Interview with a member of a group related to the ransomware activities named REVIL

At the moment, many organisations in the world are chasing this group, including American intelligence agencies.

**Interviewer**:

REVIL hackers put a million dollars as credit in the hackers forum, this post appeared in HACKER magazine and the reporter recorded that the hackers want to prove to partners that they are serious. For me as a blogger, it is interesting to hear what REVIL is and what its connection to Sodinokibi is.

https://xakep.ru/2020/09/29/revil-million/

**Answers**:

-REVIL or as it is called manufacturers of protection products sodinokibi is a heresy registered in the language C. The software encrypts the user's files and thus his access to them is denied.

- For a successful attack, it is necessary to destroy backups such as on NAS or tapes and take as much information as possible to you (EXFILTRATION), it is very common to pay money not for the information itself but so that the information does not leak.

-Example of what not to do - TRAVELIX. From what I remember the company fell in the wake of our attack just because the stock fell.

**Interviewer**:

As journalists reporter, REVIL works in the form of RANSOMWARE-AS-A-SERVICE, which means that the distributors of the heresy and the developers share in the profits. Is it true that the division is XXXX?

Answer:

The interviewee confirms that in the case of infidelity the developers get 20% -30% and the distributors get 70% -80% of the money. In his opinion the software is just the tool and most of the work is done by the distributors.

**Interviewer:**

What is the difference between REVIL and other viruses such as WANNACRY?

Answers:

* WANNACRY was a very stupid and uncontrollable experiment. Making only a lot of noise and making less than $ 100K
* At a minimum we do not have EXPLOIT RCE so REVIL does not automatically infect sibling computers like a worm across the internet.

- Within the network the software will try to spread using different methods.

**Interviewer:**

How was this software created?

Answer:

* Another software was bought as a basis for development and we built our product for our needs.

**Interviewer:**

How do you see Revil against the TOP 5 competitors that exist today? Why do your distributors choose you?

**Answers**:

- Because of the encryption method. MAZE or LOCKBIT has no elliptical encryption, no triple schema - cube key, system key, user key.

- but probably because of our good work in making money and technologies.

* We treat competitors in a neutral way and are always ready for negotiations. It often happens that two ransomewares infect the same company and if they do not reach an agreement the two attack groups will remain unpaid.

**Interviewer:**

What is the symbol of the first letter R called REVIL?

**Answer:**

- REVIL is an abbreviation of RANSOMEWARE EVIL, the idea came from the famous game RESIDENT EVIL.

**Interviewer:**

What are the three REVIL attacks that you think made the most noise?

Answers:

- TRAVELEX

- 23 cities in TEXAS

* There will be one more very loud attack but at the moment we will not talk about it, I can only say that it is related to a very large company of computer games developers.

**Interviewer:**

- Somewhere they wrote that in May 2020 you demanded $ 42 million from US President Donald Trump, another record that you cracked an elliptical encryption that a company used to protect its information.

**Answer:**

- No no, we wished the American intelligence agencies succeeded in cracking the encryption of the information, Not Trump but of Alon Grubman (Grubman Shire Meiselas & Sacks).

The money was paid for the information. Who bought it? I will not say.

- The information was related to the tax evasion of companies associated with Donald Trump.

**Interviewer:**

You made a million dollars when it was equivalent to about 7 million rubles in the value of the current currency. If not a secret, what is the revenue approximately at REVIL in 2019 and 2020 in comparison?

- More than $ 100 million a year.

- Speaking of rubles then well over a billion

**Interviewer:**

Are you not afraid of losing the million dollars if the forum is hacked or the encryption keys are leaked? After all, as you say, Western intelligence agencies are chasing you.

Answer:

We will earn more money, money comes and money goes.

**Interviewer:**

To maintain a product as complicated as REVIL , do you need more than 10 people in a group?

- Speaking of a group of developers then less than 10 people is enough

- If we are talking about the PENTESTERS group (perhaps referring to RED TEAMERS) then more than 10 are needed

**Interviewer:**

Why did you decide to use the RANSOMWARE-AS-A-SERVICE model and not do everything yourself from start to finish? Break in, get a hold (PERSISTANCE), encrypt, demand ransom and launder the money?

- We work both ways but RAAS model is more profitable to work, it turns out that there is more profit.

**Interviewer:**

As I understand this model allows you to increase your business significantly

**Answer**:

- Unequivocal

**Interviewer:**

What services do you provide to your partners today?

Answer:

- Negotiation

- Click on the organization

- and of course software support, payment receipt and DECRYPTION software

**Interviewer:**

When a partner contacts you with a request to receive service, you give him a REVIL on loan. I mean, the partner does not run EVEIL but uses a ready-made product, right?

