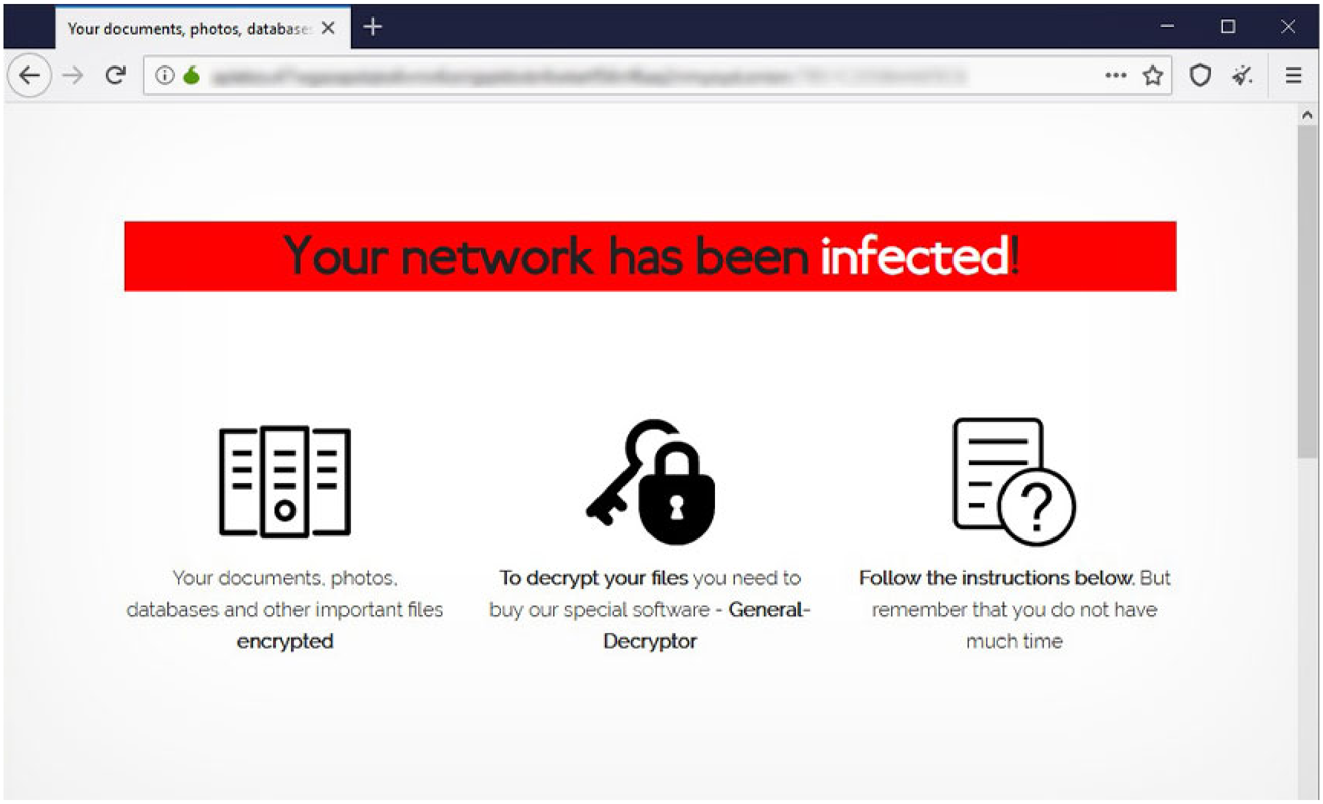
# ‘I scrounged through the trash heaps… now I’m a millionaire:’ An interview with REvil’s Unknown

therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/

March 16, 2021



Your network has been infected!

Your documents, photos, databases and other important files **encrypted**

**To decrypt your files** you need to buy our special software - **General-Decryptor**

**Follow the instructions below.** But remember that you do not have much time

Dmitry Smilyanets
March 16, 2021

Editor’s Note: It’s undeniable that ransomware is the big moneymaker in cybercrime right now. And some groups looking to make a fortune are aggressively pushing the boundaries by raising their demands to seven or eight-figure sums, threatening to release data online if payments aren’t made, and targeting hospitals and other vulnerable organizations.

One group that has gained prominence for its audacious and lucrative tactics is REvil, also known as Sodinokibi. The group runs a ransomware-as-a-service operation, in which developers sell malware to affiliates who use it to lock up an organization’s data and devices.

