Tracking Down REvil's "Lalartu" by utilizing multiple OSINT methods

By Alon Gal—Under the Breach

Published: 2023-03-15 · Archived: 2026-04-06 00:56:55 UTC

7 min read

Jan 30, 2020

In recent months we've seen a spike in companies having their servers breached and files encrypted.

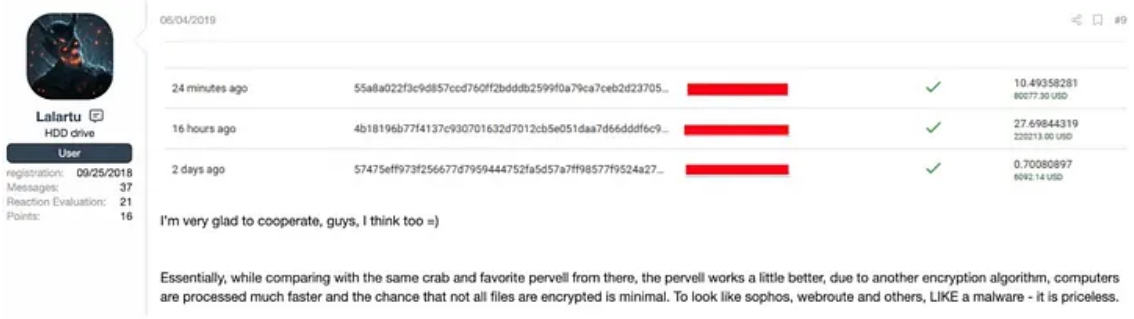
in order for the company to decrypt the files, hackers are demanding a payment, typically in Cryptocurrencies, for which in return they will give the key to open the files.

A specific highly talented group has risen to power lately, they named themselves "REvil"[1] and have already built quite the resume for themselves.

*If you don't want to read the whole thing go to the bottom of the page, I attached an image showing how I arrived to conclusions without a thorough explanation.

On October 14, McAfee released a report[2] in which they analyzed one of the threat actors within REvil group. the threat actor named himself "Lalartu" and posted several images of his earnings from his Ransomware activities:

Press enter or click to view image in full size



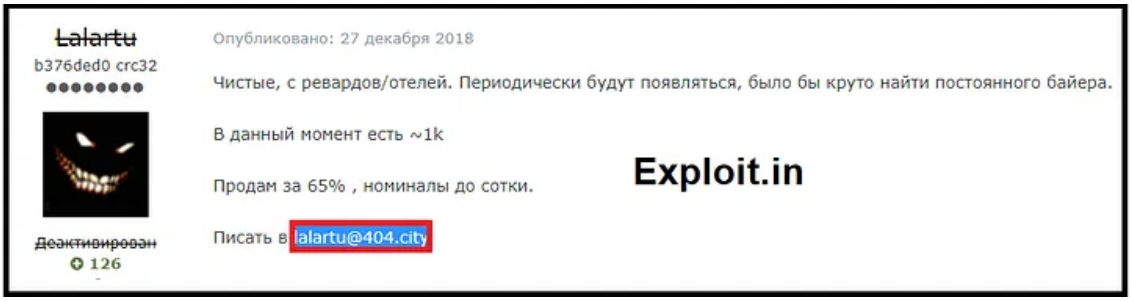
Earnings of almost $500,000 were posted by Lalartu in total.

I decided to investigate Lalartu and see who is the person behind that scary avatar.

First I figured out that Lalartu posted the picture above via an exclusive hacking forum named Exploit.in where Russian hackers hang out and sell different illegal services to each other.

I noticed Lalartu's account was banned on the forum for some reason but I could still view his old threads.

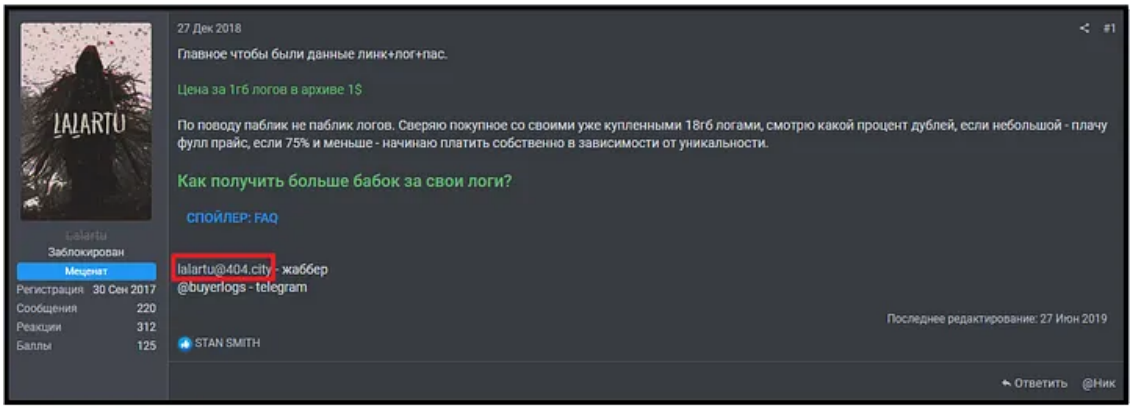
Press enter or click to view image in full size



I found Lalartu was using the XMPP address "Lalartu@404.city" and wanted to find other forums Lalartu is active in, considering his banned Exploit.in account won't help me much.

