DeathRansom Part II: Attribution

By Artem Semenchenko and Evgeny Ananin

Published: 2020-01-02 · Archived: 2026-04-05 23:39:09 UTC

Introduction

FortiGuard Labs recently discovered an ongoing DeathRansom malicious campaign. Our first blog on this new variant was devoted to a technical analysis of the samples that had been gathered. In this second part, we will try to shed a light on how this DeathRansom campaign is connected with other campaigns, and who might be behind them.

False Scent and Connections with Vidar Stealer

False Language Lead

We start our investigation with the sample 13d263fb19d866bb929f45677a9dcbb683df5e1fa2e1b856fde905629366c5e1, which was mentioned in our previous blog. This sample has debug paths, but we could not recognize the language used. In addition, it has nine resources, with a LANG_SLOVAK identifier constant (0x041B) in the resource section. This means that the sample could have been compiled on a machine with a Slovak language installed by default.

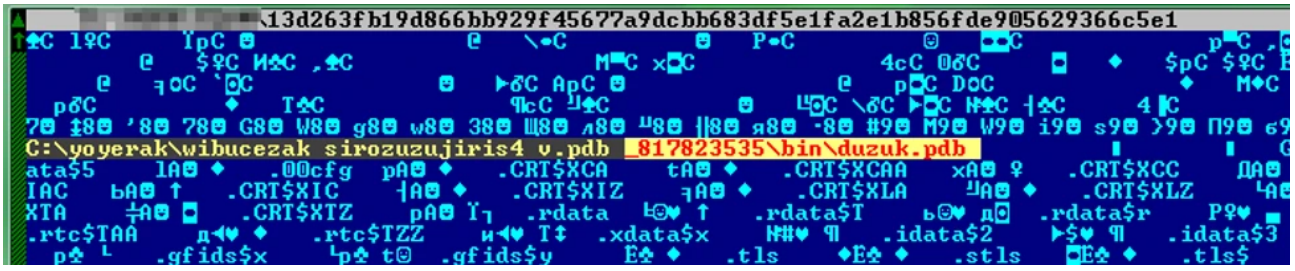


Figure 1: A debug path inside the sample

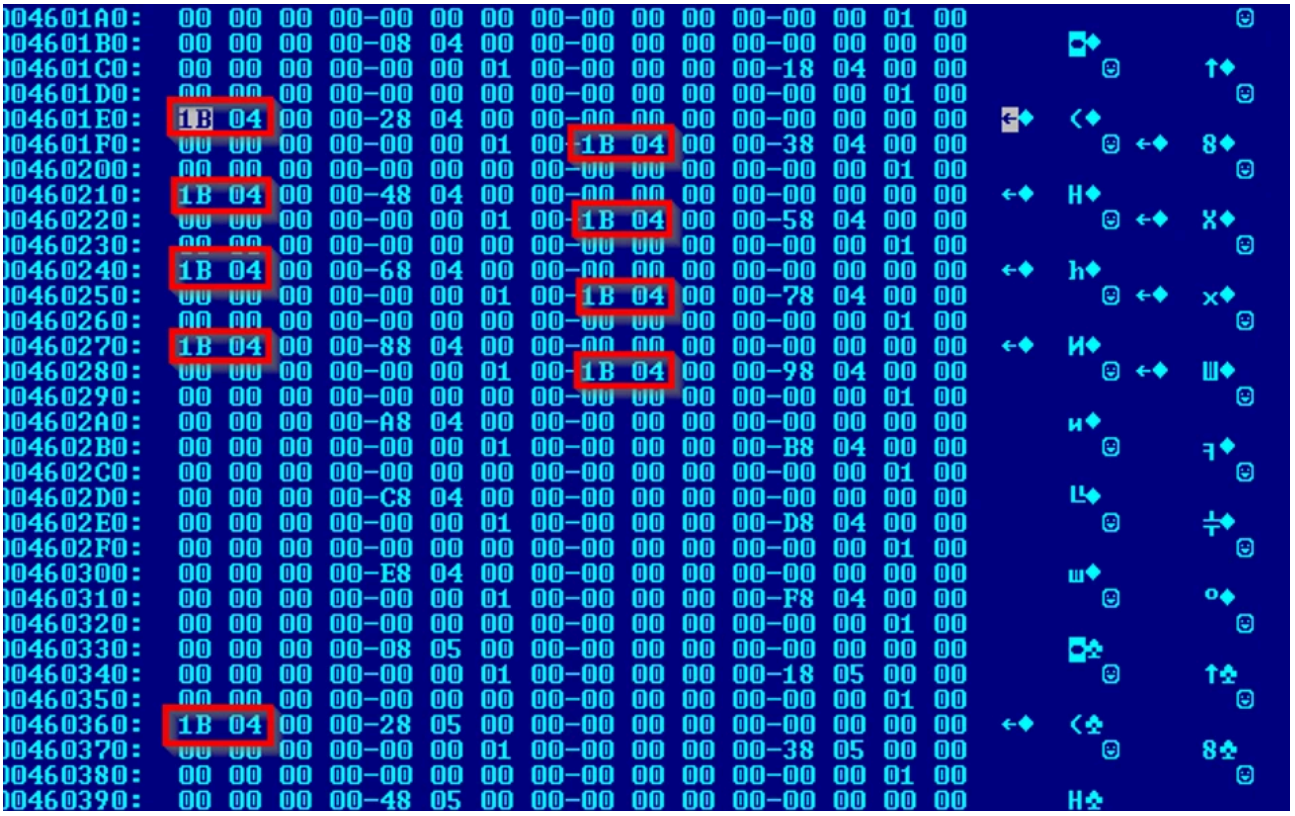


Figure 2. Part of the .rsrc section of the sample

We tried to translate a PDB path from Slovak by splitting the words in different ways and then feeding the results to various automatic translation services. However, none of these attempts led to a correct translation. In fact, the word “duzuk” was recognized by Google Translate not as Slovak, but as Basque (for the English “you have”).

A Basque word was an intriguing lead, since this sample was downloaded from a domain in the *.es* domain zone (Spain). We believe that this domain was hacked, therefore we will not disclose the domain name here.

The name of the sample was also interesting: *Wacatac_2019-11-20_00-10.exe*. The word “Wacatac” can be translated from Basque in several different meaningful ways, so we decided to dig deeper.

Since the file name has a clearly distinguishable name-date-time construction, we decided to search for this pattern among all known files. Nine files were found. Their details are provided in Figure 3.

Name	Resource_Lang	Debug Path
Wacatac_2019-11-16_11-47.exe	NEPALI DEFAULT	C:\\yagubo79-mit wusizefac\\buwuv38-bigunuvepixulujim.pdb
Wacatac_2019-11-16_14-06.exe	NEPALI DEFAULT	C:\\hayanoram.pdb\x00_server\\runtime\\crypt\\tmp_98790941\\bin\\zotojenet.pdb
Wacatac_2019-11-16_15-39.exe	NEPALI DEFAULT	C:\\minax povapuziwepufefu.pdb\x00me\\crypt\\tmp_1435530333\\bin\\nelidayo.pdb
Wacatac_2019-11-19_18-15.exe	SLOVAK DEFAULT	C:\\dubefedoyaxamile golosotipelozujawaco_pipebamog\\maj.pdb
Wacatac_2019-11-20_00-10.exe	SLOVAK DEFAULT	C:\\yoyerak\\wibucezak sirozuzujiris4 v.pdb\x00_817823535\\bin\\duzuk.pdb
Wacatac_2019-11-20_04-06.exe	NEUTRAL	NO
Wacatac_2019-11-20_19-54.exe	NEUTRAL	NO
Wacatac_2019-11-20_23-34.exe	NEUTRAL	NO
Wacatac_2019-11-21_02-59.exe	SLOVAK DEFAULT	C:\\rokumuv29-locatag66-hod\\monekuxusuh jimorocolej.pdb

Figure 3. A part of our investigation table

Again, we were a little disappointed: the resource language ID's were changed from Nepali to Slovak then to Neutral then back to Slovak at a very fast pace. In addition, the debug paths look like machine-generated gibberish rather than any paths a human programmer would use.

Therefore, we had to conclude that a Basque trace was just a coincidence. However, the Slovak and Nepali traces are not. Most probably, they were intentionally inserted to mislead potential investigators.