In addition to publishing victim data online when companies don’t pay demands, REvil has attracted attention for trying to extort then-President Donald Trump and claiming to bring in $100 million in revenue from their operations. And according to an REvil representative that uses the alias “Unknown,” the group has big plans for 2021.

Some of Unknown's claims, like affiliates with access to ballistic missile launch systems and nuclear power plants, seem outlandish—until you read reports that make them seem eerily plausible. The Record is not able to verify the assertions. Unknown talked to Recorded Future expert threat intelligence analyst Dmitry Smilyanets recently about using ransomware as a weapon, staying out of politics, experimenting with new tactics, and much more. The interview was conducted in Russian and translated to English with the help of a professional translator, and has been edited for clarity.

**Dmitry Smilyanets: Unknown, how did you decide to get into the business of ransomware?**

**Unknown:** Speaking personally, it was a long time ago. Since 2007, when there were winlockers and SMS. Even then, it brought a good profit.

**DS: You had a $1 million deposit on a hacking forum and mentioned $100 million in revenue—considering you get payments in cryptocurrency, then today you probably have half a billion dollars. How much is enough to make you quit ransomware?**

**UNK:** You counted everything correctly. The deposit was withdrawn precisely because of the exchange rate. For me personally, there is no ceiling amount. I just love doing it and making a profit from it. There is never too much money—but there's always the risk of not enough money. Although, if we talk about advertisers, one felt that $50 million U.S. was enough and he retired. However, after four months he returned—turned out that wasn't enough money. Think about it.

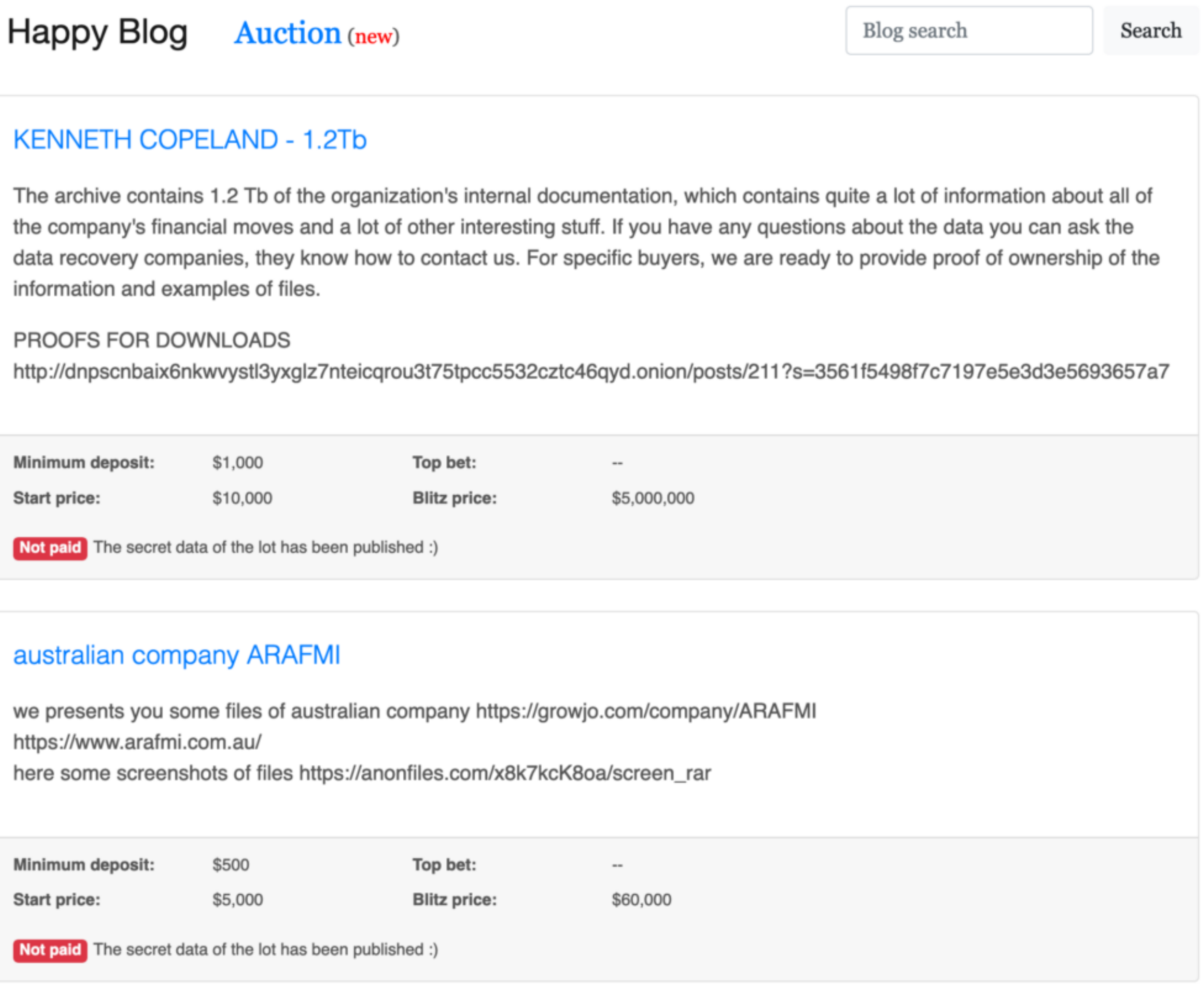
> For me personally, there is no ceiling amount. I just love doing it and making a profit from it. There is never too much money—but there's always the risk of not enough money."

