but has two samples currently communicating with it.

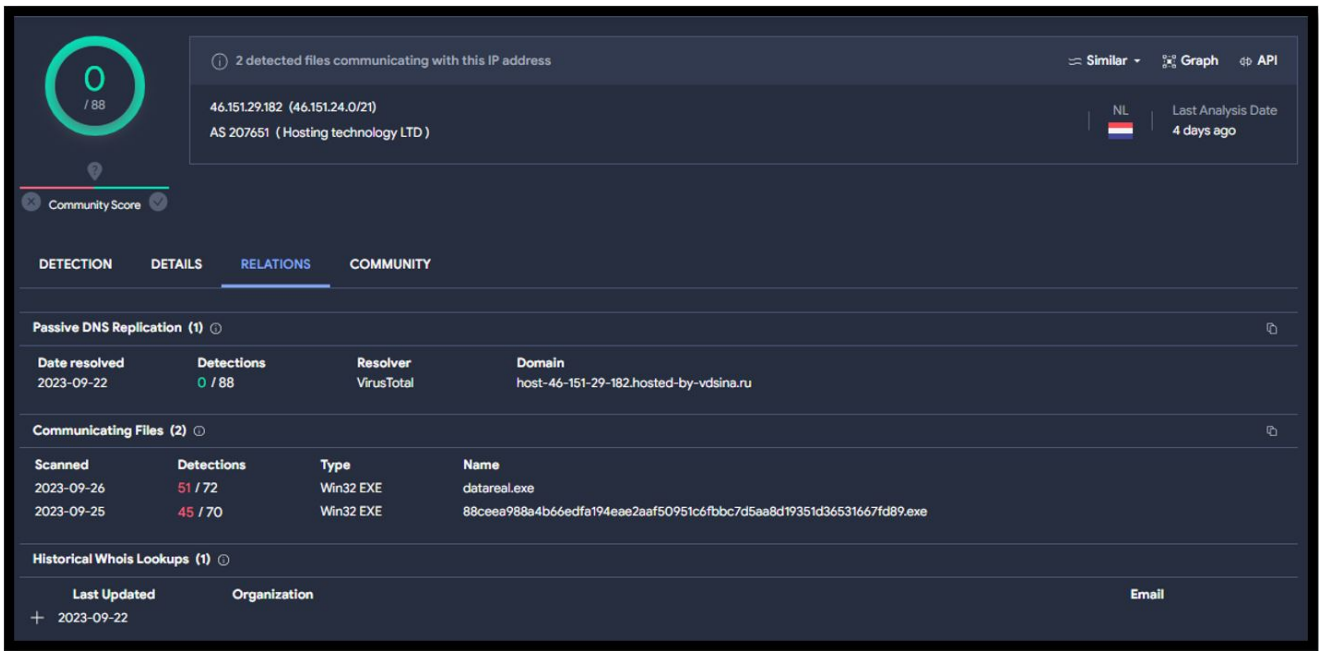


Figure 9. Easy Stealer C2 Virus Total Result

Initial Findings

We have also uncovered a number of interesting observations associated with the C2 server 46.151.29[.]182 that will be subject to ongoing analysis and will be included in this report once completed. However, our initial findings based on the information known so far arepublished in this report. We welcome collaboration and input from the wider security community, please get in touch at email address

Based on our initial findings, we can observe a possible correlation with Proofpoint's TA866 and their campaign called "Screentime". In this, the Threat Actor uses its "custom toolset including WasabiSeed and Screenshotter, TA866 analyses victim activity via screenshots before installing a bot and stealer." In this campaign, WasabiSeed is utilised to drop a number of files, ending with the Rhadamanthys Information Stealer.

https://www.proofpoint.com/uk/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

Based on the infection chain identified by Bridewell, we have identified a possible Wasabi Seed sample dropping Easy Stealer. A number of attributes from our findings link to this Proofpoint report which we will continue to correlate. We have observed the use of Wasabi Seed, JavaScript files and similar persistence mechanisms such as the use of .lnk files. However, we have also observed the use of PowerShell to drop Easy Stealer.