I looked for that specific XMPP in several hacking forums until I got a match.

Press enter or click to view image in full size



Lalartu's XMPP was found in another Russian hacking forum named BHF.io.

I knew it had to be the same person and not a different one using the same username because an XMPP address can only be used by one person unlike a username.

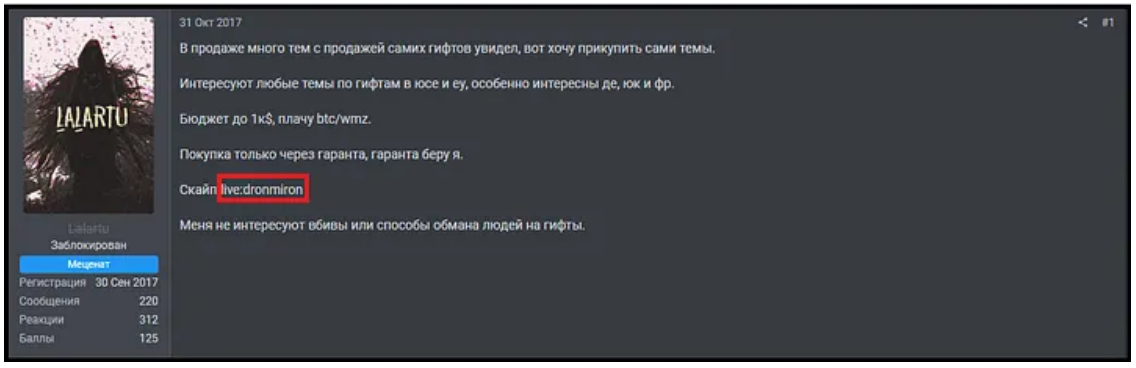
I noticed Lalartu is banned on BHF.io as well and wanted to figure out why so I went to his latest thread dated August 25, 2019 and found this:

Press enter or click to view image in full size

Lalartu is essentially admitting to exit scamming and to having three more usernames on BHF (also banned): Protokol, Marka, and Eng_Fog.

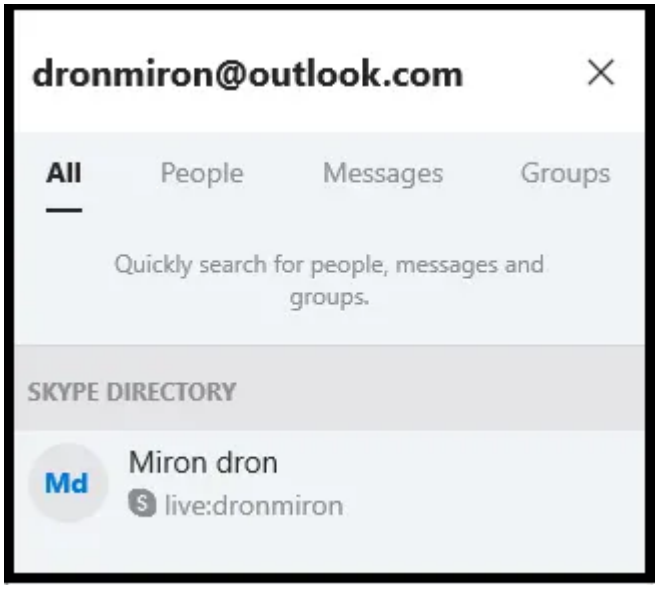
I didn't jump to conclusions and assumed Lalartu is telling the truth, he could be lying about those usernames which could belong to other people he wanted to bring down, so I kept looking at Lalartu's threads and found this:

