REvil Ransom Arrest, $6M Seizure, and $10M Reward

krebsonsecurity.com/2021/11/revil-ransom-arrest-6m-seizure-and-10m-reward/

The U.S. Department of Justice today announced the arrest of Ukrainian man accused of deploying ransomware on behalf of the **REvil** ransomware gang, a Russian-speaking cybercriminal collective that has extorted hundreds of millions from victim organizations. The DOJ also said it had seized $6.1 million in cryptocurrency sent to another REvil affiliate, and that the **U.S. Department of State** is now offering up to $10 million for the name or location any key REvil leaders, and up to $5 million for information on REvil affiliates.

If it sounds unlikely that a normal Internet user could make millions of dollars unmasking the identities of REvil gang members, take heart and consider that the two men indicted as part this law enforcement action do not appear to have done much to separate their cybercriminal identities from their real-life selves.

Exhibit #1: **Yaroslav Vasinskyi**, the 22-year-old Ukrainian national accused of being REvil Affiliate #22. Vasinskyi was arrested Oct. 8 in Poland, which maintains an extradition treaty with the United States. Prosecutors say Vasinskyi was involved in a number of REvil ransomware attacks, including the July 2021 attack against **Kaseya**, a Miami-based company whose products help system administrators manage large networks remotely.

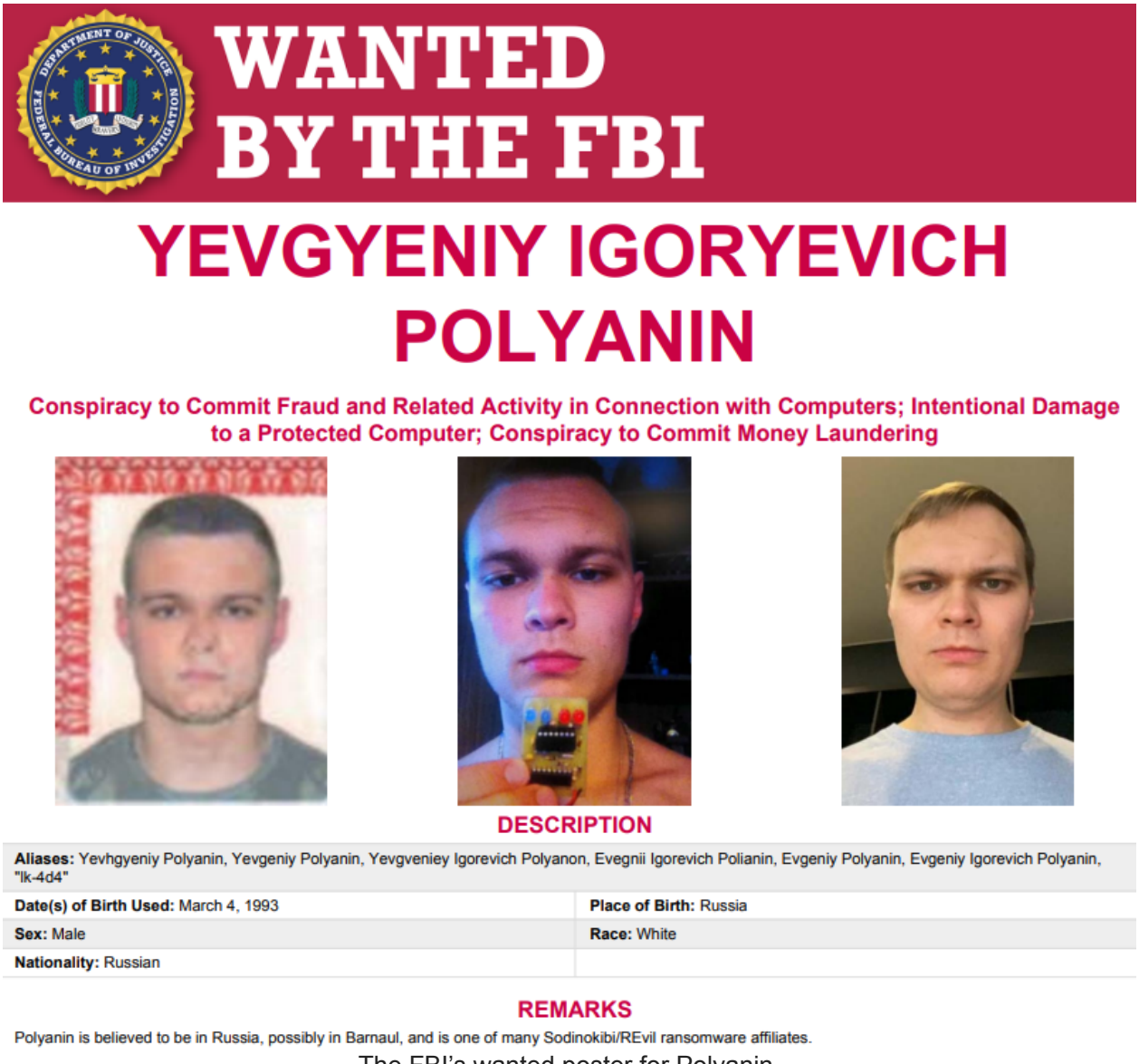
Yaroslav Vasinksyi's Vkontakte profile reads "If they tell you nasty things about me, believe every word."