When understanding the Easy Stealer infection chain, we came across open-source reporting by an independent security researcher called ULTRAFRAUD detailing a malware sample payload directory and C2 IP address. We currently believe that this sample is Wasabi

Seed and is the file used to drop Easy Stealer.

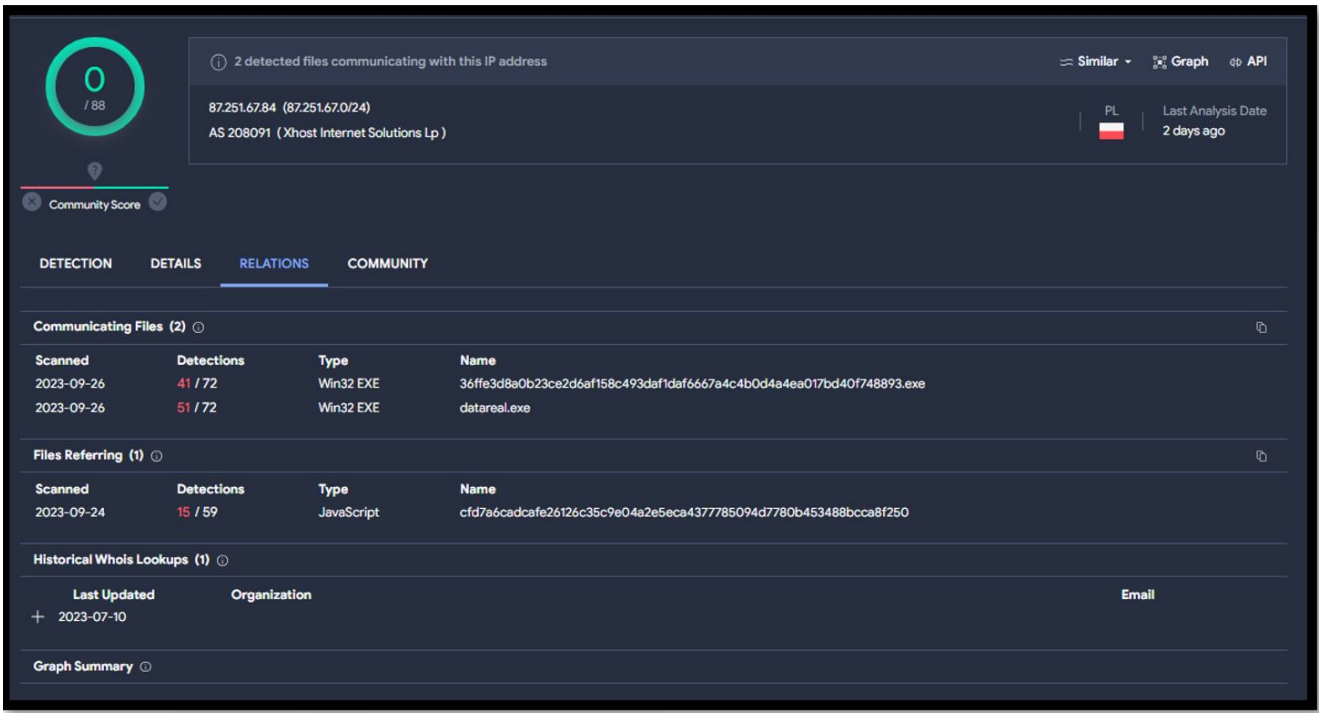


Figure 10. Easy Stealer Virus Total Result

*The above image shows the payload/C2 IP address **87.251.67[.]84**, associated with the possible Wasabi Seed sample.*

The connection between this finding and Easy Stealer is shown in the following Virus Total graph which can be found here: https://www.virustotal.com/graph/gc94fed32595f4b72afc706de02913667c14812e7ca8146299522e993c80dc7ac

