

/var/log/notes

 ropgadget.com/posts/originlogger.html

20DEC2023 - The Origin of OriginLogger & Agent Tesla

By Jeff White (karttoon)

After I published a blog at \$dayjob on how I came to realize that what I thought was a sample of Agent Tesla turned out to actually be a new malware called OriginLogger, a fellow threat researcher botlabsDev reached out some months later. They had noticed that the two GitHub repositories I referenced for the profile "0xFD3" each had a commit from a different account which exposed some new e-mail addresses to pivot on. Holy shit. I was unaware this was even a thing so looking into this further showed that each repository received an update from a different account on the same days the respective code was initially committed. This crucial piece of info took me down a fun little rabbit hole that I wanted to share wherein I was able to identify an individual who may be the developer behind one of the most prominent keylogger malware families - OriginLogger and Agent Tesla.

Starting with the two GitHub repositories, I wanted to show both of the commit logs and the connections that resulted from them.

For the first one, Chrome-Password-Recovery, we see a commit by "Omer Demir" with an e-mail address of "omer.demir-@hotmail.com" on March 11th, 2020. This was six months before the builder I found in the original blog, which was compiled in 2020 as well and that authenticated against the domain which led me to this GitHub profile originally.

```
Chrome-Password-Recovery $ git log commit
5d0c09a9c3e23004a08017dfc916196ac8971983 (HEAD -> master, origin/master,
origin/HEAD) Author: Omer Demir <33671489+0Fdemir@users.noreply.github.com> Date:
Wed Mar 11 04:23:11 2020 +0300 Update README.md commit
305ef43b4b138660bdfd1cdee638cce47e487769 Author: Omer Demir <omer.demir-
@hotmail.com> Date: Wed Mar 11 04:14:39 2020 +0300 first commit commit
ffbe0189c30804844e767dcfc2fa38aef1813b1d Author: Omer Demir
<33671489+0Fdemir@users.noreply.github.com> Date: Wed Mar 11 03:50:52 2020 +0300
Initial commit
```

Checking the e-mail against the usual database leak sites revealed that the e-mail has been observed in breaches for "ledger.com", "leet.cc", and Tumblr. This also provided a bit more information about the account - specifically a middle name, address, and phone number located in Turkey. This is an important piece of information as will be discussed shortly.

Name Omer Faruk Demir Email omer.demir-@hotmail.com Address Miralay Rafet Sokak
34360 Istanbul Turkey Phone 5464200269

For the other repository, OutlookPasswordRecovery, there is a commit by account "0Fdemir" with the e-mail "ssfenks@windowslive.com" on the 15th of November, 2017 - three years prior to the above. At this point, seeing the "0Fdemir" moniker and recalling the "0xfd3" one, I realized the hex code used is representative of "Omer Faruk Daemir" or "0xFD". Definitely a cool moniker in my book but more importantly it links both accounts.

```
OutlookPasswordRecovery $ git log commit c6816ce933dd42d81048e658a58720f9f1f75cb3  
(HEAD -> master, origin/master, origin/HEAD) Author: 0Fdemir  
<33671489+0Fdemir@users.noreply.github.com> Date: Wed Nov 15 01:00:06 2017 +0300  
Update README.md commit 0f5208d79a3178c1e45ebbcf8afac19298374741 Author:  
0Fdemir <33671489+0Fdemir@users.noreply.github.com> Date: Wed Nov 15 00:44:03 2017  
+0300 Update README.md commit b459361e74b28584ef487d4929f5707663055265  
Author: 0Fdemir <33671489+0Fdemir@users.noreply.github.com> Date: Wed Nov 15  
00:43:39 2017 +0300 Update REEDME.md commit  
67b9632d6bf147eb5ccec3e4f7fb8a8a0bee7d3d Author: 0Fdemir  
<ssfenks@windowslive.com> Date: Wed Nov 15 00:42:38 2017 +0300 nocommit commit  
f431ace4378c2db84e14f59cc3086b6eee4dd09d Author: 0Fdemir  
<33671489+0Fdemir@users.noreply.github.com> Date: Wed Nov 15 00:37:19 2017 +0300  
Initial commit
```

This e-mail address is likewise observed in database leaks and was seen using the username of "agenttesla" from a forum dump.

