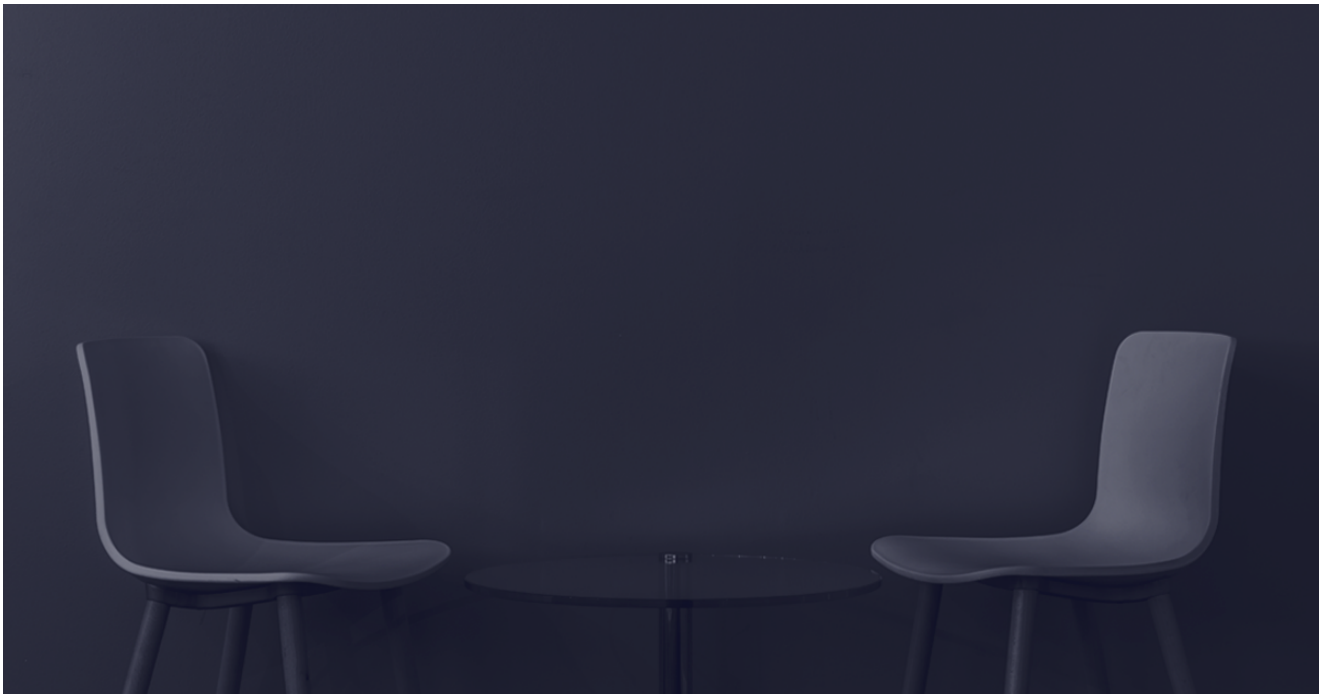
Russian hacker Q&A: An Interview With REvil-Affiliated Ransomware Contractor

flashpoint-intel.com/blog/interview-with-revil-affiliated-ransomware-contractor/

September 29, 2021



Blogs

Blog

A threat actor—who claims to work with REvil and other sophisticated ransomware collectives—recently spoke with Russian-language website Lenta[.]ru on the condition of anonymity.

A Different Mindset and Approach

A threat actor—who claims to work with REvil and other sophisticated ransomware collectives—recently spoke with Russian-language website Lenta[.]ru on the condition of anonymity.

This interview is a marked departure from a typical Q&A with a threat actor. Discussions between media and Russian-speaking ransomware operatives are generally filled with braggadocio emanating from the threat actor. To them, what they do is luxurious, anarcho-capitalist, cool, and lucrative; they may think of themselves as invincible.