Bitbucket Profile

In spite of these disappointments, these new samples also gave us an important clue. One of the samples shown on Figure 3 was downloaded not from the hacked .es site, but from a different URL:

hxxp://bitbucket[.]org/**scat01**/1/downloads/Wacatac_2019-11-16_14-06.exe

The link was not accessible, and neither was the *scat01* profile itself:

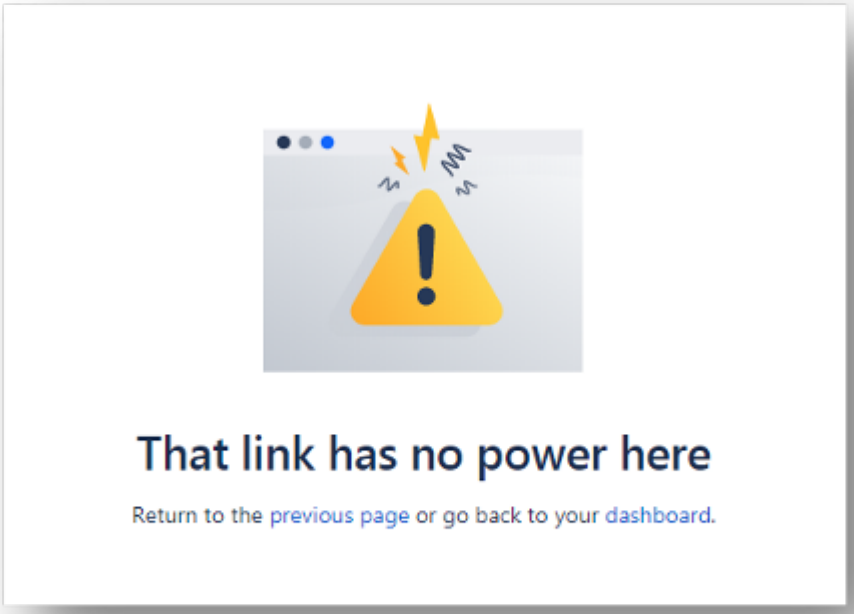


Figure 4. Bitbucket message shown on an access attempt to the scat01 profile

Nevertheless, when we searched for other malicious samples which attempted to access this Bitbucket directory, we found an interesting connections log from May 2019. The sample was related to the Vidar stealer malware family.

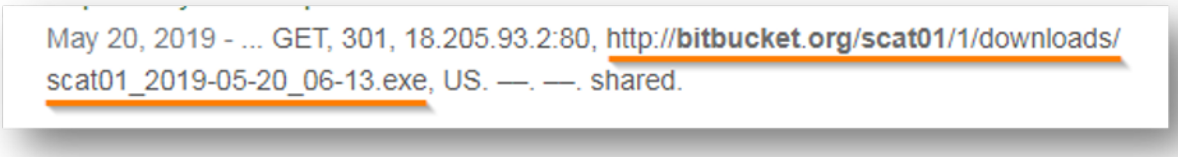


Figure 5. A part of a connections log for the Vidar sample

The name pattern has an obvious resemblance to our *Wacatac* sample:

Wacatac_2019-11-20_00-10.exe

scat01_2019-05-20_06-13.exe

Next, we decided to search among the connections logs for a connection by the URL mask

*bitbucket[.]org/scat01/**

One of the connections logs found on VirusTotal is shown on Figure 6 (sample dc9ff5148e26023cf7b6fb69cd97d6a68f78bb111dbf39039f41ed05e16708e4).

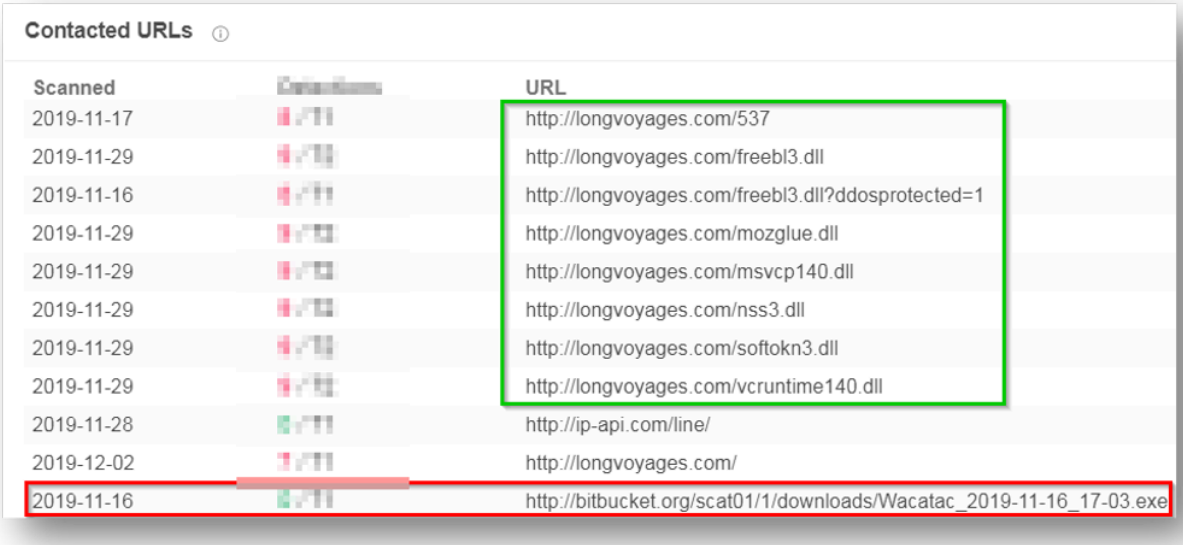


Figure 6. Contacted URL via a fresh malicious sample

Let’s now analyze these connections. The connections shown in the green frame should be familiar to anyone who has dealt with Vidar stealers, as they are standard Vidar libraries used to extract passwords from different browsers.

The connection shown in the red frame is an attempt to access an executable file with another *Wacatac* name. Unfortunately, this link was not accessible during the Vidar sample sandbox analysis, therefore we don’t have a *Wacatac_2019-11-16_17-03.exe* sample.

Nevertheless, as you may remember from our first blog, DeathRansom uses the name 'Wacatac' to store crypto keys in a registry. Therefore, we have strong reason to believe that the inaccessible *Wacatac_2019-11-16_17-03.exe* sample was another DeathRansom variant.

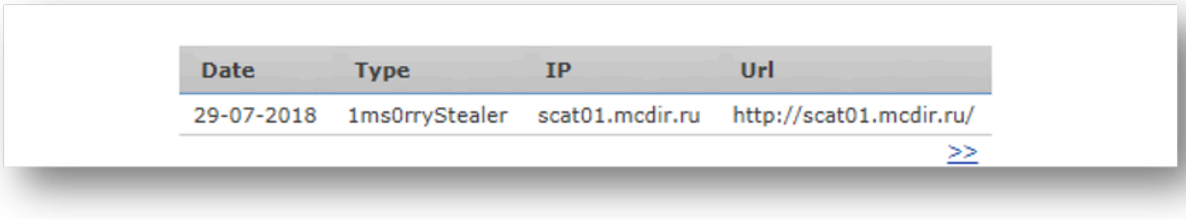
Therefore, based on the same "malware hosting", the same name pattern, and the fact that the Vidar sample tried to download a DeathRansom sample, we can conclude that the Vidar campaign and the DeathRansom campaign are run by the same actor, who uses *scat01* as a Bitbucket profile name as well as a name for some malware samples.

We decided to dig deeper and see what could be found about this *scat01*.

Following scat01

We started to look for fresh malware containing the string *scat01* in it. Here is a short summary of our findings:

- One of the samples we found was the "**Azorult**" stealer malware that connects to a C2 server "*scat01[.]tk*". a45a75582c4ad564b9726664318f0cccb1000005d573e594b49e95869ef25284
- We also managed to find a C2 panel of "**1ms0rryStealer**" with the name *scat01* in the Benkow "Panel Tracker" service:



Date	Type	IP	Url
29-07-2018	1ms0rryStealer	scat01.mcdir.ru	http://scat01.mcdir.ru/

>>

Figure 7. Archived record of the stealer control panel

- The most important sample was found here:
  *hxxp://gameshack[.]ru/**scat01.exe***
  e767706429351c9e639cfecaeb4cdca526889e4001fb0c25a832aec18e6d5e06

  This sample is a non-obfuscated Evrial stealer. When we check its configuration, we see the following "Owner" field:

```
private static void Main()
{
    RawSettings.Owner = "scat01";
    RawSettings.Version = "1.0.3";
    RawSettings.HWID = Identification.GetId();
    Passwords.SendFile();
    Module.ClipperThread();
    Run.Autorun();
    Application.Exit();
}
```

Figure 8. Malware owner field

The last sample was downloaded from a root folder of the website *gameshack[.]ru*. This could mean that attackers somehow control this webserver. Therefore, we decided to see what else could be found on this webserver.