In June 2015, two years prior to the aforementioned GitHub commit, I observed a post by user "sifenks", which is associated to the e-mail address "ssfenks@windowslive.com", to the "nulled.cr" forum titled "[FREE] [FUD] Agent Tesla Keylogger [Beta]". The post is an advertisement for an early version of Agent Telsa keylogger that could be downloaded at "<http://www.agenttesla.com/en/download/free/>". In the post, it also stated the following:

P.S.: Agent Tesla that my last project beta version with you! Please leave a message for requests , needs , bugs and errors. Program is tested. Each function working flawlessly. If you like and If you want to continuousness for Agent Tesla, please donate... Enjoy! P.S.2: Please close all AV! P.S.3: Please dont use Virustotal, jotti etc...

Focusing in on the wording here, Sifenks stated "my last project" and requests for users to message their account for "requests , needs , bugs and errors". This implies to me that the Sifenks account is a developer.

Going back a little further, this user was also observed in 2014 posting an earlier version of Agent Tesla on the hackforums.net website wherein they quickly responded to users and fixed bugs in the code that they found. One consumer of Agent Tesla posted "Before i talk

with my error, i have to say sifenks is the most active person that responds to your problems! All in the other keyloggers, the keylogger creator hasn't spoke once!".



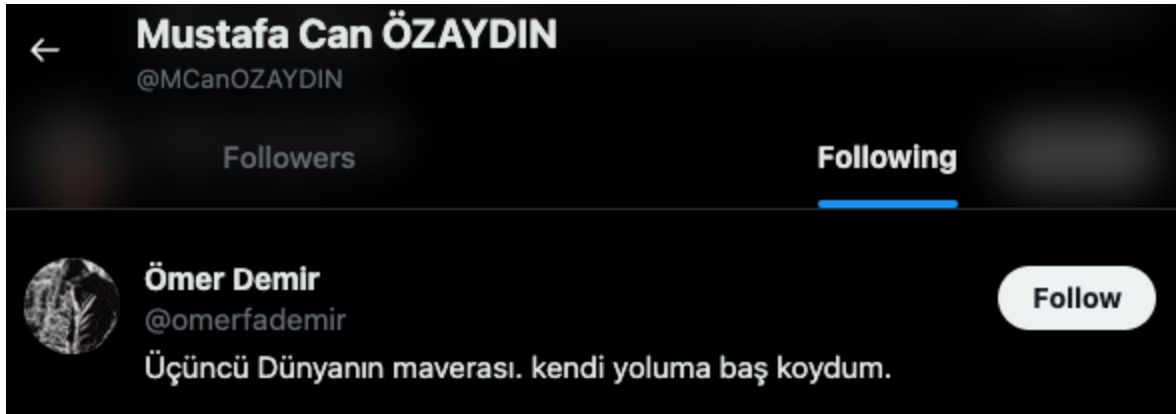
In 2018, a few months before Agent Tesla announced they were closing up shop and to instead use OriginLogger, Brian Krebs released an article titled "[Who is Agent Tesla?](#)" in which he details that the earlier version of Agent Tesla, in 2014, was made available on a Turkish-language WordPress site ("agenttesla.wordpress.com") before they eventually migrated to "agenttesla.com". Brian reported that the subsequent domain was registered in 2014 by a person named "Mustafa can Ozaydin" in Antalya, Turkey who used the e-mail address "mcanozaydin@gmail.com" before they were hidden behind WHOIS privacy services in 2016.

I'll be honest and say that it was a bit of an emotional roller coaster researching this and then finding out Krebs had written an article years ago about the very same topic. D'oh! As I started to read it though, I realized it's an entirely different person...What the hell? Brian's research here was solid, I recreated his steps and it all seemingly lined up so I was left wondering who the heck this other guy was and how he related to mine. It turned from a simple OSINT attribution exercise into a proper mystery.

In Brian's research he linked the Gmail address that registered the domain to a YouTube account by a Turkish individual with the same name who uploaded *tutorials* on using the Agent Telsa web panel. Brian went on to state that the *administrator* of the *24x7 live support channel for Agent Tesla* had the same profile picture as a Twitter account "[MCanOZAYDIN](#)".