Press enter or click to view image in full size

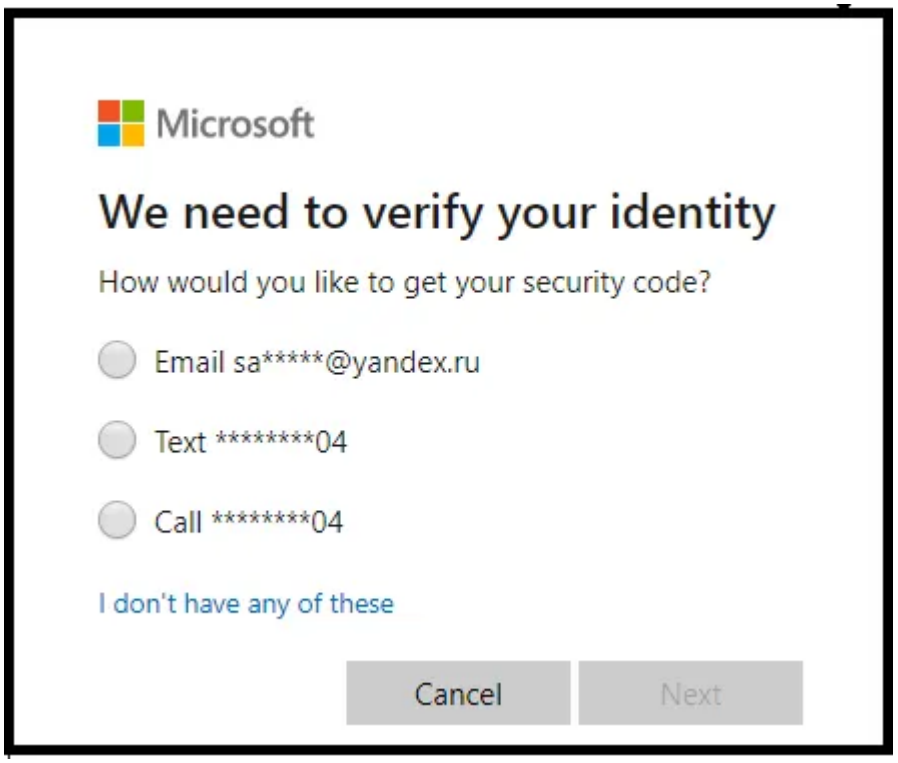


Lalartu is using the Skype live:dronmiron as a contact method. A somewhat known technique to find the email behind a username that has the word "live:" before it, is to try all of Hotmail's email domains in Skype's search field until you get a match displaying the username.

I found that the email behind that username is dronmiron@outlook.com:

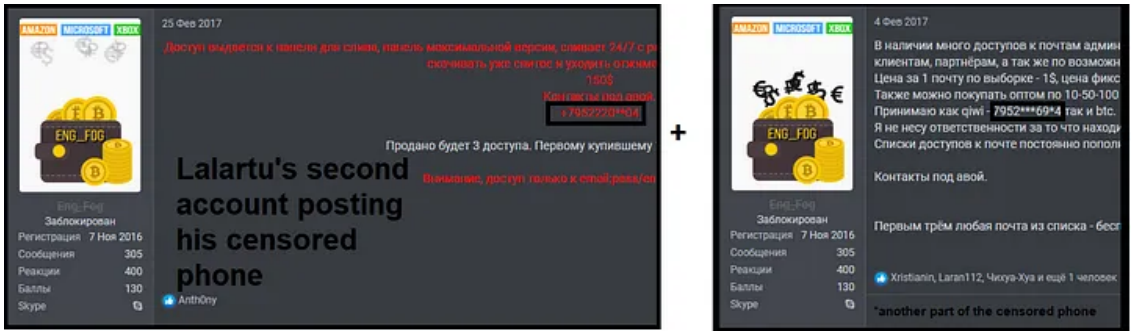


In order to find a censored email address used as a backup for this email address and a censored phone number connected to this email address, I began a password recovery process on Outlook.com and found Lalartu's phone number ends with 04:



The censored phone is great but I couldn't find it anywhere in Lalartu's threads so I looked up "Eng_Fog" on BHF.IO (Lalartu's alleged secondary account) and started looking at his old threads, I very quickly found out he was posting his censored phone on his sale threads in order for people to send him a private message in which he will give them the full number:

Press enter or click to view image in full size



being somewhat smart, Lalartu censored parts of the phone number but because he didn't remember which part he censored in every thread, I was able to piece the phone number together.

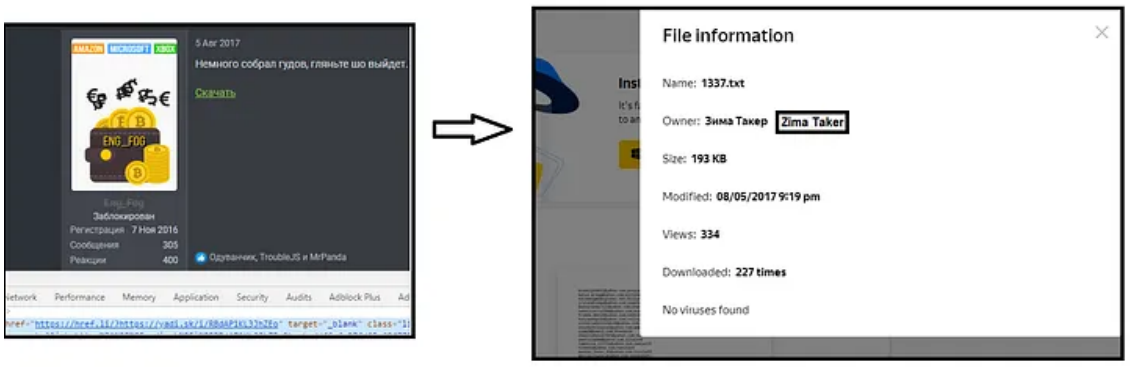
> 7952220**04 and +7952***69*4 = +79522206***04***.

