


# ObserverStealer: Unmasking the New Contender in Cyber Crime

 [medium.com/@cyberhust1er/observerstealer-unmasking-the-new-contender-in-cyber-crime-6e54a40d801d](https://medium.com/@cyberhust1er/observerstealer-unmasking-the-new-contender-in-cyber-crime-6e54a40d801d)

Taisiia G.

June 23, 2023



Taisiia G.

--

Since I have a day off today, instead of re-watching the first season of Vinland Saga on Netflix, I thought, why not browse the forums and try to find some juicy stuff instead? So, here we go. Since my blog is rather a reflection of my thinking process, it is very informal in its nature. I hope you do not mind and still enjoy reading it. I decided to dedicate my second article to the stealer advertised on numerous forums since the mid of May 2023, dubbed as ObserverStealer. Before writing about it, I verified that no vendor has written about it, which always makes the investigation more interesting. You never know what you can find.

I began by revisiting the forum where I first saw the advertisement for this stealer over a month ago (see Figure 1).

### Observer Stealer advertisement on one of the forums

According to the announcement, ObserverStealer is a very “convenient stealer” that can change the build configuration without requiring a replacement. Users can add extensions, browsers, and files they wish to collect. Additionally, the tool includes a loader and supports notifications through the Telegram bot. Some of the technical features mentioned are as follows:

- The program’s weight is between 300–330 KB.
- It is written in C++ with a backend in NodeJS.
- It can be used on Windows 8.1 to 11.

It was also mentioned that program cannot be used in countries within the Commonwealth of Independent States (CIS), such as Belarus, Russia, Ukraine, etc. The price of the stealer \$150/month.

Currently, ObserverStealer is in the BETA development stage. As is customary with this type of malware, the developers are offering temporary free access to users in exchange for, hopefully, good feedback. Although some reviews have been positive, others have noted technical issues that the developers should address before selling access to the stealer.

When scrolling down the comment line, I came across a statement that I found quite amusing (see Figure 2). The comment was made by a user named WhiteSnake, who has been promoting another infostealer dubbed WhiteSnake on the forum since February 2023. WhiteSnake suggested that other users should launch a DDoS attack on the C2 panels of ObserverStealer in retaliation for their marketing tactics of convincing users to switch to ObserverStealer from other stealers (see Figure 3–4). The representatives of the other two stealer groups, Lumma and Eternity, supported this idea. This makes me wonder again what connection various stealers have with each other.

WhiteSnake reaction on ObserverStealer post

. ObserverStealer promotion strategy

. DDoS script made by WhiteSnake

Once I finish investigating a forum, my next step is to search for C2 panels. There are multiple ways to find the C2 panels. One of the ways that I often employ when trying to identify the C2 panels is by checking the video recordings provided by the seller in which they demonstrate the use of the product. This way, when reviewing the recording, I could spot IP — **77.73.134[.]51** (port **1337**), which I will consider as one of the indicators to investigate later. Since WhiteSnake has provided me with another IP address — **5.42.64[.]41** (port **1234**), by mentioning it in a DDoS script, I think I have enough information to proceed to the next step — pivoting. Several great sources can be used to do that. Among my favourites are Shodan, Censys, VirusTotal, and URLScan. Since ObserverStealer is not the new-new stealer of a few days old, I will use URLScan since someone likely has already scanned the mentioned IP address.

I started by scanning the IP address **77.73.134[.]51**, but it didn't provide any recent results that could connect it to ObserverStealer. Even checking with Shodan and Censys didn't yield any results, so, it is likely, the IP address is no longer in use. However, I did come across that revealed the connection between **77.73.134[.]51** and our next IP address, **5.42.64[.]41**, by pivoting on the SSH Key using Shodan (**hash:-235894729**). This indicates that Observer Stealer previously used the IP address.

Proceeding to the next step, I scanned my second available IP — **5.42.64[.]41** on URLScan, and it gave me some results as could be expected, considering that more than a month had passed since the moment of advertisement (see Figure 5).

URLScan search results for IP 5.42.64[.]41

Investigating the IP — **5.42.64[.]41**, I found out that it's hosted by *LetHost LLC*, located in Ukraine. Pivoting from this IP, using a hash: 599bcb7c7d723e17254471f56fec317ec688bd1c8d62463f6001a8178db749c6, allowed to discover two additional IP's: **179.43.155[.]205** (port **81**) and **91.215.85[.]38** (port **1234**) — see Figure 6.

Pivoting results

Additional way to discover the same IP's could be through Censys. I was pivoting from the initial IP address **5.42.64[.]41** through the favicon's name, which is quite unique in this case: icon-*"b3de897a.png"*. To discover more IP addresses, I thus used the following query: **services.http.response.favicons.name= *"\*icon-b3de897a.png"*** (see [Censys](#)).