This information was used to eventually identify [Mustafa's LinkedIn profile](#). This profile listed Mustafa as a "systems support expert" for a hospital in Istanbul, Turkey at the time of his writing.

I decided to see if I could find any social media profiles for Omer and started by looking at Mustafa's Twitter account. One of the things I like to do when researching Twitter accounts is to look at the followers and following, which are displayed in the order in which they followed. It was a win in this scenario and one of the early accounts followed by Mustafa is for an [Omer Demir](#).



Pivoting off of this account name "omerfademir" led me to a [Facebook profile](#) with the same profile picture (uncropped) and name.

About

Overview

Work and education

Places lived

Contact and basic info

Family and relationships

Details About Ömer

Life events



Self-Employed

January 3, 2014 to present



Studied at **Anadolu University**



Lives in **Istanbul, Turkey**



From **Samsun**



No relationship info to show

Photos

Ömer's Photos

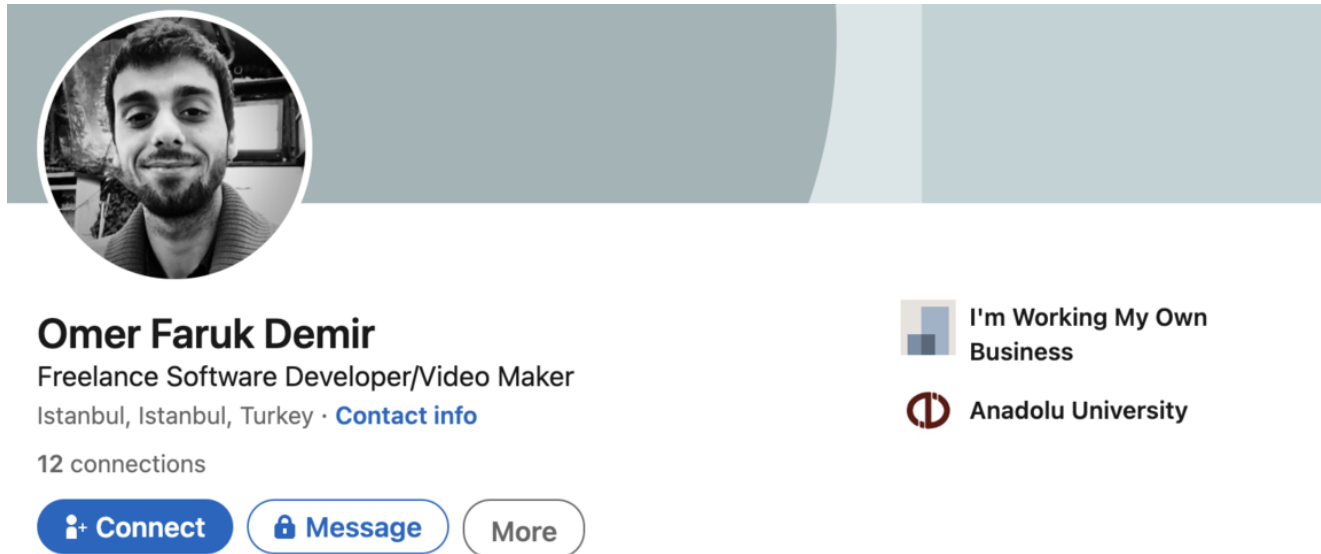
Albums



A couple of interesting points to note, even if the profile is otherwise light on information. He listed self-employment in 2014, the year that Agent Tesla came out, and he studied at Anadolu University. Mustafa's LinkedIn also showed that he attended Anadolu University and both men started the same year in 2013. Taking it a step further with that connection, in one of the previously mentioned forum posts by the "sifenks" account, which was advertising an early version of Agent Tesla in 2015, a user reported a bug that stated they were receiving the following message - "The remote name could not be resolved: '48982689868.home.anadolu.edu.tr". It's unknown if they knew each other before college, but it stands to reason they knew each other while at university.

The profile also provides a clearer picture of the individual with additional photos and stated they were from Samsun, narrowing down the geography.