**DS: You previously said that you remain apolitical, and are purely financially motivated. But if you do decide that you've made enough money, could your point of view change and you decide to impact geopolitics?**

**UNK:** I don't really want to be a bargaining chip. We brushed up against politics and nothing good came of it—only losses. With the current geopolitical relationships, everything is very beneficial for us even without any interference.

**DS: What makes REvil so special? The code? Affiliates? Media attention?**

**UNK:** I think it's all of that working together. For example, this interview. It seems like, why would we even need it? On the other hand, better we give it than our competitors. Unusual ideas, new methods, and brand reputation all give good results. As I said, we are creating a new branch of development for extortion. If you look at the competitors, unfortunately, many people simply copy our ideas and what is most surprising—the style of the text of our messages. It's nice—they try to show that they are as good as us, trying to reach the level and even striving to surpass in somethings. And in some things they are already better. For example, with those Linux versions and so on. But this is temporary. Of course, we are working on all of this as well, but with one caveat—it will all be much better. Therefore, a little bit slower.



KENNETH COPELAND - 1.2Tb

The archive contains 1.2 Tb of the organization's internal documentation, which contains quite a lot of information about all of the company's financial moves and a lot of other interesting stuff. If you have any questions about the data you can ask the data recovery companies, they know how to contact us. For specific buyers, we are ready to provide proof of ownership of the information and examples of files.

PROOFS FOR DOWNLOADS
http://dnpscnbaix6nkwvystl3yxglz7nteicqrou3t75tpcc5532cztc46qyd.onion/posts/211?s=3561f5498f7c7197e5e3d3e5693657a7

| | | | |
|---|---|---|---|
| **Minimum deposit:** | $1,000 | **Top bet:** | -- |
| **Start price:** | $10,000 | **Blitz price:** | $5,000,000 |

Not paid The secret data of the lot has been published :)

australian company ARAFMI

we presents you some files of australian company https://growjo.com/company/ARAFMI
https://www.arafmi.com.au/
here some screenshots of files https://anonfiles.com/x8k7kcK8oa/screen_rar

| | | | |
|---|---|---|---|
| **Minimum deposit:** | $500 | **Top bet:** | -- |
| **Start price:** | $5,000 | **Blitz price:** | $60,000 |

Not paid The secret data of the lot has been published :)

REvil uses its dark web “Happy Blog” to publicize data auctions for ransomware victims who have not paid demands.

**DS: Elliptic Curve Cryptography (ECC) was a really good choice [editor’s note: ECC has a smaller key size than the RSA-based public-key system, which makes it attractive to affiliates] what else are you proud of, what part of the code? How do you decide when it’s time for new features in the code?**

**UNK:** A search by IOCP [Input/output completion port], a back connection borrowed from crabs [carders], a server-side protection system—there are many advantages, it is better to read AV reviews. Personally, I really like the encryption system. It came out almost perfect.

**DS: I have been impressed with the variety of packers and crypters I’ve seen with your malware. Do you sell them to others? I saw one used in a Maze malware sample once. Do you sell them or did one of your employees move to a competitor?**

**UNK:** Partners often switch affiliate programs and because of this, there is that kind of variety.

**DS: Pavel Sitnikov said that you bought the GandCrab code from Maksim Plakhtiy, is this true?**

**UNK:** It's true that we bought it, but the names and so on are unknown to us. Even if it was the Rotten Gene, we don't care.