According to his indictment (PDF), Vasinskyi used a variety of hacker handles, including "Profcomserv" — the nickname behind an online service that floods phone numbers with junk calls for a fee. Prosecutors say Vasinskyi also used the monikers "**Yarik45**," and "**Yaroslav2468**."

These last two nicknames correspond to accounts on several top cybercrime forums way back in 2013, where a user named "Yaroslav2468" registered using the email address **yarik45@gmail.com**.

That email address was used to register an account at **Vkontakte** (the Russian version of Facebook/Meta) under the profile name of "Yaroslav 'sell the blood of css' Vasinskyi." Vasinskyi's Vkontakte profile says his current city as of Oct. 3 was Lublin, Poland. Perhaps tauntingly, Vasinskyi's profile page also lists the FBI's 1-800 tip line as his contact phone number. He's now in custody in Poland, awaiting extradition to the United States.

Exhibit #2: **Yevgeniy Igorevich Polyanin**, the 28-year-old Russian national who is alleged to be REvil Affiliate #23. The DOJ said it seized $6.1 million in funds traceable to alleged ransom payments received by Polyanin, and that the defendant had been involved in REvil ransomware attacks on multiple U.S. victim organizations.



WANTED BY THE FBI

YEVGYENIY IGORYEVICH POLYANIN

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Intentional Damage to a Protected Computer; Conspiracy to Commit Money Laundering

DESCRIPTION

Aliases: Yevhgyeniy Polyanin, Yevgeniy Polyanin, Yevgveniey Igorevich Polyanon, Evegnii Igorevich Polianin, Evgeniy Polyanin, Evgeniy Igorevich Polyanin, "lk-4d4"	
Date(s) of Birth Used: March 4, 1993	**Place of Birth:** Russia
Sex: Male	**Race:** White
Nationality: Russian	

REMARKS

Polyanin is believed to be in Russia, possibly in Barnaul, and is one of many Sodinokibi/REvil ransomware affiliates.

The FBI's wanted poster for Polyanin.

Polyanin's indictment (PDF) says he also favored numerous hacker handles, including **LK4D4**, **Damnating**, **Damn2life**, **Noolleds**, and **Antunpitre**. Some of these nicknames go back more than a decade on Russian cybercrime forums, many of which have been hacked and relieved of their user databases over the years.

Among those was carder[.]su, and that forum's database says a user by the name "Damnating" registered with the forum in 2008 using the email address **damnating@yandex.ru**. Sure enough, there is a Vkontakte profile tied to that email address under the name "Yevgeniy 'damn' Polyanin" from Barnaul, a city in the southern Siberian region of Russia.

The apparent lack of any real operational security by either of the accused here is so common that it is hardly remarkable. As exhibited by countless investigations in my Breadcrumbs story series, I have found that if a cybercriminal is active on multiple forums over more than 10 years, it is extremely likely that person has made multiple mistakes that make it relatively easy to connect his forum persona to his real-life identity.

As I explained earlier this year in The Wages of Password Re-use: Your Money or Your Life, it's possible in many cases to make that connection thanks to two factors. The biggest is password re-use by cybercriminals (yes, crooks are lazy, too). The other is that cybercriminal forums, services, etc. get hacked just about as much as everyone else on the Internet, and when they do their user databases can reveal some very valuable secrets and connections.

In conjunction with today's REvil action, the **U.S. Department of State** said it was offering a reward of up to $10 million for information leading to the identification or location of any individual holding a key leadership position in the REvil ransomware group. The department said it was also offering a reward of up to $5 million for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in a REvil ransomware incident.

I really like this bounty offer and I hope we see more just like it for other ransomware groups. Because as we can see from the prosecutions of both Polyanin and Vasinskyi, a lot of these guys simply aren't too hard to find. Let the games begin.