This led me back to LinkedIn to see if I could find a profile there with all of this new information. Filtering by "Omer Faruk Demir" resulted in 182 hits, adding location to 51 hits, and then alumni from Anadolu University to 18 hits. With the remaining hits, visual inspection and relative age comparison I was able to find his account. It provides a bit more background information, such as skills and knowledge, but further solidified the link to the Facebook profile and closed the loop.





The image shows a LinkedIn profile header for Omer Faruk Demir. On the left is a circular profile picture of a man with a beard and short dark hair, smiling. To the right of the picture is a light blue banner. Below the banner, the name "Omer Faruk Demir" is displayed in bold black text. Underneath the name is the job title "Freelance Software Developer/Video Maker" and the location "Istanbul, Istanbul, Turkey" followed by a blue link for "Contact info". Below this is the text "12 connections". At the bottom of the header are three buttons: a blue "Connect" button with a plus icon, a blue "Message" button with a lock icon, and a white "More" button with a blue border.

Omer Faruk Demir
Freelance Software Developer/Video Maker
Istanbul, Istanbul, Turkey · [Contact info](#)

12 connections

[Connect](#) [Message](#) [More](#)

 I'm Working My Own Business
 Anadolu University

About

I was born on August 22, 1993 in Samsun. I started my software adventure by learning VB.NET in 2009. At the same time, I had the opportunity to improve myself in the fields of T-SQL and SQL Server management since I was a department at Vocational High School. I've been developing desktop software with C# since 2010. I learned the basics of C# and ASP.NET. Since I love to do the coding job, most of my day is spent on my computer. In 2012, I started to develop web software with PHP. I strive to constantly improve myself in software, follow innovations and learn new coding languages. I started learning web programming with ASP.NET MVC in early 2017. Besides these; Due to my deep admiration and curiosity for cinema, I started to deal with video shooting and editing in 2010. I have been dealing with video works for about 6 years. Besides producing various personal projects, I also worked for different institutions/organizations.

Specifically, the timing they both attended Anadolu University, hailing from Samsun, studying in the languages used by Agent Tesla and OriginLogger, and finally the way the career experience is listed on both sites.

Experience



Software Developer

I'm Working My Own Business

Oct 2014 - Present · 8 yrs

Turkey

- Desktop software development (C#.NET, VB.NET) - Web API integration - Cryptocurrency automatic payment system - Web software - Technical support