**DS: Do you believe that ransomware is a perfect weapon for cyberwar? Are you afraid that one day it could start a real war?**

**UNK:** Yes, as a weapon it can be very destructive. Well, I know at the very least that several affiliates have access to a ballistic missile launch system, one to a U.S. Navy cruiser, a third to a nuclear power plant, and a fourth to a weapons factory. It is quite feasible to start a war. But it's not worth it—the consequences are not profitable.

> As a weapon [ransomware] can be very destructive… It is quite feasible to start a war. But it's not worth it—the consequences are not profitable."

**DS: What other regions besides the CIS [mainly comprised of post-Soviet republics] do you try to avoid? What organizations never pay?**

**UNK:** All the CIS, including Georgia and Ukraine. Primarily because of geopolitics. Secondly because of the laws. Thirdly, for some, because of patriotism. Very poor countries don't pay —India, Pakistan, Afghanistan, and so on.

**DS: You previously mentioned that you and your affiliates understand the risks of going abroad and don't travel. Do you think there can be a "winds of change" and local law enforcement will start paying attention to your operations?**

**UNK:** If we get into politics, yes. If we look at the countries in the CIS, yes. For everything else—we remain neutral.

**DS: Do old-school criminals cause any issues?**

**UNK:** They don't.

**DS: What's your usual reaction when you see a ransomware gang or affiliate getting charged or arrested? Netwalker and Egregor reduced their operations since the raids, how do you feel about that?**

**UNK:** Neutral. This is a normal workflow. Due to the closure of the Maze, we have only increased the number of promising affiliates. So for us, I would say it is positive, in a way.

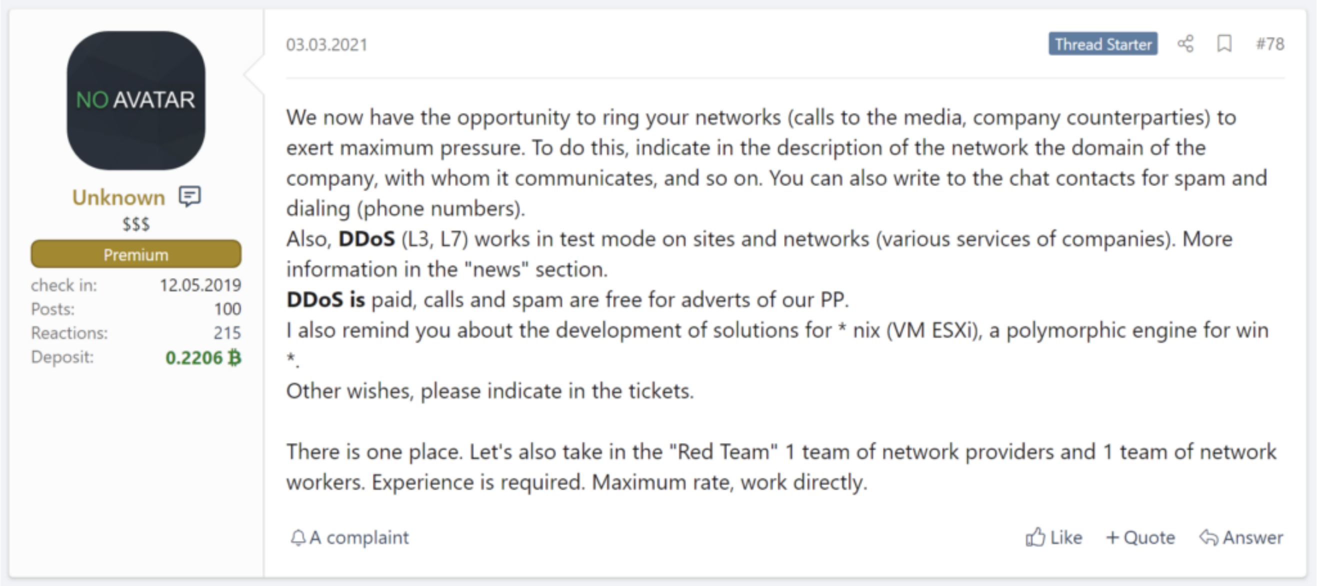
**DS: What was the highest number of affiliates you had at any one time?**

**UNK:** 60.

**DS: When they leave, is it because they're done with ransomware or because they jump ship to another ransomware-as-a-service for better rates? Does it create any issues or problems for you when an affiliate moves to a competitor?**

**UNK:** There are definitely two sides to this. 30% leave because they have earned enough. But naturally, they always come back sooner or later. Otherwise, yes, they go to competitors who dump the rates (up to 90% and so on). Of course, this is unpleasant, but this is competition. It means that we need to make sure that people return. Give them what others don't.