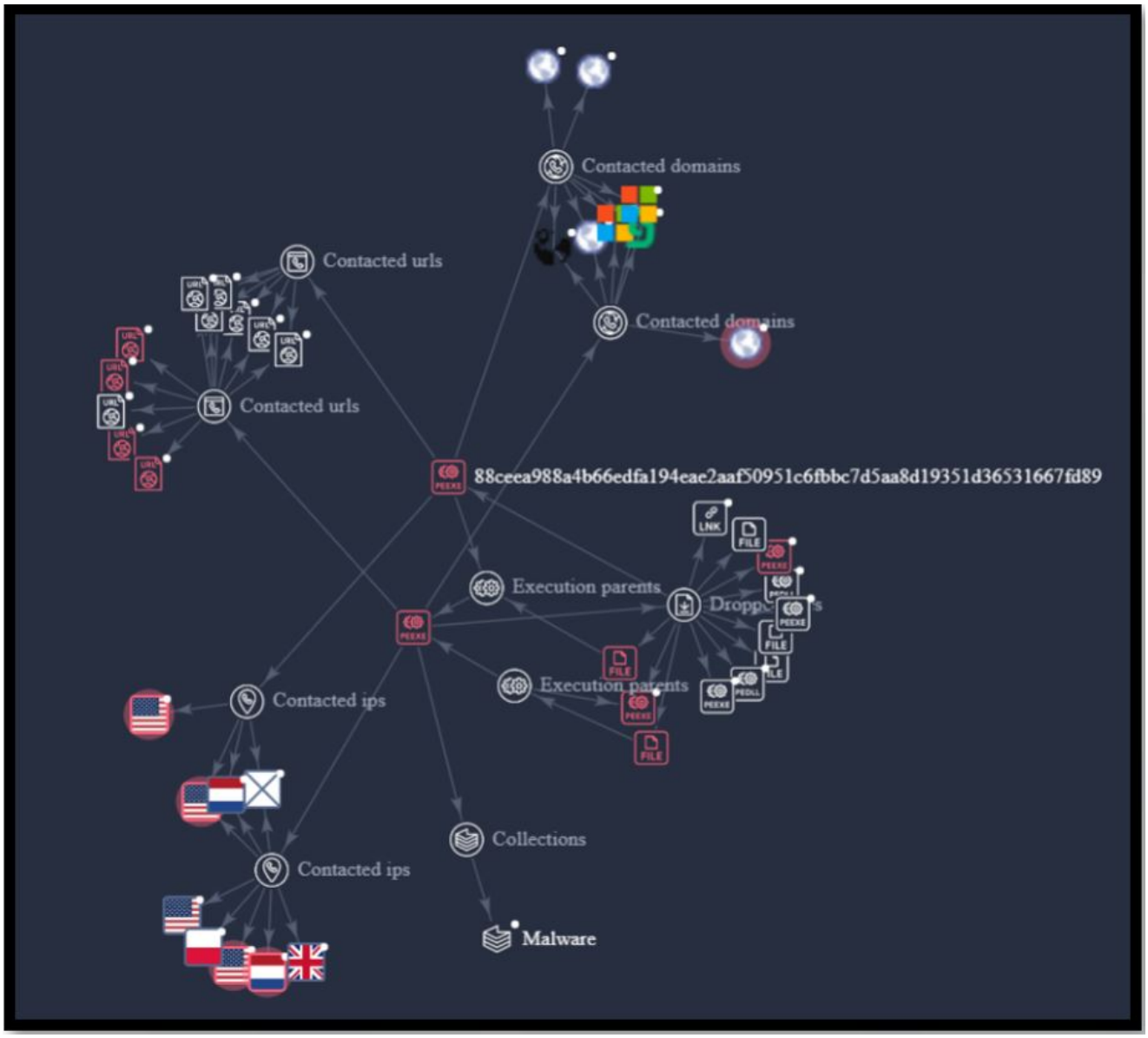


Figure 11. Virus Total Graph of Easy Stealer Relationships

As we continue to understand the infection chain, we will update this blog with more findings.