Work



Self-Employed

January 3, 2014 - Present

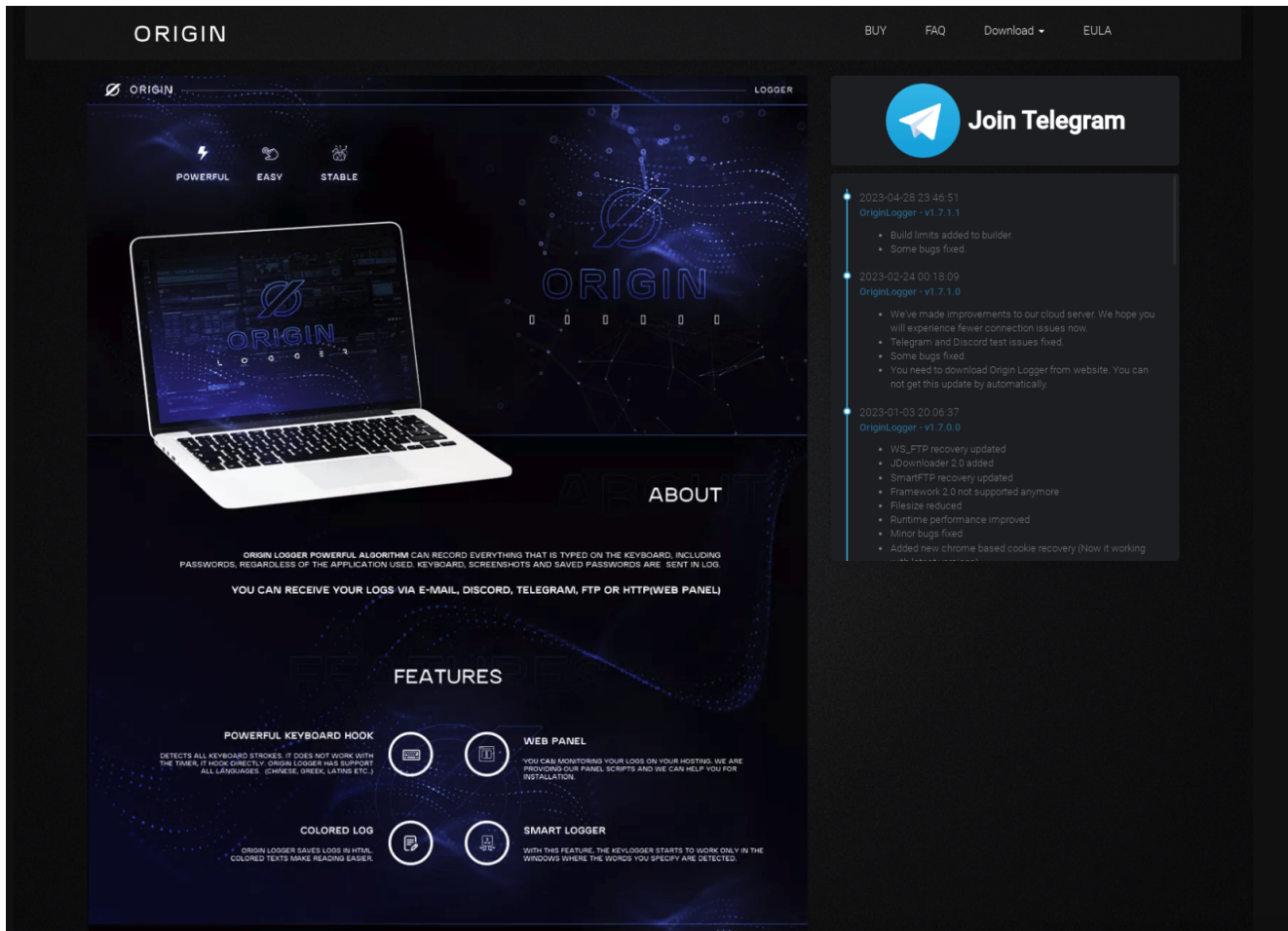
Desktop software Web software API integration

Comparing the LinkedIn for each individual, I'd say Mustafa's work experience shows him in more of a support role and less focused on development or coding whereas Omer's shows he has the skills and knowledge necessary to write the code for Agent Tesla and OriginLogger.

Based on this, I would surmise that Mustafa may have acted more in a support capacity for Agent Tesla, maybe keeping the business side running smoothly while Ömer worked on developing the malware itself. Once the Brian Krebs article came out and Agent Tesla suddenly closed down a few months later, it would appear Omer used the code to continue development under a new brand - OriginLogger.

Not too long after my blog came out, OriginLogger added a new exfiltration method for Discord...and then...silence. Updates stopped, the marketplaces to purchase it vanished, good and bad guys alike were asking "does anyone know where to find this??", and then the builder got pirated.