**DS: Some operators give a percentage of their earnings to charities. What's your opinion on this? Who would you like to donate a million to?**



| | |
|---|---|
| check in: | 12.05.2019 |
| Posts: | 100 |
| Reactions: | 215 |
| Deposit: | 0.2206 ₿ |

03.03.2021 Thread Starter #78

We now have the opportunity to ring your networks (calls to the media, company counterparties) to exert maximum pressure. To do this, indicate in the description of the network the domain of the company, with whom it communicates, and so on. You can also write to the chat contacts for spam and dialing (phone numbers).
Also, **DDoS** (L3, L7) works in test mode on sites and networks (various services of companies). More information in the "news" section.
**DDoS is** paid, calls and spam are free for adverts of our PP.
I also remind you about the development of solutions for * nix (VM ESXi), a polymorphic engine for win *.
Other wishes, please indicate in the tickets.

There is one place. Let's also take in the "Red Team" 1 team of network providers and 1 team of network workers. Experience is required. Maximum rate, work directly.

**UNK:** Free projects for anonymity.

**DS: How has your interaction with victim organizations changed since the beginning of the pandemic?**

**UNK:** It's definitely changed. The crisis is palpable, they are not able to pay the same amounts as before. Except for manufacturers of pharmaceutical products. I think it is worth paying more attention to them. They are doing just fine. We need to help them.

**DS: Do your operators target organizations that have cyber insurance?**

**UNK:** Yes, this is one of the tastiest morsels. Especially to hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves.

**DS: How do you treat ransomware negotiators? Is it easier to deal with professionals? Do they help or make it more difficult?**

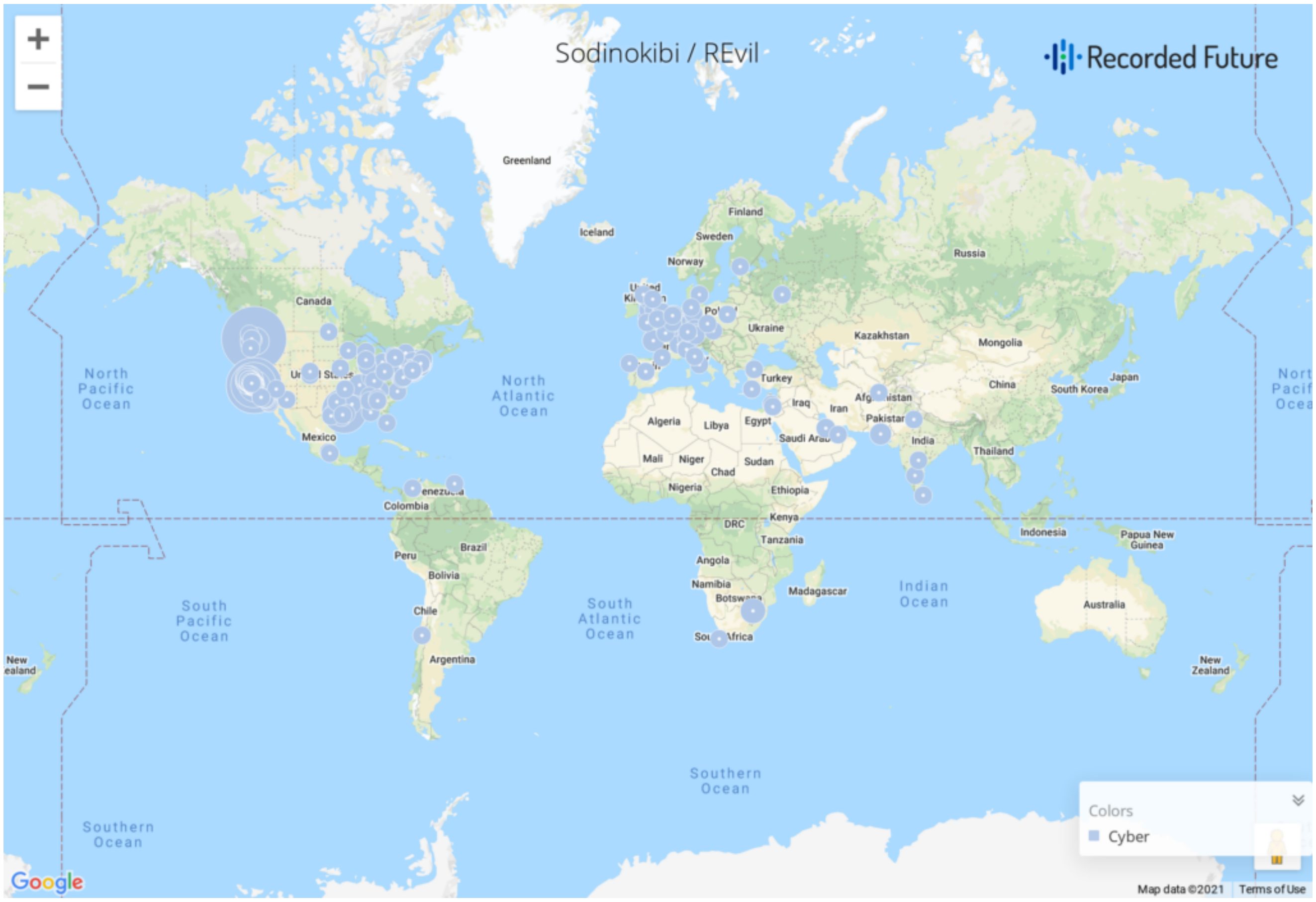
> this is one of the tastiest morsels. Especially to hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves.”