ObserverStealer panel

Since I didn't identify any additional C2 panels, I am stopping here and proceeding to the next step. Before I did, I noticed something interesting about the panel. Instead of choosing the title, developers of the panel chose to auto-generate the random title, which changes every time the page is refreshed ( see Figures 8–9). Was it an attempt to make panels more challenging to identify with search engines like Shodan or Censys? I think it was.

ObserverStealer auto-generated title (V1)

ObserverStealer auto-generated title(V2)

Going to the next step — I will check what I can find with VirusTotal related to these two IP addresses:

- 77.73.134[.]51: 1234 (inactive)
- 5.42.64[.]41: 1234 (active)
- 179.43.155[.]205: 81 (active)
- 91.215.85[.]38: 1234 (active)

When, the first IP address didn't show any relevant for us results, the second IP address — **5.42.64[.]41** gave us a lot of useful information, including the list of files communicating with this specific IP (see Figure 10). I attached the list of hashes at the end of the article.

. VT results showing files communicating to IP:

VT showing the file link to IP

In this article, I won't analyze any samples, but upon initial inspection, nothing seems noteworthy except for port **1337**, which is relatively uncommon. The stealer has similar functions to other stealers. If you want to analyze a sample, check out example shared on Twitter, which lets you preview the sample's execution in [Any.Run sandbox](#). Scanning the other two IPs (**179.43.155[.]205** and **91.215.85[.]38**) didn't give any results on VirusTotal, so that I will leave it from here.

Lastly, I checked the Telegram page dedicated to the stealer. Although the administrator initially had two private and public channels on Telegram, on the day of writing, I saw that they chose to delete them and added an additional News section to the panel instead. The reason for closing channels is the chance that the channel can be blocked, as well as to limit access to it( see Figure 12). On the forum, the Matrix contact details (**@observer:matrix.fedibird.com**) were shared instead. Access to the private channel can still be obtained by contacting the seller in PM via Matrix or Forum.

Observer Stealer explaining the switch from Telegram to Matrix

To conclude, ObserverStealer is a new player in the malware arena that still tries to earn its place under the sun. It is advertised on multiple web forums, and from my observation seller takes steps towards making the panel more difficult to find, as well as generally limiting access to the information related to stealer. In any case, it's worth keeping eyes open and monitoring the development of stealer-related activities to stop it timely.

## IOCs

77.73.134[.]51

5.42.64[.]41

179.43.155[.]205

91.215.85[.]38

11fc584f1bd753c3f68de7313a2bcc5fe51c150002dbad3e331bbf12ce007281  
1e9dc15ff729f34b4b65c0742c433494f969a8f606d46dab010f34d05ee057f6  
1facdfcd57424c577662c7cee0bc3fd03d2ac8420f5c8fc9f02908261bb0b3e1  
26bc9287f34be69cef7beca9e91c4a4f1de6f5934d9bc643f8d8de7754bda294  
2a5c0c087f07dd64f42dd93356233dcef45b37cf606c3881277b79295b0e210d  
3b21c39c7e327f8876cf45ee882fa8b1c5d6eb140e11e1b0aa03f65e9d73f9d3  
4b3e6ae964d293d711de434896b19651ee1ffb089f279dc38bdcbd56008ed4dc  
4e1d47f621979e582f61659baf8a38479c4fcb02fed4d3b3ab48bfed89e3d9e9  
69f9b5e563e314a1eef85dca636b85ae0afdd3e91fd5b66351ce60eaa8d63778  
74e353ca0b63d17e49ec99744fd027701fc54956a792f741b0143bc52791768a  
79c62136dbeb4d294fb569ba6679363b1e790f884dc923b6bee4a6ee33d8f1fb  
79c6fdedbe965a9ebf8d80f13e27332b18cdb0b313c5bb9a7c2b6723b53d3335  
83cef007c65d676564637cfacc639a13ae6a06d37851ca08d734a25ab35da520  
9e57ccd47600e2e5483b7464549bad124f2f529f09ad29a570f4e583a3355968  
a35eb6812a61448900993e7e42017dcad0ba5c29fef0eba8b5d13c7d9a111cc0  
a9db0b8c828a3dedfb985b117f4d4dba043ca09cf6b5f59ef44e3d5d40f5ba9b

aec3ff058065df87c6eb2f5f654c27a9c56f72a053661fcbe8a4193e26fd486a

b119196b6f6c2127e37c6ddaf36d26087420b7e77017016f90dee3c000750960

b796b25f10ac609c4a05393fb5ac4b33da8c5325148a8c30cd273bdbe475eeff

cd2abfbc7b13db5ad7162c634034a7661bb81f19ddc7052cbae27346d3fada39