Gameshack[.]ru Portal

We found many malicious samples, which were downloaded directly from a root folder on Gameshack[.]ru. We decided to analyze all available samples and extract any information that could help us in our investigation.

Scanned	[redacted]	URL
2019-04-30	[redacted]	http://gameshack.ru/scat01.exe
2019-04-02	[redacted]	http://gameshack.ru/adobeflashplayer.exe
2019-03-23	[redacted]	http://gameshack.ru/csgo/gameshack.exe
2019-03-17	[redacted]	http://gameshack.ru/
2019-03-06	[redacted]	http://gameshack.ru/gameshack.exe
2019-04-04	[redacted]	http://gameshack.ru/AdobeFlashPlayer.exe
2019-03-31	[redacted]	http://gameshack.ru/systems.exe
2019-04-30	[redacted]	http://gameshack.ru/miner.exe
2018-04-09	[redacted]	http://gameshack.ru/gameshack.rar
2018-03-19	[redacted]	https://gameshack.ru/gameshack.rar

Figure 9. Malicious samples downloaded from “gameshack[.]ru” (according to VirusTotal)

The malware samples “hosted” on the *gameshack[.]ru* website were downloaders. This means that their purpose was to download a payload and run it. The main payload was of two types:

- Evrial stealer;
- Miner+Clipper+Stealer (Supreme miner).

The Evrial stealer samples were not obfuscated and contained the same “Owner” field – “**scat01**”.

The Supreme miner samples were obfuscated by “NULL SHIELD” (Confuser variant) and had an e-mail embedded: **vitasa01[@]yandex.ru**.

Figure 11 shows part of the strings from the miner “Supreme.exe” (sample 1e1fcb1bcc88576318c37409441fd754577b008f4678414b60a25710e10d4251). This miner also had the Evrial stealer inside its body:

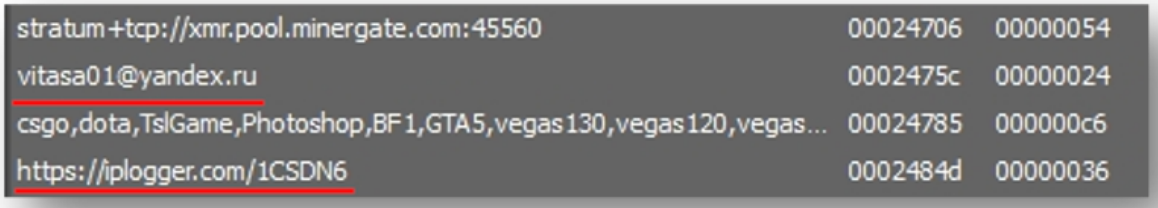


Figure 10. Strings from the miner’s part of the malware

As you can see, this sample uses the same *iplogger* service for counting the infected hosts as the DeathRansom samples (see our recent blogpost for details.)

The Evrial stealer inside has the same “scat01” ownership:

Figure 11. Strings from the Evrial stealer’s part of the malware

As you can see, the website “*gameshack[.]ru*” is controlled by attackers and they distribute malicious samples with *scat01* attribution strings inside.

Here is a short summary of the info about the attackers that we have found so far, including the spread of malware families associated with them:

- DeathRansom
- Vidar stealer
- Azorult stealer
- Evrial stealer
- 1ms0rryStealer
- Supreme miner

As well as attribution info:

- **scat01** nickname;
- **vitasa01[@]yandex.ru** e-mail.
- Control over **gameshack[.]ru**

It seems obvious that these attackers use a Russian email service and a Russian domain zone *.ru*. In addition, we must remember that DeathRansom performs a check for the system language, and it will not encrypt files if it detects locales from an ex-USSR country.

In addition, when we analyze the stealers used by this group, we find that they can be purchased on Russian underground forums. Therefore, we decided to continue our search there.

Russian Underground

Once we searched for “scat01” and “vidar” on the Russian underground forums, we found a person with the same nickname providing a review (in Russian) of the **Vidar stealer**:

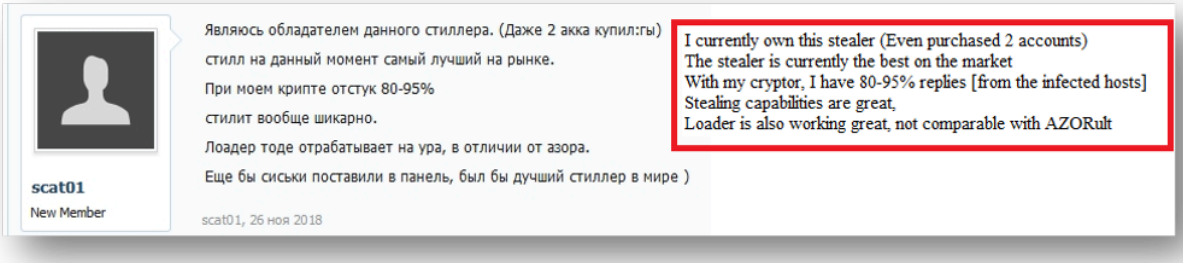


Figure 12. Feedback for Vidar stealer left by scat01

We found another post left by **scat01** on another forum. This time it concerns the **Evrial stealer**. He is afraid that someone might access his logs from that Evrial stealer, as all the information goes to the malware seller’s servers.

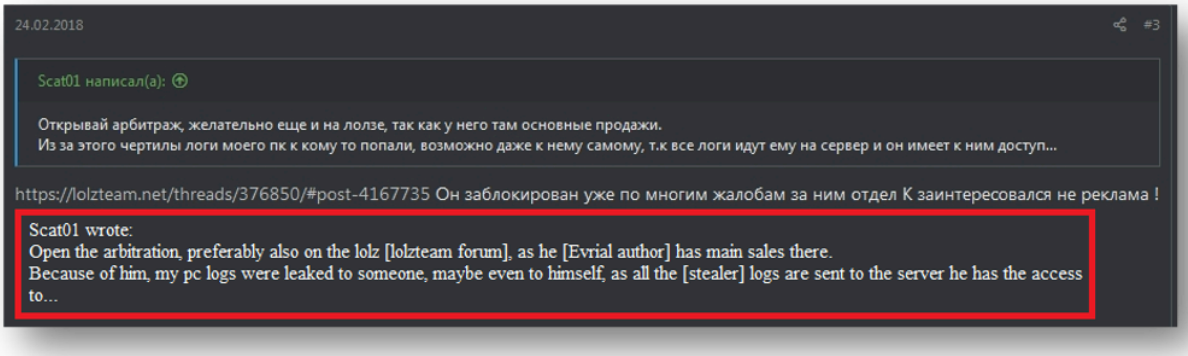


Figure 13. Complaints of scat01 regarding Evrial stealer seller

Another post with a review was found on another Russian underground forum. This time the review is for **Supreme miner**:

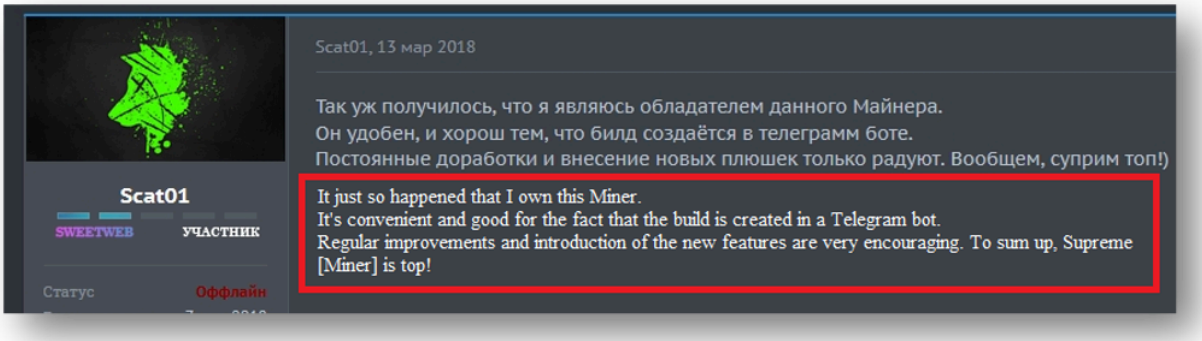


Figure 14. Feedback for Supreme miner

Moreover, a user with the same name was active on yet another Russian underground forum (from now on, we will refer to this underground forum as *Russian underground forum #4).* The user is currently banned for having multiple accounts with different names. Please pay attention to the profile picture used here.