**Answer:**

- We give our software and services for negotiation, the partner's job is to get a grip on the network and destroy the backups, download files to the computer, that is, all the rest is our concern.

**Interviewer:**

If the company ransoms the money goes straight to you then you divide them between the partner?

Answer:

The money is automatically distributed by the system, our first wallet of course.

**Interviewer:**

Have you had a problem with a partner? Can you give an example without mentioning names and how did you manage to overcome it?

Answer:

* To be honest, I do not remember, with us it is a closed family. The filtering is very strict and the personality is strange we do not even add to our media.

**Interviewer:**

Who is currently oppressing you on the side? CIA, NSA, FBI?

Answer:

US intelligence authorities

Interpol

Companies all over the world

This is normal. The project was built to withstand such pressure.

**Interviewer:**

Have there been cases where under the cover of a partner tried to reach you agents of US intelligence agencies.

Answer:

Yes, but they are filtered by the usual questions of general and social politics of the Soviet Union.

There were also Russian speakers but when we talk about specific things of work the person starts to "float"

**Interviewer:**

Do you have an interesting story after they tried to recruit you to intelligence agencies?

Answer:

to draft? Recruit unfamiliar.

We are apolitical. Do not see how we can be used as a technological body.

If you recall the case of Trump, there it is net money and not politics.

We do not care who the president will be, we work, we have worked and we will work.

**Interviewer:**

Have they tried to break into your affiliates with the help of links in phishing with a virus or something?

**Answer:**

Affiliates no but security experts yes.

You can see an example on the screen - trying to break in every day. (Shows an example of XSS)

It’s hard to break into something you don’t know what it looks like.

I'm sure the experts do not know what systems are on the servers and what kind of web server.

Just trying to break out like shooting in the air.

The product is built for such sizes and is ready to withstand such operations.

**Interviewer:**

How do you treat a famous journalist named Brian Krebs? Do you think he is making an objective impression on you?

Answer:

We read. Treat neutrally.

**Interviewer:**

At the beginning of September 2020, the bank ESTADO, one of the three largest banks in Chile had to close all branches after an attack of infidelity. Record that the incident happened after one of the employees opened an office document he received through the mail. Another record that the document created BACKDOOR on the bank network and on the night between Friday and Saturday the hackers used it to distribute the heresy in the bank.

It was further recorded that at first the experts at the bank quickly aimed to deal with the attack but the damage was much more severe than they estimated because the attacker encrypted most of the organization’s internal servers and end stations.

The details of the attack were not released, but a source close to the investigation said that the bank was attacked with REVIL. Is this a true or fictional story?

**Answers:**

Yes, it happened, it's our job.

It is very common for companies to remain silent about the source of an attack.

The company has a very important reputation. In particular it can affect the stock value.

**Interviewer:**

TYLER TECHNOLOGIES recently paid a large ransom. Probably $ 10 million.

Do you know of any other interesting cases where ransomeware operators have exploited the weaknesses of systems developed by large technology companies? Can you give a specific example when saving updates has led to great damage?

**Answers:**

GRUBMAN and TRAVELIOX companies, both breached through security breaches in old CITRIX and PULSAR products.

How stupid is that? We gained access to the entire network in 3 minutes thanks to one loophole treated with PATCH.

**Interviewer:**

What is the percentage of cases in which large companies negotiate with you for the payment of the ransom so that there will be no publicity about the case in the US and there will be no risk of hatred against them because they did not adequately address security?

Answer:

In 70 percent of the cases

**Interviewer:**

To what extent are you fair? Do you negotiate with companies following a successful attack? If the company pays the amount how can it be sure that it will not double the demand and not ask for money again?

**Answer:**

Our reputation is important to us, it affects the percentage of payments.

No betrayal on our part has been and never will be, that is the basis.

**Interviewer:**

From your experience have there been cases when there was no success after receiving the ransomware to open the encryption of the files? The intention was to get involved and you could not do anything about it.

**Answers:**

Yes, if you have previously tried to use the file recovery software.

If you change even one BYTE in the file, the key will be lost.

This happens a lot with anti viruses. They simply delete the ransom notes containing keys.

Speaking openly, such a case is not common, remember 12 cases and of course we never took money.

At the page of the ransomware there is a warning to the victims, if they do not read them, it is their their problem

**Interviewer:**

Which sectors are now the most « fruitful «  for RANSOMWARE attacks? Where is the most profit?

Answers:

IT vendors

Insurance companies

Law Firms

especially agriculture

**Interviewer:**

A recent Microsoft report stated that very effective attacks are BRUTEFORCE on RDP. What do you think, will the approaches change and will there be changes in attack vectors?

**Answers:**

BRUTEFORCE attacks have been alive for 20 years and will remain alive.