Here, however, the anonymous threat actor does not exhibit the same sentiments as their colleagues. Instead, the anonymous interviewee talks of sleepless nights, living in fear, and the general mindset and business of a modern-day ransomware contractor.

The following interview, originally published on September 20, has been lightly edited for clarity.

Lenta.ru: Our conversation today will center on reports of the resurrection of the REvil group, which is categorically linked with Russia in Western media. The ransomware collective is credited with attacks on large American companies, and, with this, cooperation with Russian special services. Have you collaborated with REvil? Are these accusations justified?

"Antivirus": In the normal world, I was called a contractor—doing some tasks for many ransomware collectives that journalists consider to be famous. The very fact that I am giving an interview is unlikely to please my clients, which is why I hide behind an alias that means nothing. Among my customers once was the REvil group.

When doing this kind of work, you do not always know who is actually setting the task. But the practice of the US authorities to appoint culprits amuses many [inside my circle]. There are Chinese groups that for years have been labeled in all media as connected with the authorities of the country, who allegedly work out of the Chinese version of Lubyanka [headquarters of the FSB]. But inside the community, everyone guesses that these are simple guys scattered all over the world who even have difficulty communicating among themselves, let alone the government.

Of course, nothing can be ruled out. But personally, I have no feeling that the Russian special services are planning any attacks.

Another source of mine believes that REvil has disappeared from the radar due to increased interest from the US authorities.
Many in one way or another came across the user Unknown, who was the official spokesperson of the group on the dark web. He disappeared this summer and it is not known what happened to him. There is a version that the Americans managed to find out his identity, after which this information was passed to the Russian security forces. It is possible.

But sometimes a banana is just a banana. A person could have fallen ill with coronavirus, gotten into a traffic accident, or simply left the business.

Is [Unknown] leaving the business?

This is not the mafia. Plus you're anonymous. When you want to leave the business, you simply press the shutdown button on your laptop.

Let’s figure it out: how profitable is cybercrime and what must happen in a person’s life for them to decide to leave it?

Let’s put it this way: this is a very time-consuming job. And if you’ve earned enough, then you can quit the game. Chronic fatigue, burnout, deadlines—all these words from the life of ordinary office workers are also relevant for malware developers.

There are two factors at play. On the one hand, you are afraid all the time. You wake up in fear, you go to bed in fear, you hide behind a mask and a hood in a store, you even hide from your wife or girlfriend. I’m younger than you, but I’ve already earned for the rest of my life. Not millions, but enough to live in peace and never work. Here is also a second factor: how to quit a job that brings such earnings in a country where you are not much sought after?

LockBit representatives said in an interview that they cannot sleep properly. Is it true?

Yes, you don’t sleep well. I’ve been sleeping four to five hours consistently for years. The problem here is more that you have a family during the day and all work is at night, plus you have to take different time zones into consideration.

Before COVID, did you have any desire to move to Europe or somewhere else?
If there comes a moment when I need to pack my backpack and leave the country on the first flight, I will. But now I’m comfortable.

Is patriotism a common story among cybercriminals?

This is not a community to survey. It is clear that there are some platforms for hiring freelancers and exchanging opinions, where news is also posted. But every person in my profession lives without any connection with the community. I don’t know what’s in my employer’s mind, just as he doesn’t know what’s in mine.

But if you try to answer globally, then I see that in the interviews of many associates, even from the one with the LockBit group, there is rather a discussion of social equality. If you go to the Italian forums on the darknet, they write more about socialism than about hacks.

This idea is close to me. The world is unfair to the weak, everything is built on financial gain. There are people who lead the largest corporations by birthright. At best, they throw off hundredths of a percent of their super profits to charity, for which they are deified by the hands of their personal PR specialists. At worst, they hide their billions from the tax authorities. This should not be so, but this is happening not only in the USA and Europe, but also in Russia.