The phone indeed ends with 04 like the one connected to Lalartu's outlook, this made it pretty clear that Lalartu wasn't lying about his other accounts.

I kept investigating both Lalartu's and Eng_Fog's threads and noticed that at one point Eng_Fog posted a thread leading to a Yandex Disk download page with a file he wanted people to download.

This is great because most file uploading sites keep metadata:

Press enter or click to view image in full size



As can be seen in the photo, under file information, Yandex kept the owner's name, which when translated from Russian is "Zima Taker"

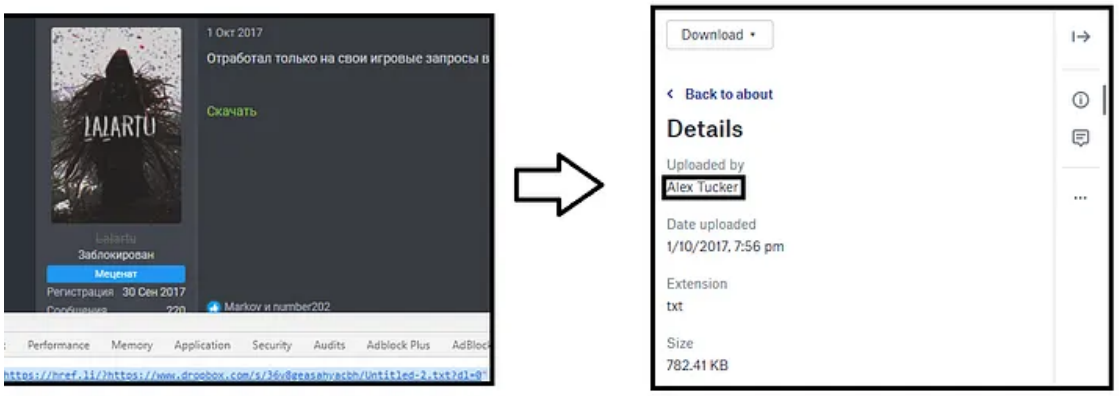
Get Alon Gal — Under the Breach's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

I decided to see if Lalartu had any similar threads, he did:

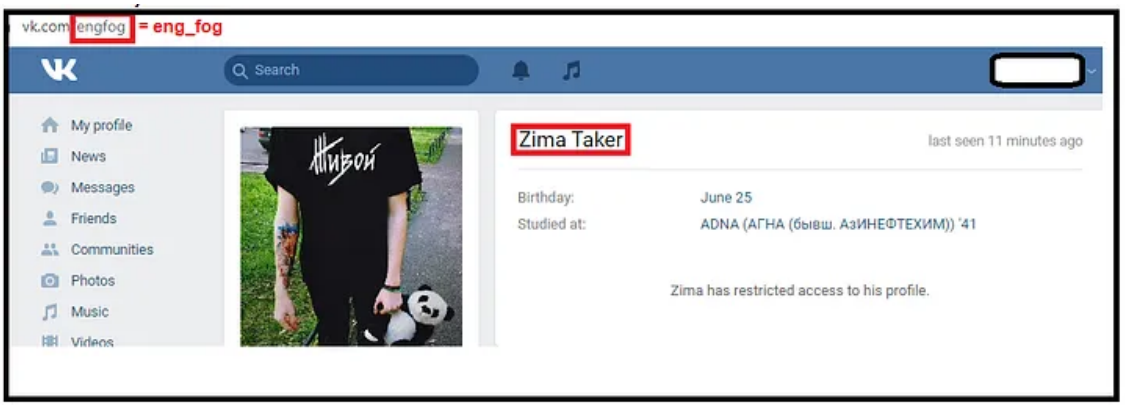
Press enter or click to view image in full size



This time from Dropbox and it says the file was uploaded by an “Alex Tucker”.

when looking up “Eng_Fog” on Yandex’s search engine, which is way better when looking for Russians than Google, I found a VK profile in the url [https://www.vk.com/**engfog**](https://www.vk.com/engfog). it belongs to a person named Zima Taker!