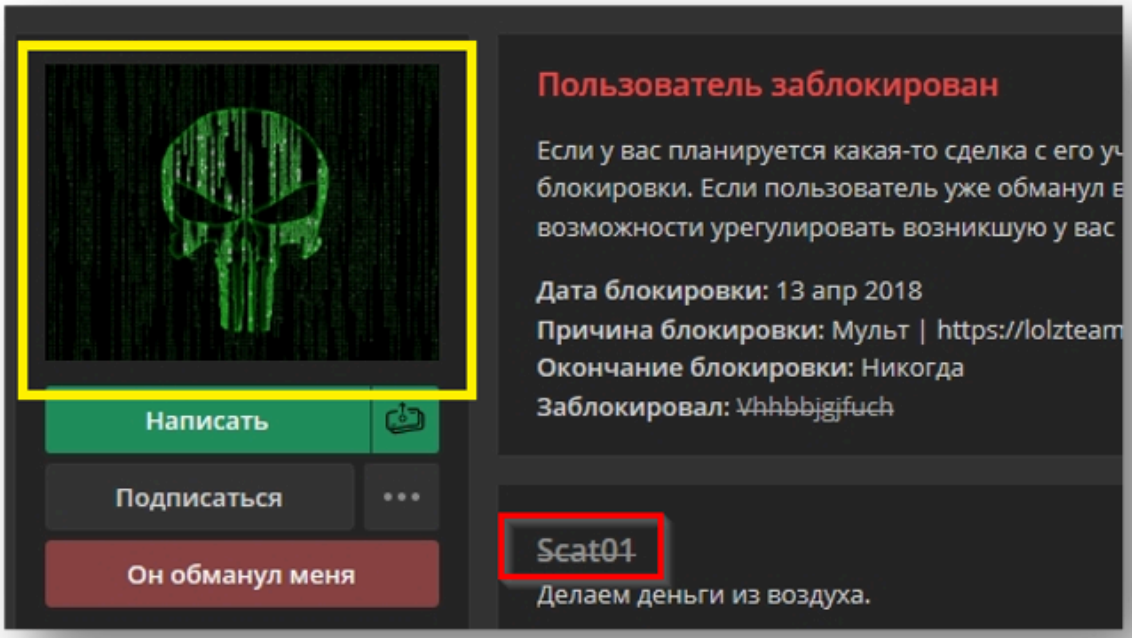


Figure 15. Scat01 profile on the Russian underground forum #4

Now, having found his/her profiles on the underground forums, we next extended our search, comparing the information. One interesting piece we discovered is a product review on Yandex.Market – the same company that provides the email service in the @yandex.ru domain.

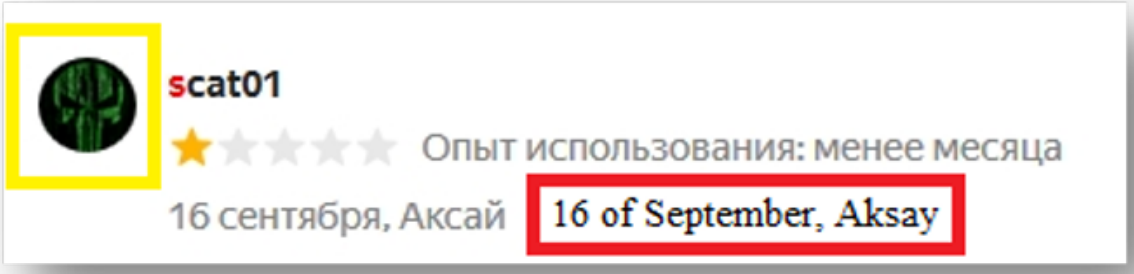


Figure 16. Review for a purchase

In the review there is no text (only a score), but we can see its location. The review was made from Aksay. Aksay is a small Russian town near **Rostov-on-Don** (we will come back to this clue a little later).

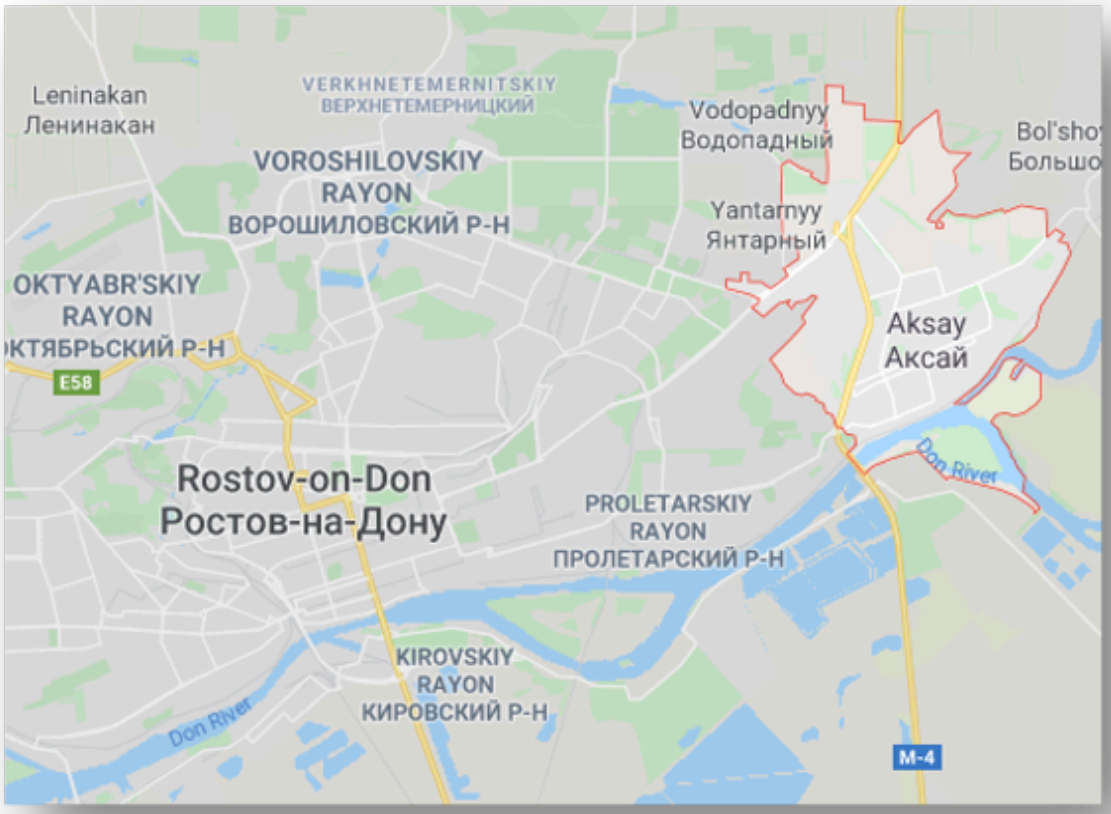


Figure 17. Aksay on Google Maps

Another important clue here is the username of the reviewer account: *vitasa01*. Therefore, it is highly probable that this reviewer has access to the email *vitasa01[@]yandex.ru*, which we have seen in previous malicious samples.

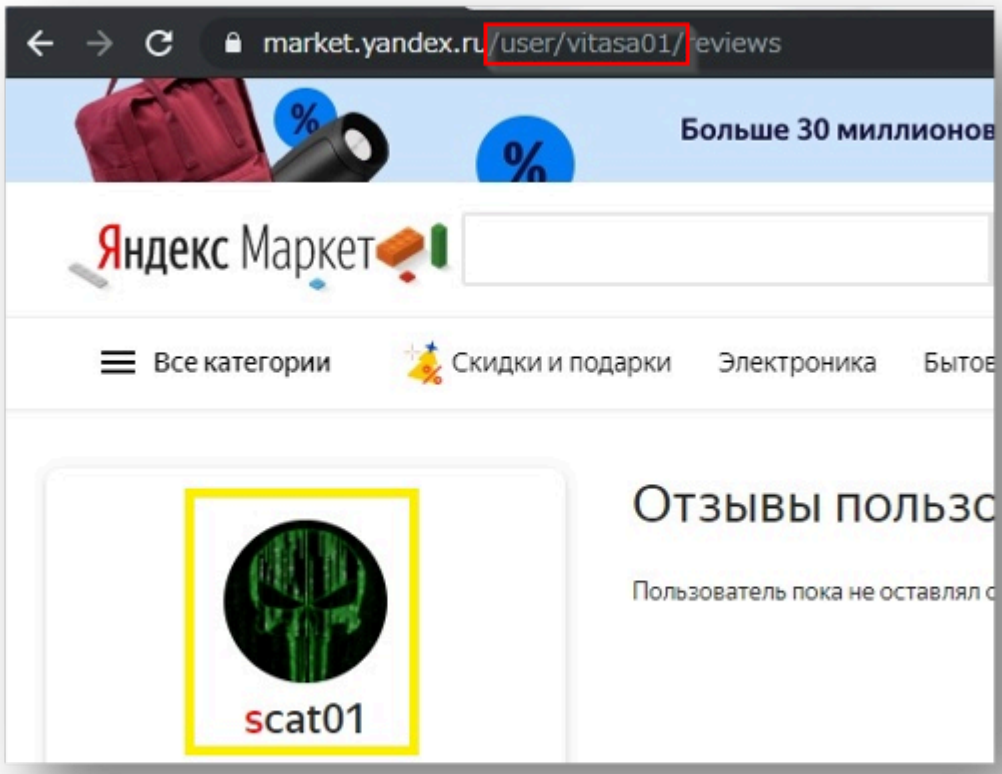


Figure 18. Yandex username in the URL string

Also, please pay attention to the picture used in this profile. It is the same picture shown in Figure 15. Therefore, we have a triple match:

- the profile picture
- current username
- Yandex username

At this point, we are pretty sure that this Yandex profile is related to the *scat01* profile we found on the *Russian underground forum #4* as well as to the malware distributed from g*ameshack[.]ru*. But how can we find the possible real identity of this author? We decided to see what info we could find about g*ameshack[.]ru* itself.

Gameshack[.]ru Portal

We found an interesting YouTube channel that promotes the website *gameshack[.]ru*. The link to *gameshack[.]ru* is named: “our game portal.”

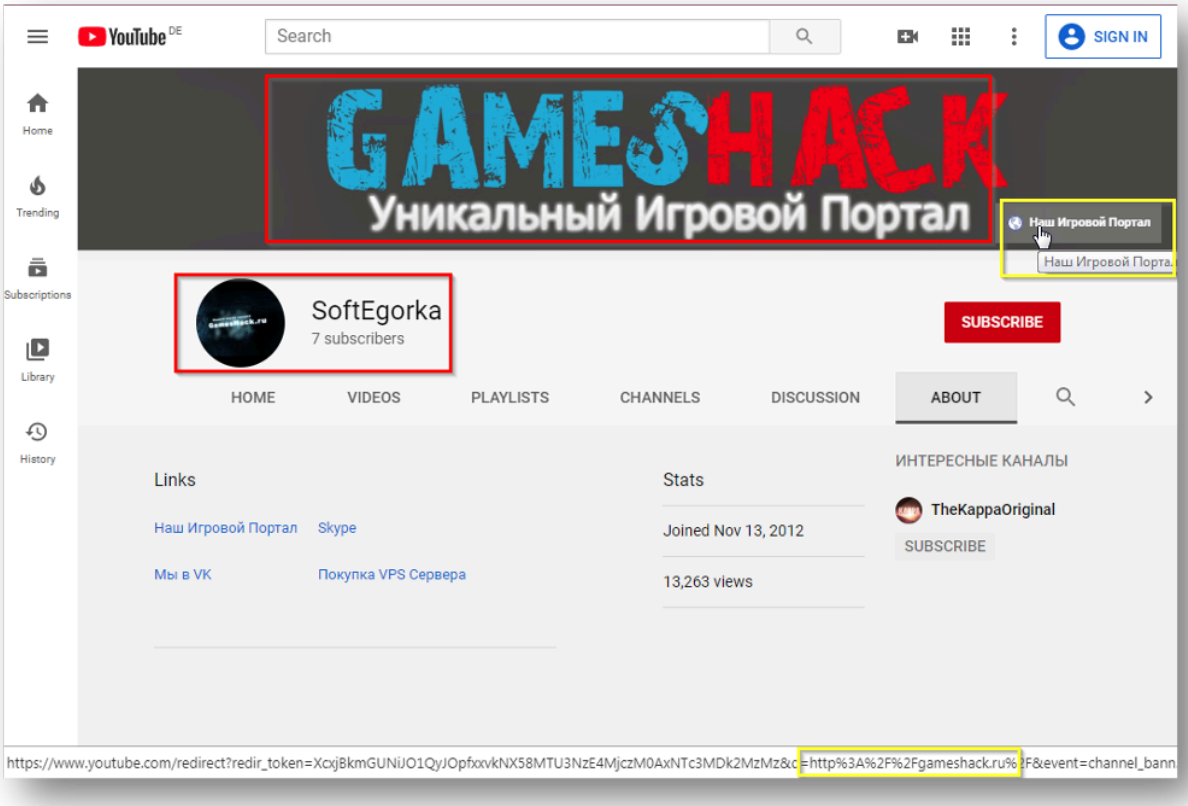


Figure 19. YouTube channel advertising malicious website

The username given here is “SoftEgorka.” “*Egorka*” is a diminutive for the Russian name “*Egor.*” The avatar picture also refers to *gameshack[.]ru*.

Another interesting piece of information we found is a Skype link. In figure 20, you can see that it refers to the skype username *SoftEgorka:*

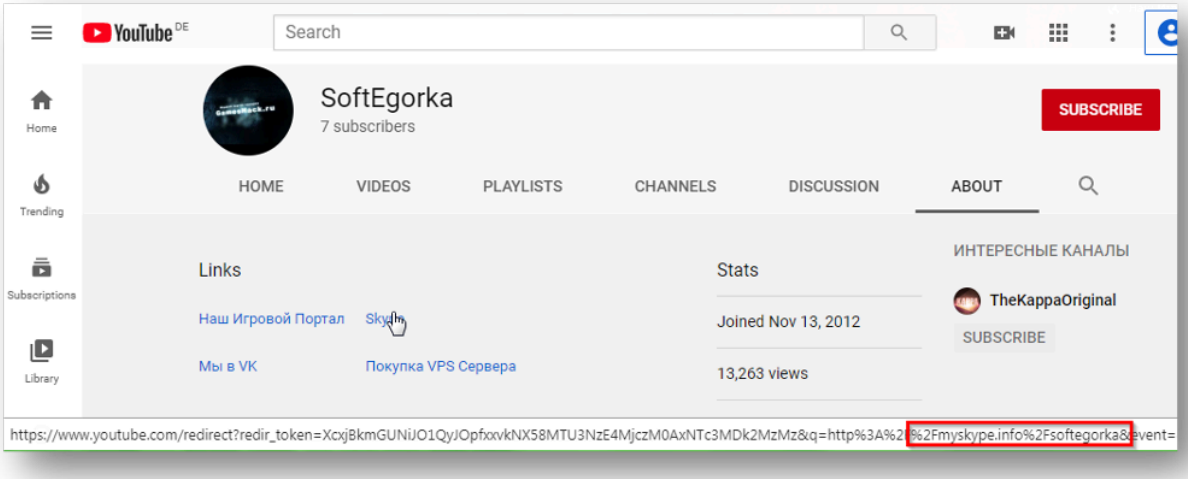


Figure 20. Skype link in the YouTube profile

When we searched for a “SoftEgorka” skype user, we found the following user profile on the same *Russian underground forum #4.* This time the username “Super info” is used.