Comparison of Easy Stealer with other of existing Information Stealers

The sample associated with the command and control IP address **46.151.29[.]182** has the following file hash:
88ceea988a4b66edfa194eae2aaf50951c6fbbc7d5aa8d19351d36531667fd89 which was used for initial analysis. The following characteristics were utilised to observe any form of relevance with other malware:

- **Code Block similarity:**There were no malware samples found sharing code structure with this particular malware sample.

- **SSDeep Hash:** SSDeep hashes are a type of fuzzing hashes which are useful for comparing if two or more files are similar. There were no malware samples having the same SSDeep hash as this sample.
- **VT Feature Hash:**This is a type of internal hash that Virus Total leverages to determine file similarities. There were no file samples found sharing the same VT feature hash to this sample.
- **Imphash:**Also known as import hash is the hash calculated based on the import functions invoked by the malware and their corresponding sequence. A total of 13 files were identified which shared the import hash with this sample.

The number of files sharing this Imphash can still be considered to be low in number and suggests uniqueness of the malware sample. This is because there exists a large variety of malware in the wild whereas the number of import functions are limited. Hence, it is plausible that some malware samples use the same import functions in the same order. These files were labelled as Redline, Zusy, Stealc, DCrat, generic trojan, ransomware and other unknowns.

Based on the above observations, it can be stated with moderate-high confidence that Easy Stealer is new and unique when compared to other information stealers and not a variant from one of the existing malware families.

Additionally, basic malware analysis assisted in validating that the malware sample analysed is in fact Easy Stealer. This was based on over hundred references made to the string “easy” which can be attributed to Easy Stealer. Some of the specific strings are mentioned in the table below.

Key References to Easy Stealer Based on Malware Analysis

easy/user	easy/reqursion.Start	easy/network.HTTP
easy/decrypt	easy/decrypt.GrabFromBrowser	easy/wallets.Grab.func2
easy/discord	easy/shell.Liquidation	easy/zip.addFiles
easy/network	easy/decrypt.MasterKey	easy/user.SystemInfo
easy/wallets	easy/network.SaveConfig	easy/reqursion/main.go
easy/telegram	easy/registry.GetRegistryKey	easy/geoposition

Based on our analysis of the first submitted sample of Easy Stealer, some of the potential crypto wallets that the malware attempts to search for were found. These included but are not limited to **Zcash, Armory, Yandex, Electrum, Ethereum, Exodus** and **Jaxx**. It should

be noted that we have not yet conducted an exhaustive malware analysis and there are likely to be additional capabilities or features that the infostealer may have which have gone unnoticed and unadvertised.

Files Hashes	Submission
88ceea988a4b66edfa194eae2aaf50951c6fbbc7d5aa8d19351d36531667fd89	2023-09-22 (CH)
25a71650ac89b1b9bb43a8b879243688df40b95ab5a47b6676d818fe471695c3	2023-06-16 (US)
2e87653bba901fc4b3f75d17fc744815147443598d8166ffbb03a678003814f2	2023-06-28 (RU)
db97ccc408b5c9df4c87dc7dbaacd1a6a5eaf771997ef815e4dbfd7a4ec58222	2023-06-29 (Unknown)
e4999b9645ea89a3e3142e6579b449d9caaec0a3a70784d24141cc10c0c48416	2023-06-29 (Unknown)
9169f5a0e68ca42366f85d40a7bd9cd46430723e05920cd8db11602dfb4b173e	2023-07-07 (US)
d0e3e7a543911861799f7c50278115c73cfa5cdac306de2631aababe1bdaa2a2	2023-07-23 (CA)
e8d9fb1649babc353746e3e5c3b2773b572e7e00662e64d22b762ce93ee1a9c2	2023-07-23 (CA)

To conclude, given the ease of using the panel due to its user friendly design and the affordable price range combined with similar capabilities of this malware when compared with other information stealers, the Easy Stealer is likely to see an increase in distribution among various cyber criminals as it continues through active development.