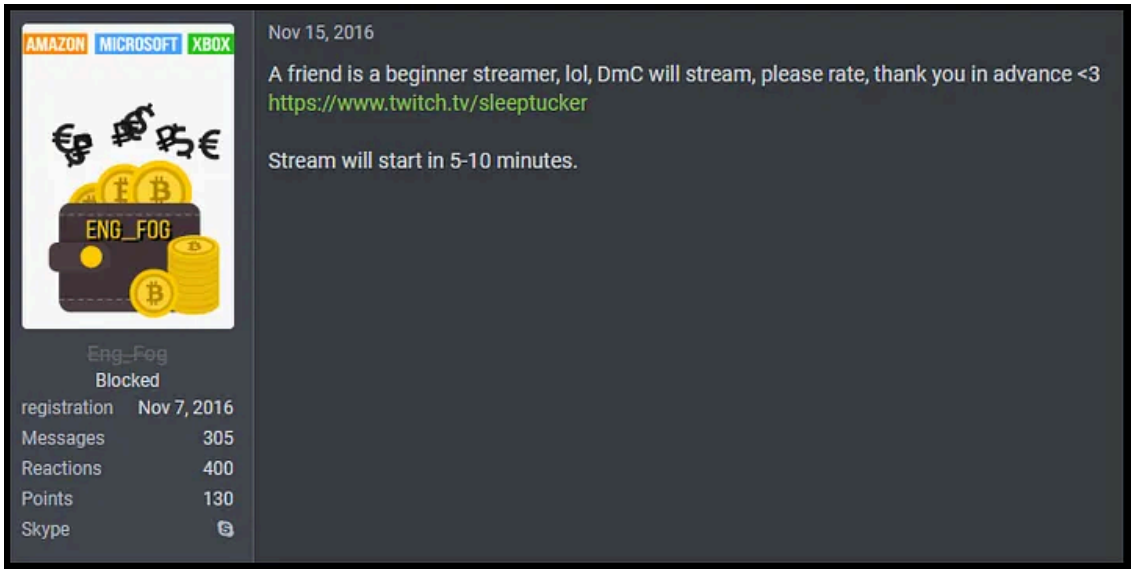
Press enter or click to view image in full size



I figured it could be him, but what about that “Alex Tucker” name?

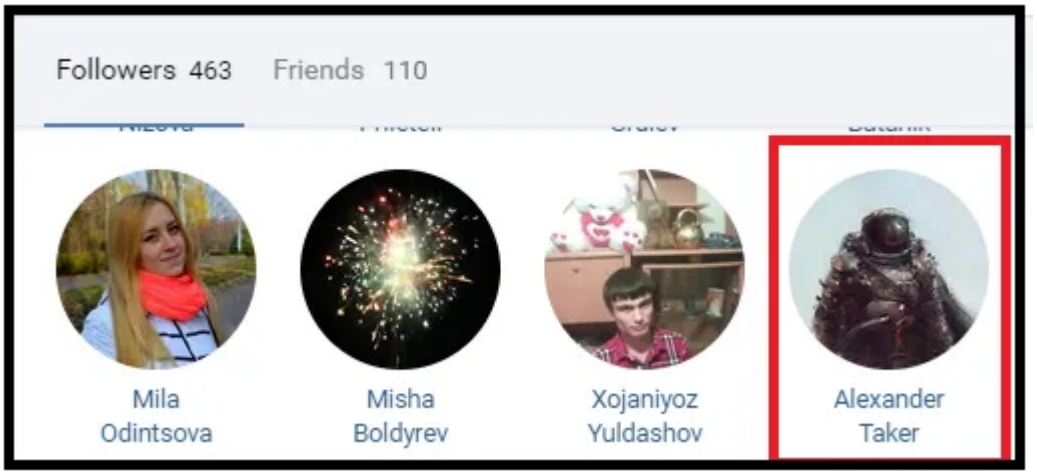
Well I found a thread posted by Eng_Fog asking to watch a Twitch stream of his friend:

Press enter or click to view image in full size



In her Twitch profile, SleepTucker linked her VK account in the url [https://www.vk.com/sleeptucker.](https://www.vk.com/sleeptucker)

I examined her followers and found this:



One of her followers is named Alexander Taker, similar to the person who uploaded the Dropbox file, I am now torn between two options: Lalartu could either be Alexander Taker or Zima Taker and I can't really know the answer.