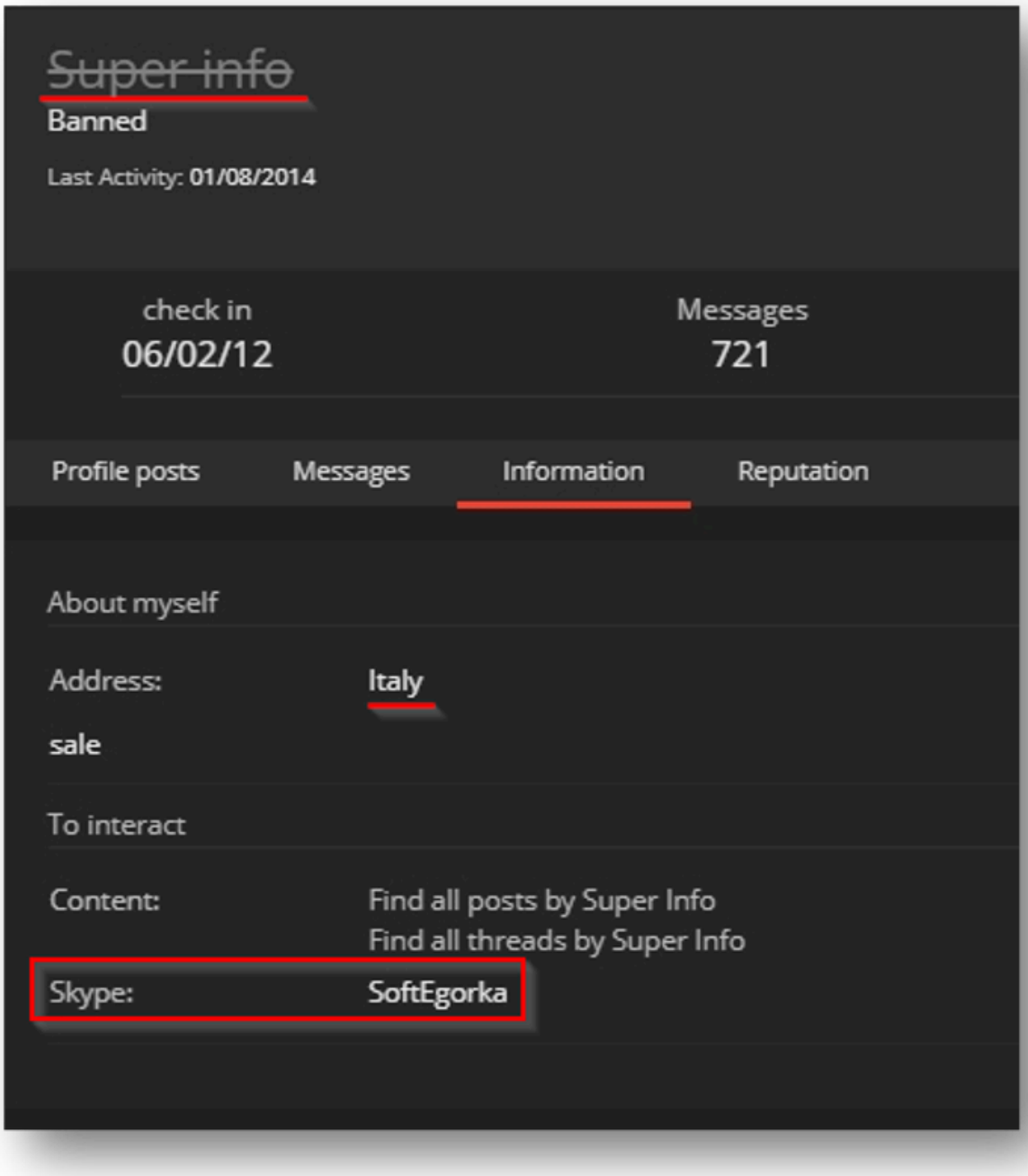


Figure 21. “Super info” profile on the Russian underground forum #4

The Skype address corresponds to the YouTube channel discussed above. The user states that he lives in **Italy**. Moreover, searching further for his messages, we found another confirmation that this could be true:

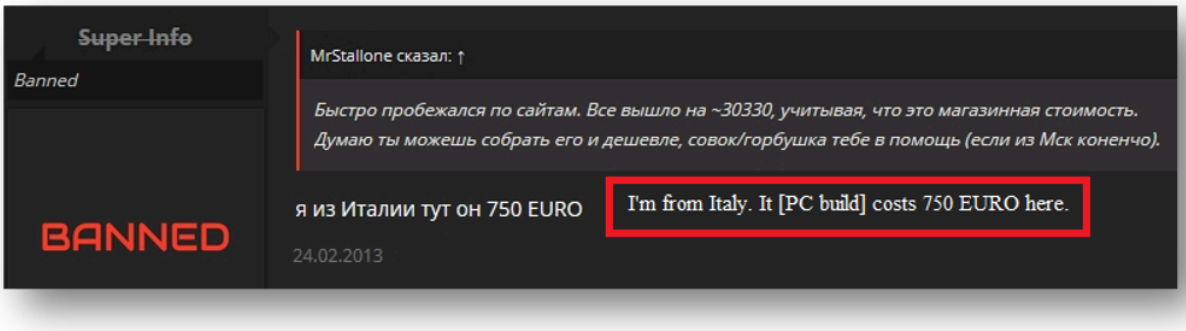


Figure 22. The actor claims that he/she is from Italy

By digging further among *Super Info* posts, we found an announcement about game accounts sales (Steam, WoT, Origin). Here we should note that stealers observed above are capable of stealing passwords from different games and game distribution platforms. This more indirect evidence that Super Info may be connected to the ongoing stealers campaign.

Figure 23. A message with a WebMoney ID and the known skype link inside

In the contacts section of the sale, you find “Skype: SoftEgorka” as well as the WebMoney ID **372443071304**. This same WMID is mentioned in another post from the same user. It is also related to Steam accounts for sale. And this time, another skype profile is mentioned: **nedugov99**

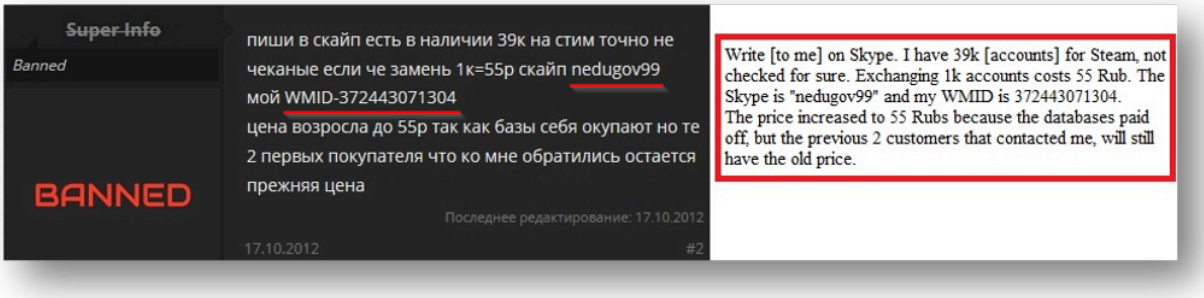


Figure 24. A message with the same WMID and skype account nedugov99

Searching again, this time for this new Skype ID, an old advertisement for the sale of a game account shows up:

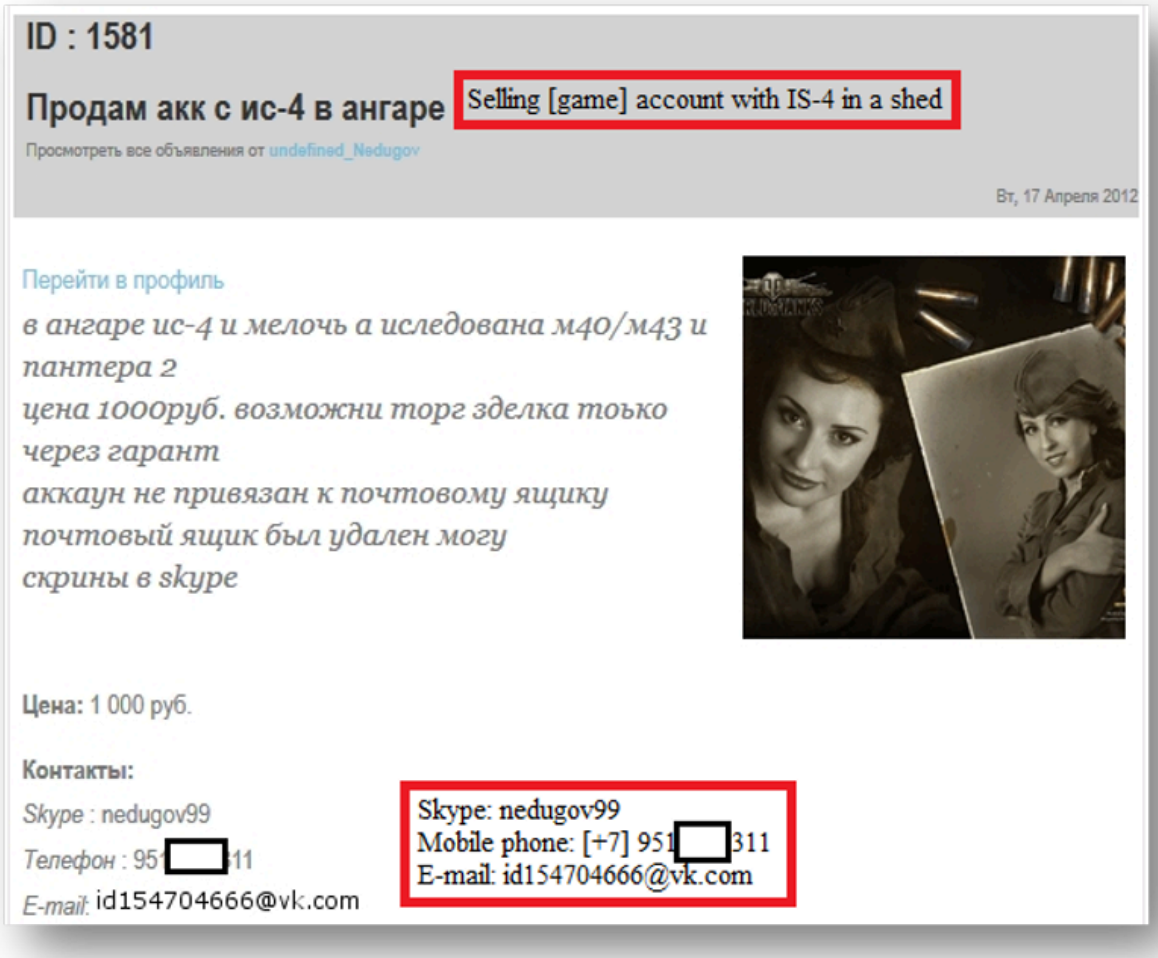


Figure 25. Old advertisement of a game account for sale

Here, we can see several important pieces of information:

User name: undefined_Nedugov

The skype id: **nedugov99**

The phone: +7951****311

Vkontakte SNS id: **id154704666**

We checked the mobile phone number and it belongs to the **Rostov-on-Don** region.

Next, we checked out the VK **id154704666** profile:

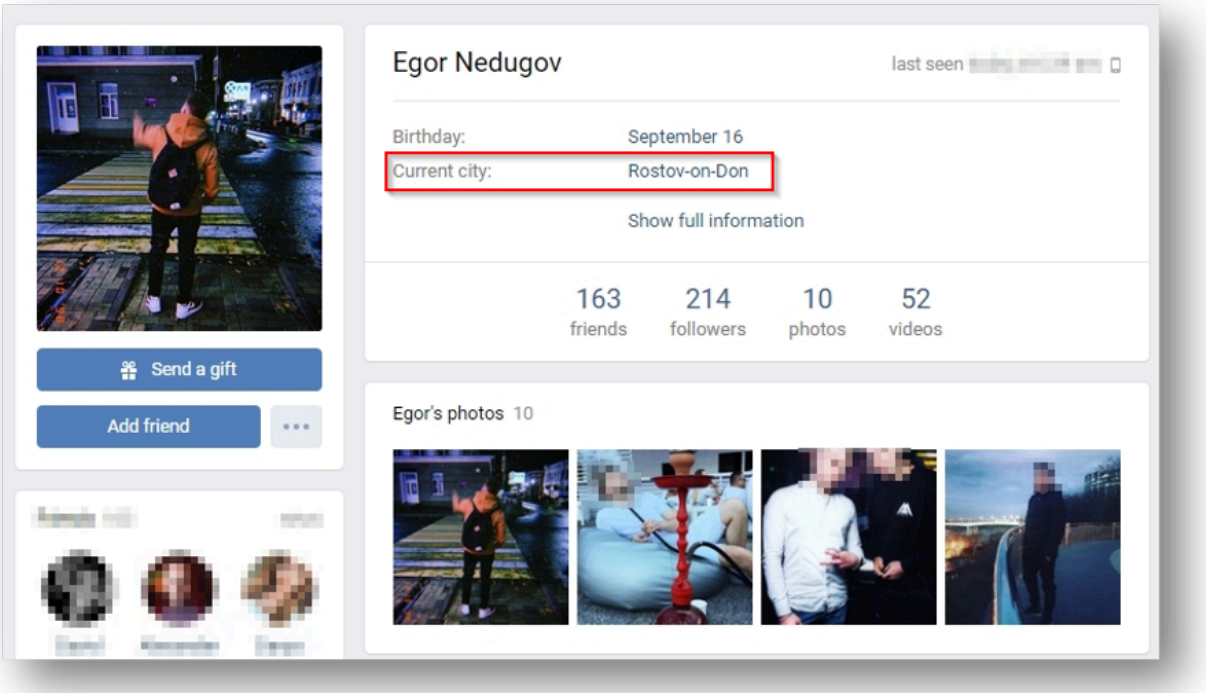


Figure 26. Vkontakte SNS profile of Egor Nedugov

The name “Egor” corresponds to one of the underground nicknames, “Soft**Egor**ka,” and the surname “Nedugov” corresponds to the Skype account “**nedugov99**”. According to the profile, this individual lives in Rostov-on-Don. Remember that the Yandex review made by *scat01* was done from Aksay – a small town near Rostov-on-Don.

And even more interesting, he is following (or maybe even administrating?) the “Gameshack[.]ru official group”. The link to the same group is found in the YouTube profile shown in Figures 20-21.

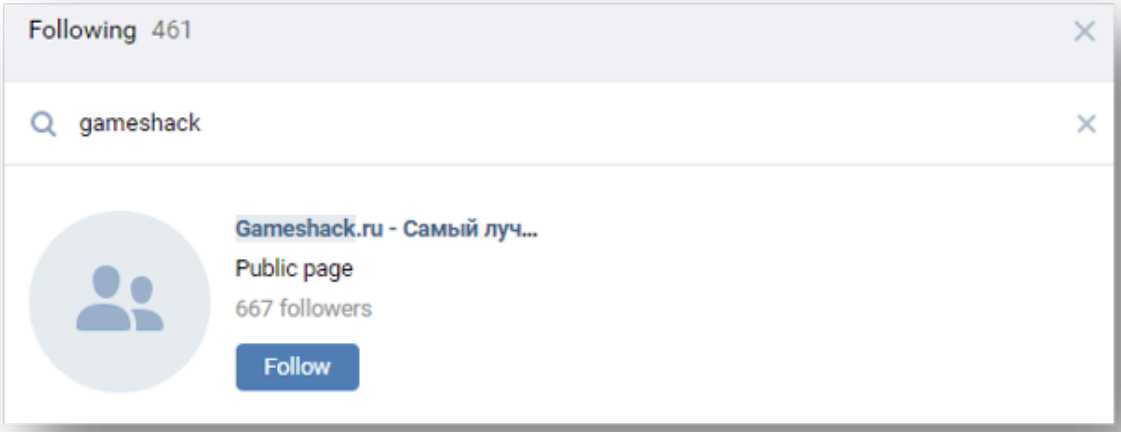


Figure 27. “Egor Nedugov” is following the malicious website VK group

Here an astute reader might ask: “Rostov-on-Don? But what about Italy, mentioned in Figures 21-22?” To get an answer, we have to visit Egor’s Instagram page:

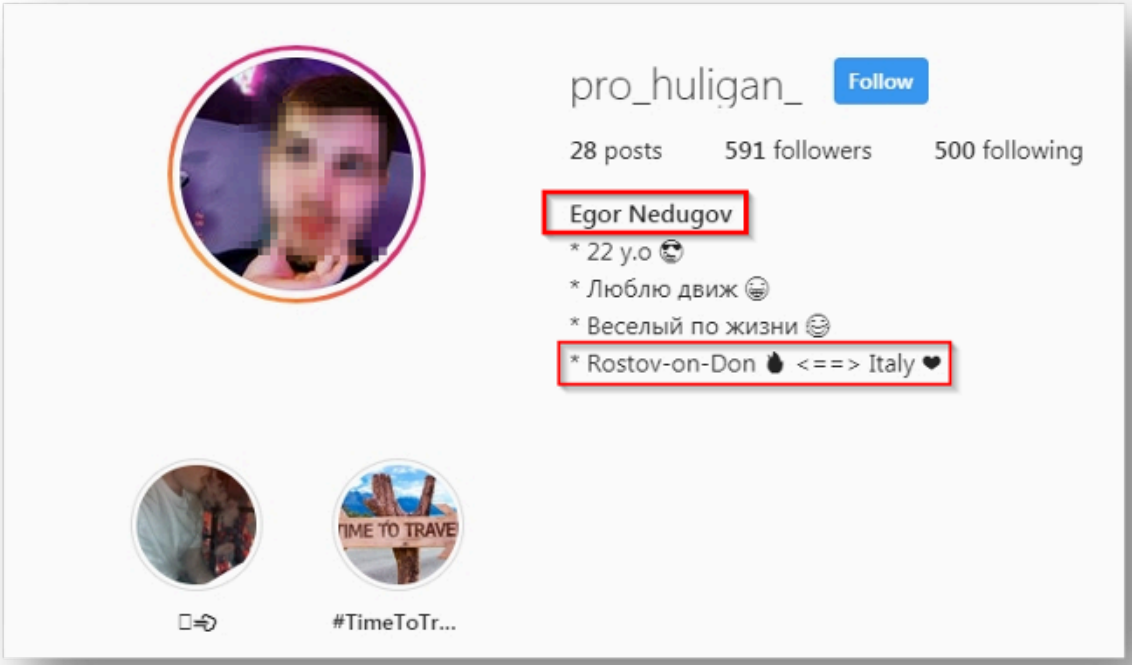


Figure 28. Instagram account of Egor Nedugov

As we might learn from his Instagram and Facebook accounts, he indeed lived in Italy for some time.