Do you feel like Robin Hood?
Honestly? No. I am against romanticizing my work. Money is being stolen or extorted with my hands. But I’m not ashamed of what I do. I sincerely try to find at least something bad in this and cannot. Probably, my concepts of what is good and what is bad are somehow shifted.

But in this case, they are shifted for many in this profession.

Many groups declare on their blogs that they do not attack social objects. Have your developments ever been used for such purposes?

As far as I know, no.

You, like many of your colleagues, have a bright socialist rhetoric. Can we assume that, even if not always, but at least occasionally, American companies attack precisely because they are capitalists?

First, they are a
ttacked because they are rich and have a lot of money. It's hard for me to imagine an ideologically motivated attack. Second, cybercrime is an international phenomenon and the communities themselves are international. This year I worked with code snippets commissioned by the community, with whom I corresponded in Russian. The code itself contained comments in French.

If we go a little deeper into the specifics of attacks, what areas are now considered the most promising and what protective tools cause the greatest inconvenience to malware developers?

It seems to me that I will not tell you anything new here. Most of the attacks can be compared to automated spam mailing. Whoever gets hooked will be "milked." That is why each group has such a geography of defeat: from strong European companies to Vietnamese or Cambodian medium and even small businesses.

Sometimes a specific company is attacked. Here, tactics change depending on the goal. I read somewhere a story about the guys who could not get inside the security perimeter *(the conditional border between the outside world and the internal systems of the company)* of a large corporation for several years and came up with an elegant solution. They began tossing flash drives with the company's logos to its office so that one of the employees thought that his colleague had lost important documents, and inserted the flash drive into the computer in an attempt to find out whose it was. After that, malicious code should have been launched, which would instantly spread over the internal network. I don't remember how the story ended.

In such situations, in the modern world, it is not the company itself that is attacked, but small organizations from its supply chain. For example, it is not a bank that is attacked but a manufacturer of minor software that covers a minor problem. It is now the most popular point-to-point attack method that bypasses traditional defenses and penetrates the security perimeter.

The strategy of our conditional adversaries—information security departments—network segmentation according to the principle of zero trust. All the security forces now talk about this, but the tactics have not yet been brought to the ideal.

Does the service model of malware development as a service already dominate the dark web?

Not yet, but it's only a matter of time. Convenient approach.

BlackMatter hit the Japanese giant Olympus a few days ago. Before that, they said that they considered themselves the leaders of the hacking community. Will the revival of REvil interfere with their plans?

To be honest, I don't make those [leadership] ratings for myself. And no one is. How do you imagine it?

Together with REvil, the DarkSide ransomware collective, responsible for the attack on the Colonial Pipeline, disappeared from the Dark Web. There is a theory that BlackMatter and DarkSide are one and the same community. This is true?

I think yes. Although I am not sure that for someone other than journalists and security officials, this is of principle.

Many noticed that in the very first interview, BlackMatter promised not to attack American infrastructure facilities. It looked like a white flag—they say, guys, we won't be like this anymore.

Perhaps so, but it doesn't matter. BlackMatter is just making money and they don't want to draw attention to themselves. You can hit the jackpot once, but provoke such a geopolitical conflict that you will be quickly found. It is better to quietly receive stable small sums from mid-sized companies, only occasionally entering corporations such as Olympus.

Reduce ransomware risk and see Flashpoint intelligence in action

When organizations, such as financial institutions and law enforcement agencies, gain insight into the operational dynamics of malicious cybercriminal communities, they can better understand threat actor TTPs; access potentially vital observations in real-time; leverage that information to thwart a ransomware attack.

Sign up for your risk-free 90-day trial and see how Flashpoint can provide you with the actionable threat intelligence you and your entire team need to identify and respond to threats targeting your organization. When equipped with Flashpoint Intelligence, your team has immediate access to collections across illicit online communities ranging from private forums and illicit marketplaces to encrypted chat services channels to gain insight into threat-actor activity on a global scale.