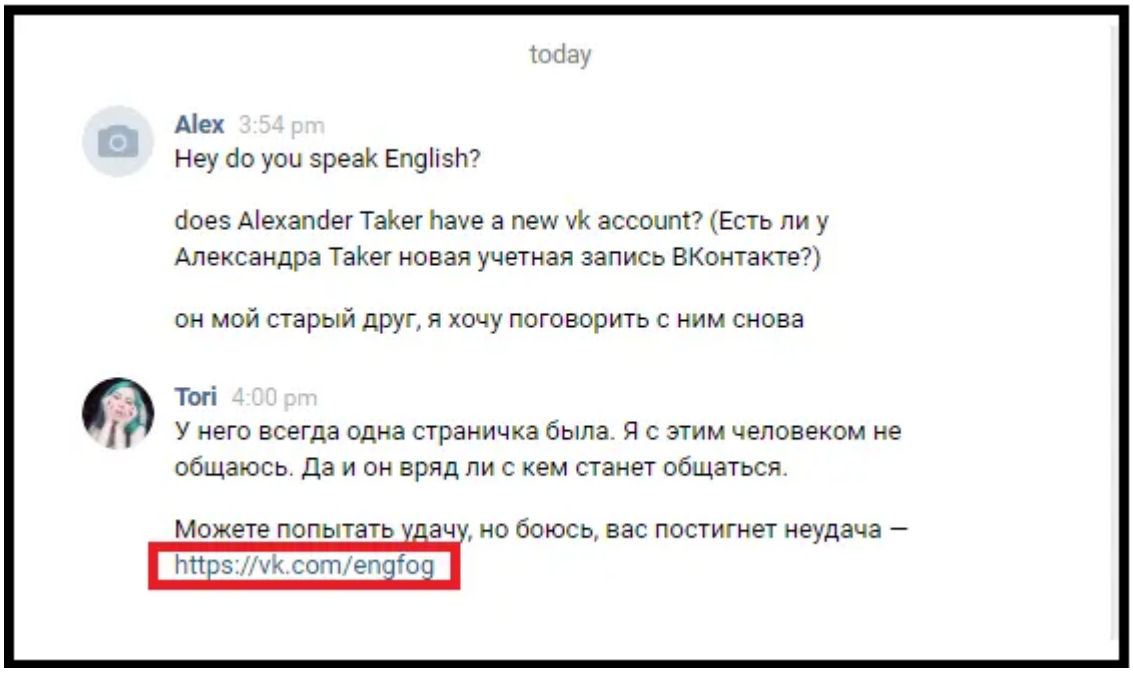
That is unless I recalled a smart person once said:

" There is no technology today that cannot be defeated by social engineering." — Frank Abagnale

I decided I will try contacting the Twitch streamer who could potentially still be in touch with the real Lalartu who posted a thread sharing her twitch account.

Despite my poor Russian, I had Google Translate and some Hutzpa.

I sent her a message asking if she still knows Alexander Taker, considering I knew he was following her, and asked where I can contact him by claiming I was an old friend of his who wanted to get back in touch again:



To my surprise she literally replied to me with his updated profile, https://www.vk.com/engfog, the same profile I contemplated whether it belonged to him!

Social Engineering truly never fails.

So now I know that the identity behind Lalartu is a Russian person named Alexander Taker who also goes by the nickname “Zima”.

Tori warned me that he might not be friendly towards me considering we haven’t talked in a long time so I stopped my effort to reunite with my old pal…

In conclusion —

We learned several OSINT methods to find our target’s real identity:

a. Grave-digging old posts belonging to the person.

b. Examining meta data.

c. Finding emails behind Skype usernames.

d. Finding censored emails and phones connected to an email address.

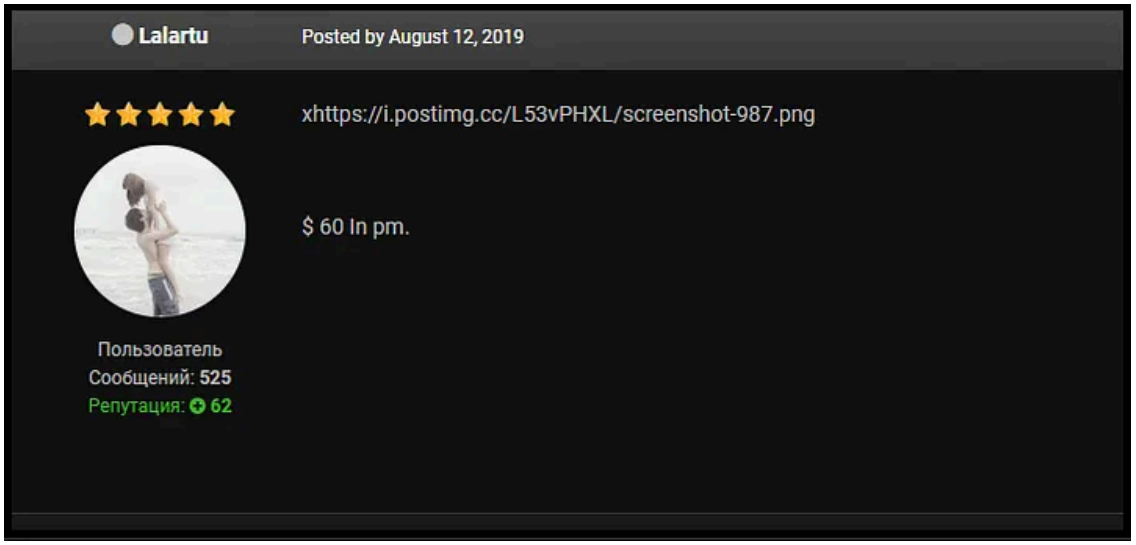
e. Utilizing Social Engineering.