There is one more thing here. At this point in the investigation, we asked ourselves: “what if *scat01* and *SoftEgorka* are different actors? The former one compiles malware and the later one “hosts” it on Gameshack[.]ru portal?” Obviously, we have connections via *gameshack[.]ru* and geographical connections, but what if they are friends and live in the same region?

Well, we found yet another clue: the profile on *csgo-stats[.]net* is shown in Figure 29. The user with the username *scat01* names himself as *Egor* (Russian: Erop). We must note that the name “Egor” is rare in Russia.

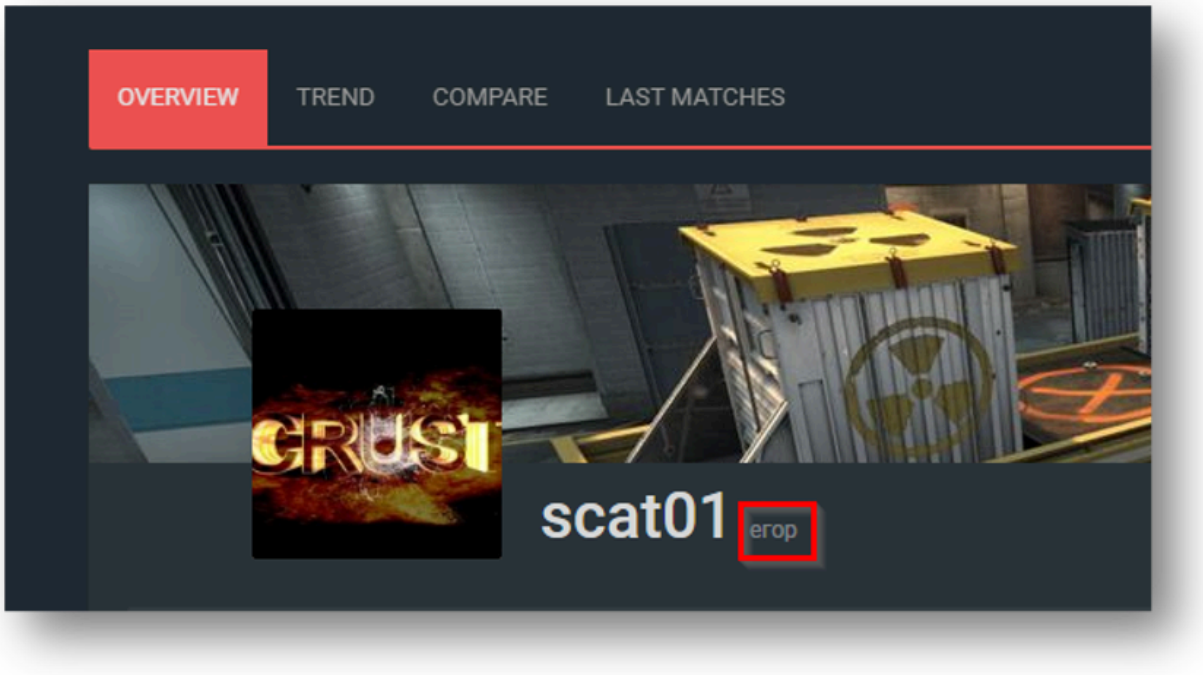


Figure 29. Scat01 profile on csgo-stats[.]net

We also found many other profiles of the same actor. According to information on underground forums, this person is responsible for account stealing, carding, malware distribution, and even the phishing and scamming of his forum mates. That is why nearly all his accounts on underground forums were eventually banned.

Conclusion

FortiGuard Labs established a significant connection between the ongoing DeathRansom and Vidar malware campaigns. They share the naming pattern and infrastructure used. We also found evidence that a Vidar sample tried to download the DeathRansom malware.

We believe that an actor with the nickname *scat01* could be responsible for the latest DeathRansom attack, as well as other malicious attacks. We also found evidence of strong Russian roots in the malware being distributed.

Based on the evidence left on Russian underground forums, we were able to find a person who seems to likely be behind these malicious campaigns.

Solution

All samples mentioned in this article are detected by the FortiGuard antivirus engine:

05b762354678004f8654e6da38122e6308adf3998ee956566b8f5d313dc0e029 - W32/Kryptik.GYME!tr
0cf124b2afc3010b72abdc2ad8d4114ff1423cce74776634db4ef6aaa08af915 - W32/Kryptik.GYQI!tr
13d263fb19d866bb929f45677a9dcbb683df5e1fa2e1b856fde905629366c5e1 - W32/Kryptik.ANT!tr
2b9c53b965c3621f1fa20e0ee9854115747047d136529b41872a10a511603df8 - W32/GenKryptik.DYFO!tr
4bc383a4daff74122b149238302c5892735282fa52cac25c9185347b07a8c94c - W32/GenKryptik.DYBP!tr
6247f283d916b1cf0c284f4c31ef659096536fe05b8b9d668edab1e1b9068762 - W32/GenKryptik.DXWB!tr
66ee3840a9722d3912b73e477d1a11fd0e5468769ba17e5e71873fd519e76def - W32/Kryptik.GYMH!tr
dc9ff5148e26023cf7b6fb69cd97d6a68f78bb111dbf39039f41ed05e16708e4 - W32/GenKryptik.DXWQ!tr
f78a743813ab1d4eee378990f3472628ed61532e899503cc9371423307de3d8b - W32/GenKryptik.DXWH!tr
fedb4c3b0e080fb86796189ccc77f99b04adb105d322bddd3abfca2d5c5d43c8 - W32/Kryptik.GYQI!tr
a45a75582c4ad564b9726664318f0cccb1000005d573e594b49e95869ef25284 - W32/Generic!tr.pws
e767706429351c9e639cfecaeb4cdca526889e4001fb0c25a832aec18e6d5e06 - MSIL/Agent.QJH!tr
1e1fcb1bcc88576318c37409441fd754577b008f4678414b60a25710e10d4251 - MSIL/CoinMiner.AHY!tr

The FortiGuard Web Filtering service blocks the following URLs as malicious:

iplogger[.]org/1Zqq77
bitbucket[.]org/scat01/
scat01.mcdir[.]ru
gameshack[.]ru
scat01[.]tk

IOC

SHA256:

05b762354678004f8654e6da38122e6308adf3998ee956566b8f5d313dc0e029
0cf124b2afc3010b72abdc2ad8d4114ff1423cce74776634db4ef6aaa08af915
13d263fb19d866bb929f45677a9dcbb683df5e1fa2e1b856fde905629366c5e1
2b9c53b965c3621f1fa20e0ee9854115747047d136529b41872a10a511603df8
4bc383a4daff74122b149238302c5892735282fa52cac25c9185347b07a8c94c
6247f283d916b1cf0c284f4c31ef659096536fe05b8b9d668edab1e1b9068762
66ee3840a9722d3912b73e477d1a11fd0e5468769ba17e5e71873fd519e76def
dc9ff5148e26023cf7b6fb69cd97d6a68f78bb111dbf39039f41ed05e16708e4
f78a743813ab1d4eee378990f3472628ed61532e899503cc9371423307de3d8b
fedb4c3b0e080fb86796189ccc77f99b04adb105d322bddd3abfca2d5c5d43c8
a45a75582c4ad564b9726664318f0cccb1000005d573e594b49e95869ef25284
e767706429351c9e639cfecaeb4cdca526889e4001fb0c25a832aec18e6d5e06
1e1fcb1bcc88576318c37409441fd754577b008f4678414b60a25710e10d4251

URL:

iplogger[.]org/1Zqq77
bitbucket[.]org/scat01/
scat01.mcdir[.]ru
gameshack[.]ru
scat01[.]tk

Learn more about FortiGuard Labs and the FortiGuard Security Services portfolio. Sign up for our weekly FortiGuard Threat Brief.

Learn about Smart Tips to Avoid Crypto Scams.

Read about the FortiGuard Security Rating Service, which provides security audits and best practices.