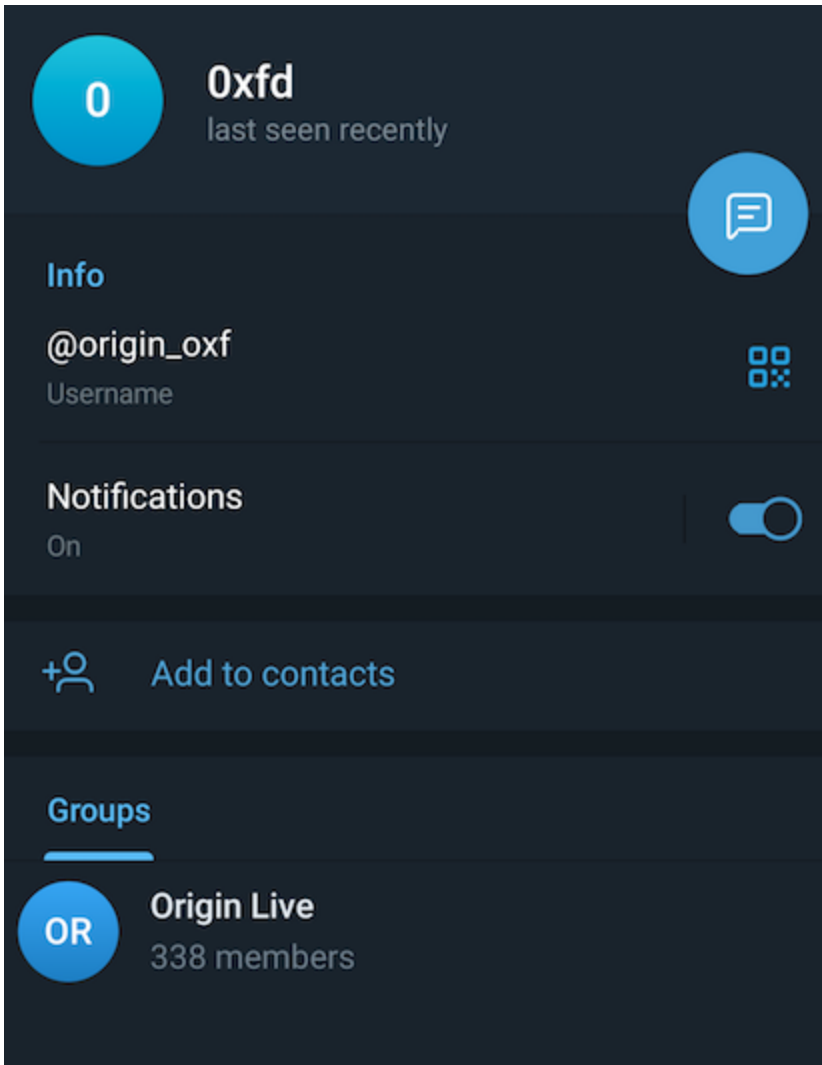
Fast-forward to late September 2023, it re-emerges on my radar at a new marketplace site - <http://originpro.nl>.



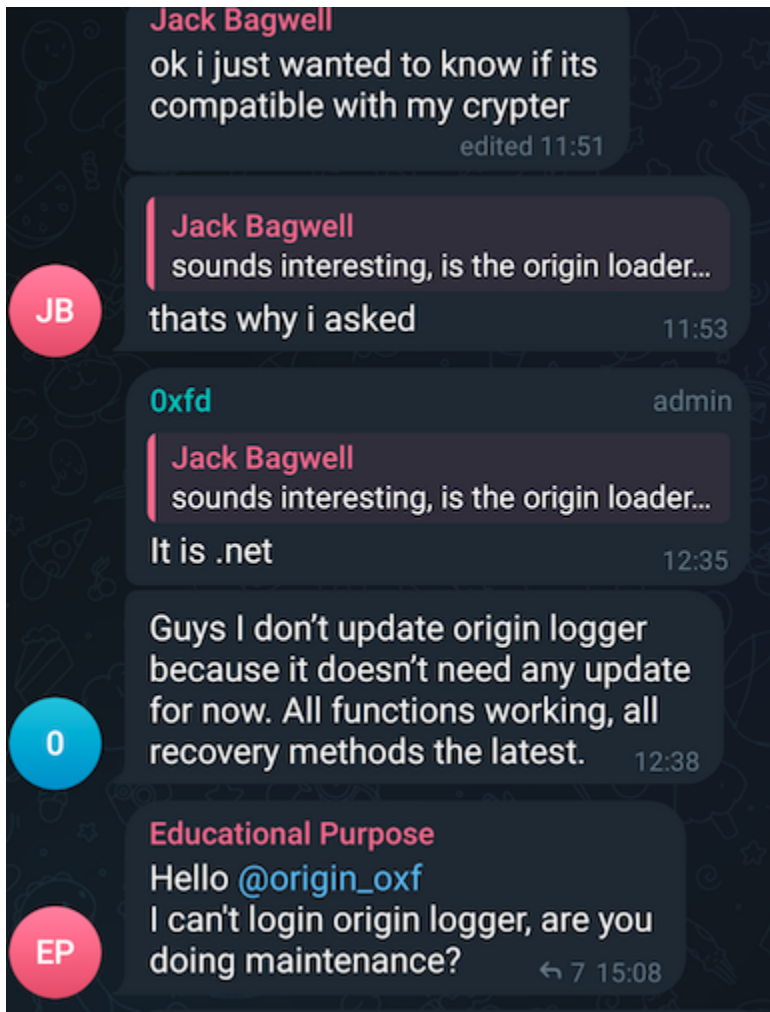
Note the giant "Join Telegram" button they've added to the new marketplace site? Of course fam.