And this is just OSINT in a nutshell, there are still many unique and interesting methods I use and would love sharing if I see posts like this spark the interests of people.

***I would also like to mention that in the McAfee report the researchers display Lalartu as a serious threat actor who earned almost $500,000 from his Ransomware activities but considering that in my research I found he was banned for scamming with over 8 different identities and I’ll add that he posted a sales thread**

trying to earn himself “merely” $60, I would conclude that he is just a sophisticated scammer who fabricated the photo of his earnings and nothing else.

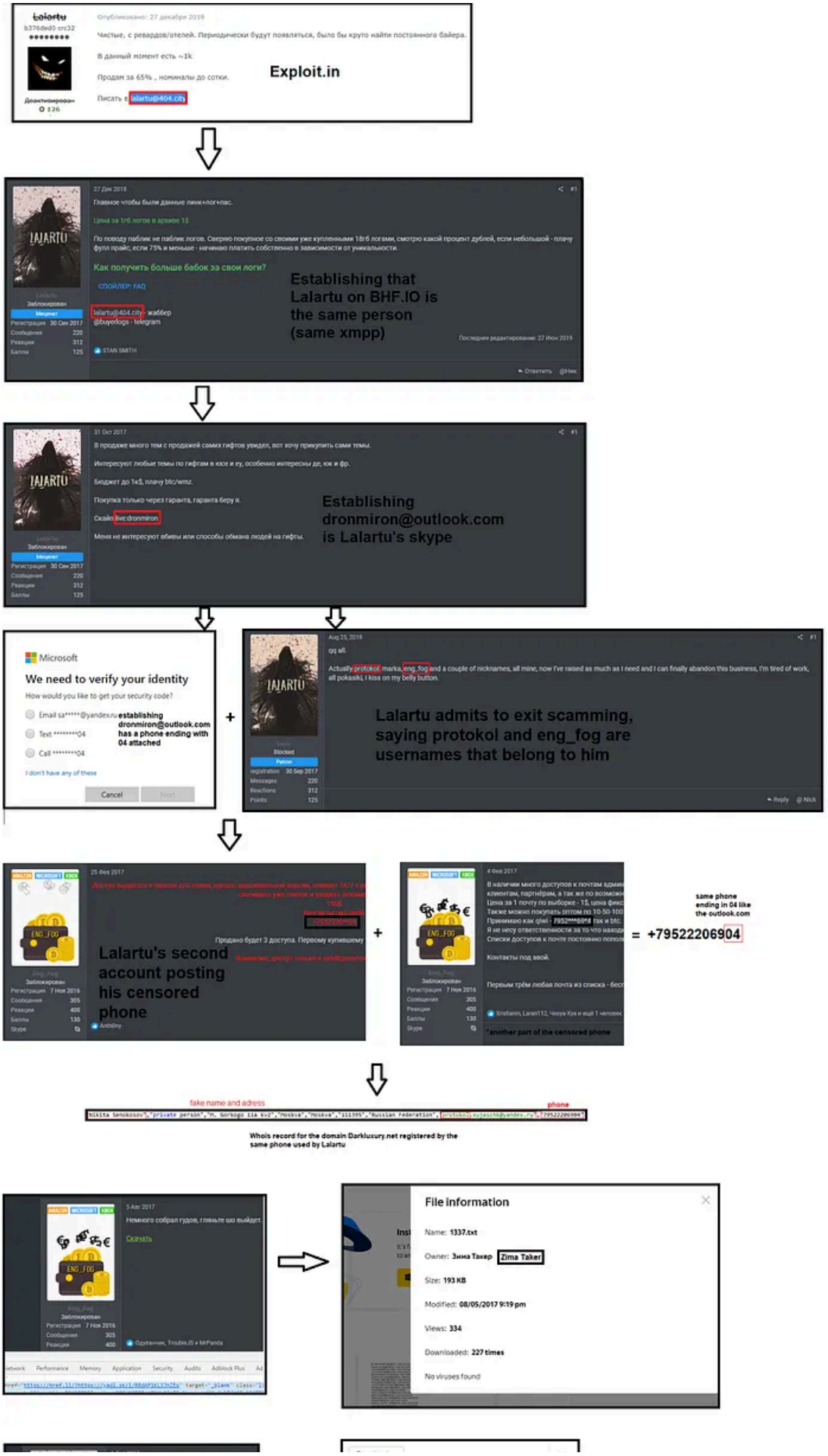
Press enter or click to view image in full size