**UNK:** 70% are just there to knock down the price. Very often they make it harder. Well, for example, the company has a revenue of $1 billion. They are being ransomed for $1 million. The negotiator comes and says, we don’t care, we won’t give more than $15,000. We reduce the price to $900,000. He offers $20,000. Well, then we understand that the conversation with him is meaningless and we start publishing the data so that the owners of the network smack him upside the head for negotiating like that. And of course, after those kinds of tricks, the price tag only goes up. Instead of $1 million, they will pay one-and-a-half. Nobody likes hagglers, especially show-offs. So, more often than not, they are likely to do more harm. They only help purely in buying BTC or Monero. The rest is harmful.

**DS: Do you recommend any specific negotiators to the compromised businesses or do they act on their own? Not everyone has 100 BTC on hand to buy out the data and it’s not that easy to get on short notice.**

> To finish off with DDoS is to kill the company. Literally. I also think we will expand this tactic to persecution of the CEO and/or founder of the company.”

**UNK:** We write to decent intermediaries to let them know the target so that they can reach out themselves. We give good discounts to decent intermediaries so that they can make a bit of profit and the companies pay less. And in terms of deadlines—we can always give some extra time. In general, if there is an understanding that you have to pay, no other options, but not as much, we will find a common language. But if we get delusional messages like, “There is no money” or, “We will pay one-tenth,” you have no one to blame but yourself.



References to REvil attacks gathered from private and underground sources. Courtesy of Recorded Future.

**DS: You said that you like to apply additional pressure through DDoS [editor’s note: distributed denial-of-service attacks involve flooding a site with junk traffic, making it unreachable]. How effective is this scheme?**

**UNK:** We do not use it often, in contrast to calls. Calling gives a very good result. We call each target as well as their partners and journalists—the pressure increases significantly. And after that, if you start publishing files, well, it is absolutely gorgeous. But to finish off with DDoS is to kill the company. Literally. I also think we will expand this tactic to persecution of the CEO and/or founder of the company. Personal OSINT, bullying. I think this will also be a very fun option. But victims need to understand that the more resources we spend before your ransom is paid—all this will be included in the cost of the service. =)

**DS: Tell me a secret.**

**UNK:** As a child, I scrounged through the trash heaps and smoked cigarette butts. I walked 10 km one way to the school. I wore the same clothes for six months. In my youth, in a communal apartment, I didn’t eat for two or even three days. Now I am a millionaire.

Mission-driven and Russian-speaking intelligence analyst with type A personality. Dmitry has twenty years of experience and expertise in cybercrime activity that includes being a former member of an elite Russian-based hacking organization.