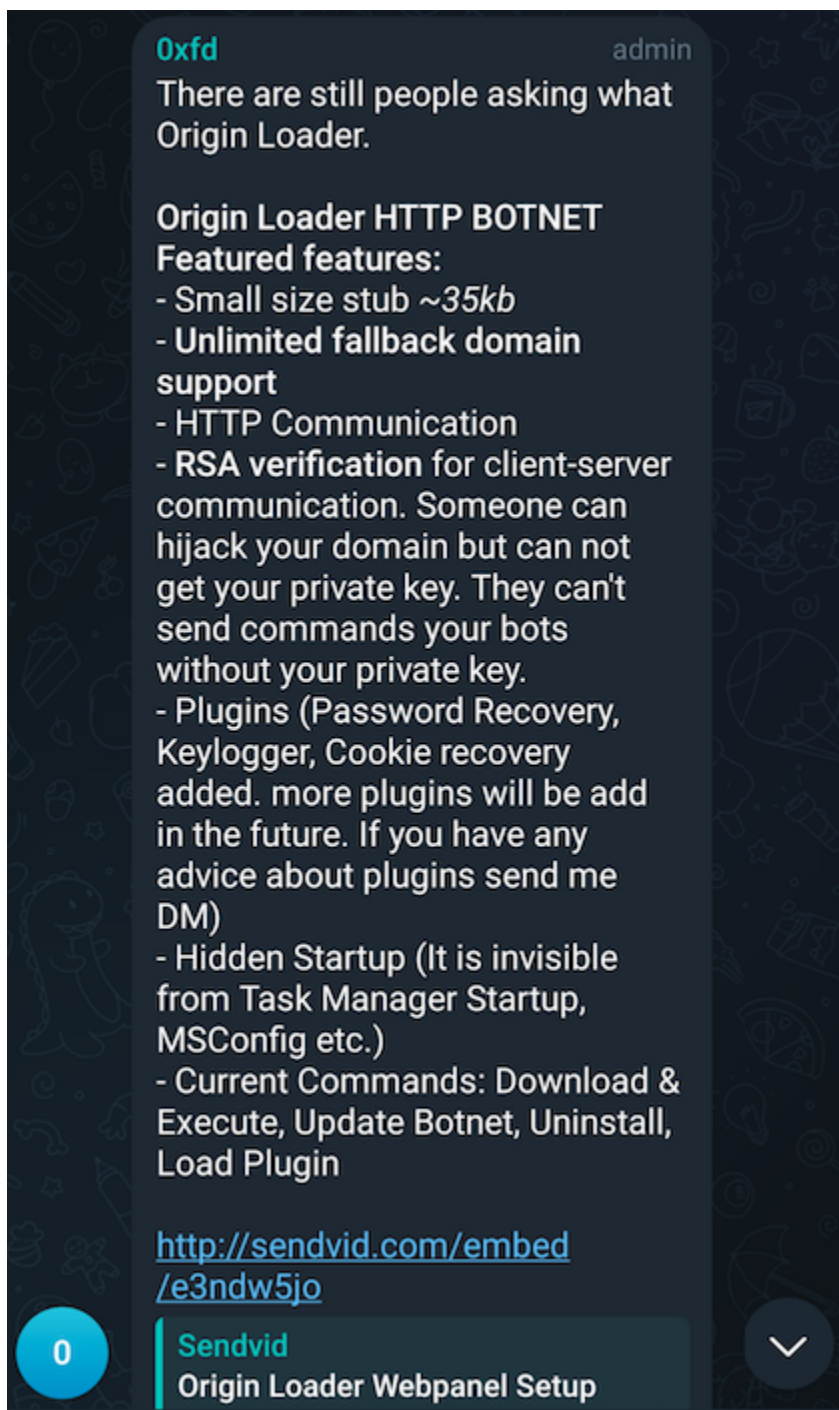
Everyone will be shocked to see the admin is none other than the one and only 0xFD aka Omer Faruk Demir. :surprised_pikachu: But, if nothing else, at least they are done hiding now which helps connect all of the other research together.