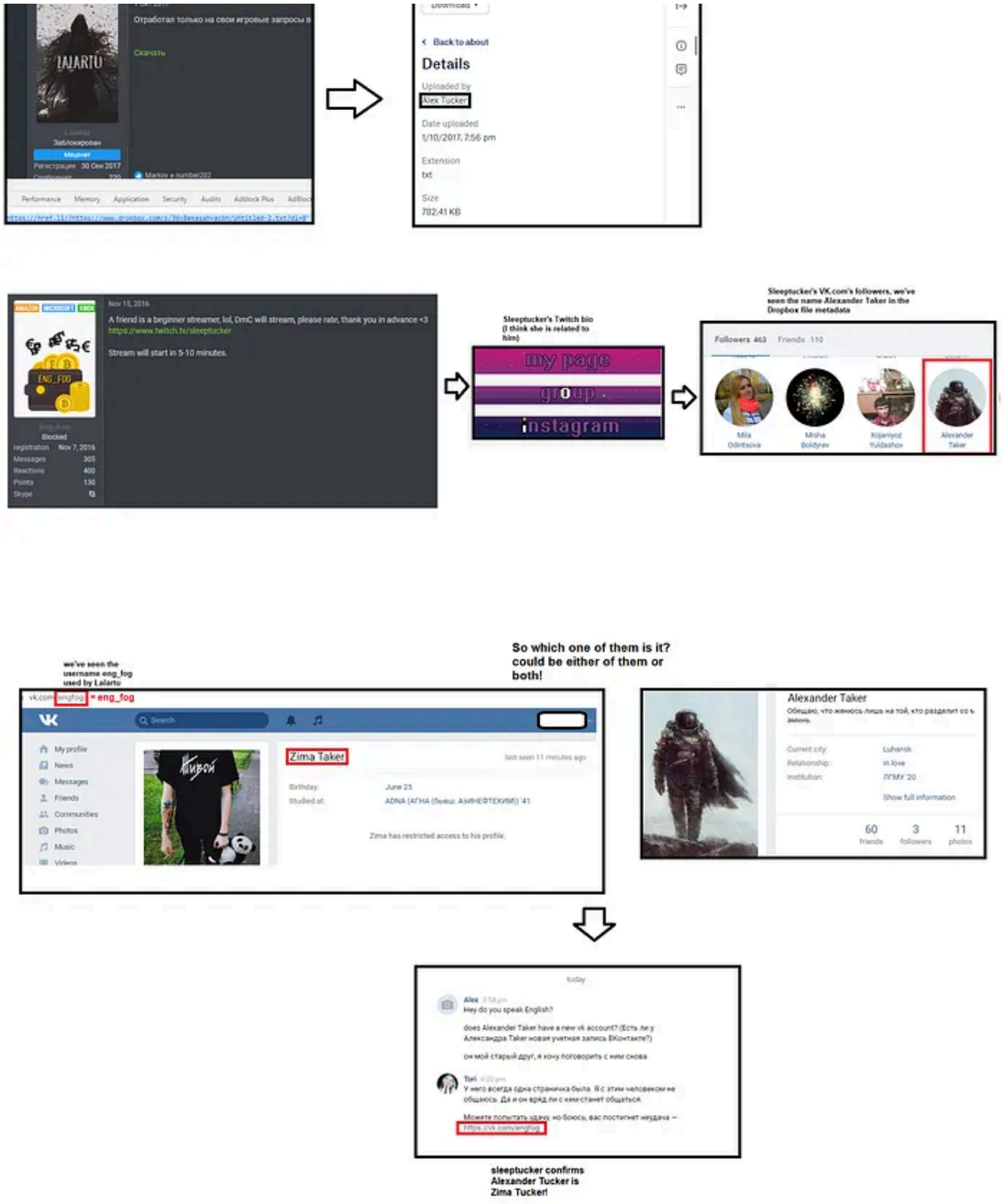


It is worth mentioning this thread is dated August 12, 2019 while Lalartu’s revenue thread is dated June 4, 2019 so we can rule out the option that Lalartu just started making a lot of money very fast after his scamming sprees.

If you’re too lazy to read the whole thing here is a graph displaying it without much to read

Press enter or click to view image in full size


Exploit.in
Establishing that Lalartu on BHF.IO is the same person (same xmpp)
Establishing dronmiron@outlook.com is Lalartu's skype
We need to verify your identity
establishing dronmiron@outlook.com has a phone ending with 04 attached
Lalartu admits to exit scamming, saying protokol and eng_fog are usernames that belong to him
Lalartu's second account posting his censored phone
same phone ending in 04 like the outlook.com
= +79522206904
fake name and adress
phone
Whois record for the domain Darkluxury.net registered by the same phone used by Lalartu
File information
Name: 1337.txt
Owner: Зима Такер
Zima Taker
Size: 193 KB
Modified: 08/05/2017 9:19 pm
Views: 334
Downloaded: 227 times
No viruses found



Connect with me — https://www.linkedin.com/in/alon-gal-utb/

References:

1. https://www.kpn.com/security-blogs/Tracking-REvil.htm
2. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-follow-the-money/