I spent a few days reading through the chat history and found a couple of nuggets I'll share. The first one is that OxFD states there have been no updates to OriginLogger because its feature complete.



So what's 0xFD been up to if not working on OriginLogger then? Apparently a new product called "OriginLoader" which is touted as an HTTP based botnet that comes complete with keylogging and all the usual bells and whistles.

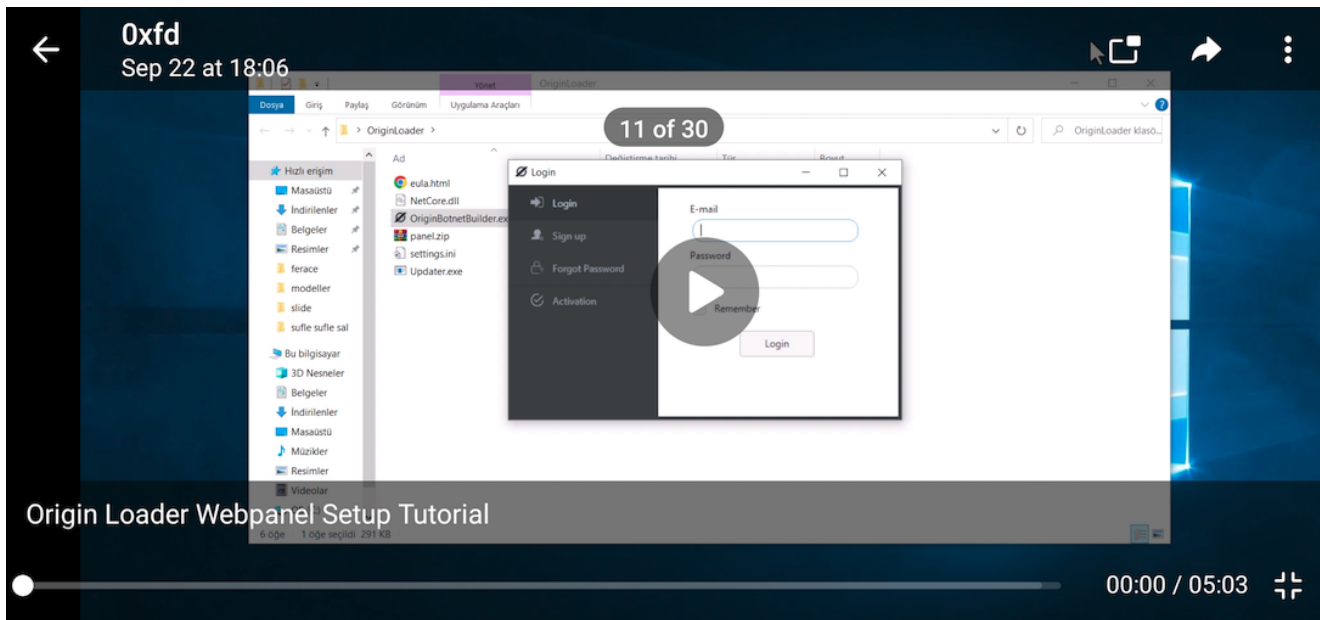


OxFD doesn't like when people don't understand the difference between these two products and has to break it down repeatedly for potential customers. They are also very fond of crowdsourcing ideas for new features to add to either product. At this point, it's a hallmark of their character - always placing the customer first.

OriginLoader will be one to keep an eye on and see if it continues to evolve and be as successful as the other products.

Finally, in one post they share a video on installing the panel for OriginLoader and within the video, every instance where they open the file explorer is blurred out...except the very first frame of the video :facepalm:. It shows the file names for OriginLoader and further

strengthens the idea that the developer is someone of Turkish origin due to the language pack.



Annnnd that's a wrap! It was a fun OSINT rabbit hole to go down...*gets on soapbox* now please stop calling OriginLogger Agent Tesla.

[Older posts...](#)