The best vector is the RDP, especially the fresh burst BLUEGATE will give a strong blow to the attacking vector.

**Interviewer:**

Is there a RANSOMWARE for Android and iOS today and is it worth messing with? For example encrypting the phone memory or cloud storage and will there be movements in this direction?

Answers:

You have to be really fucked up to do that. I'm totally against it.

Android and even more iOS are perfect for developing a banking environment, the question arises what to encrypt.

Pictures in which you eat matzah? Yes, very dangerous.

**Interviewer:**

In your forum post you write:

Our software has been tested more than once by the Europol, Interpol, FBI, CIA, NSA and the US Secret Service and agencies around the world. Our software has been tested worldwide and passed government-level security tests. Their budget and increase the arsenal (of tools) for work.

Together with us a new company (JUNIOS) that only recently downloaded the free version of MSF (referred to as METASPLOIT) within one month moved to a version with a license of COBALT software (referred to as COBALT STRIKE).

Within 6 months they already had 0DAYS and exploits for successful work and such examples are enough.

Basically from what you wrote I understand that SUPPORT helps and teaches the new company and in fact you have our hierarchy and correct division of labor. Hence the question, can a really new company make money so fast?

**Answers:**

The SUPPORT will only help in negotiations. They learn the technical details on their own.

Yes really so fast can earn.

In front of my eyes one ransom group came from ransom payments of 20-30 thousand dollars within half a year came from ransom payments of 7-8 million dollars.

Do not think that "hierarchy" is called "smart division of labor".

We do not have heads (ranks of management). The answers I give now are my personal opinions.

All decisions are made together. I really appreciate it and respect it.

**Interviewer:**

So that young people do not run after easy money, I want to ask a question about risk regarding such activities. How many years can a young man get in jail for such activities and how high is the risk in your game?

**Answers:**

If you look at the world of ransom seriously, I would not be surprised if I get murdered. I will understand that.

No one in our field will ever fly to the US and similar countries because there is no justice for us, murder is definitely a possibility.

We create big problems , Speaking of jail then two life sentences.

**Interviewer:**

Considering that you are probably also being pursued by the CIA and the NSA, for safe communication what would you recommend to paranoid TALKS or JABBER?

**Answers:**

Tested operating system version and custom comp. For example Gentoo, the same goes for software.

For paranoids I recommend DECENTRALIZATION.

**Interviewer:**

ALTCOIN and MONERO, can the agencies still track them?

Answers:

yes.

In stock exchanges it is rare to get them.

A large amount of MONERO in DEPOSIT raises questions.

Therefore MONERO can only be considered as a means of payment from a range.

**Interviewer:**

Do you also donate? For example, donate part of the amount of ransom you received to all kinds of open source project funds such as Project TOR or ELECTRONIC FRONTIER FOUNDATION?

**Answer:**

I will answer briefly. It is possible.

**Interviewer:**

Record in NAKED SECURITY that your favorite attack methods for intrusion into this organization's network EXPLOIT KITS, scan methods and exploit vulnerabilities of RDP servers and installation files with BACKDOOR.

What kind of attack do you think is most effective than what was stated?

**Answers:**

Do not know how to access enterprise network through EXPLOIT KIT. For example RIG, software is somehow wrong (that means not to his liking).

The best personalized method for me is to obtain SYSADMIN authorization from a standard STEALER and get a full MSP of the entire organization.

Not inventing it, such a thing actually happened. The organization was serious, a six-zero ransom. Attack with the help of exploiting RDP vulnerabilities. For very important purposes link SPAM (possibly phishing) along with a phone call.

**Interviewer:**

Do you think there is a RANSOMWARE market in the next two or three years? What global changes will there be in the market?

**Answers:**

Yes. Everything goes in the direction of information theft and not its encryption.

Encryption is just a pleasant addition.

I personally liked the idea of ​​SUNCRYPT where DOS was done on the infrastructure site along with encrypting the files and threatening their publication and that is very strong pressure.

We are thinking about this idea in these moments.

**Interviewer:**

When you earn a large enough amount of money do you think you personally can stop at the right point or the process associated with high risk and money is like a drug, attractive.

Answers:

If I talk about myself personally - it's time to stop.

The money will last for a few hundred years but there is never such a thing as a lot of money. There is always not enough money.

**Interviewer:**

Give an example of the funniest resume, perhaps an autobiography that came to you shared or interviewed throughout your work period.

**Answers:**

To be honest there are a lot of those. The most mediocre - buys DEDICATED servers in the store and wants to work with you.

It is rare for us to register people who are really talented. I think everyone who was already sharing between the partners.

So I personally think of betting on the young, giving them a chance to prove themselves, if they do not prove there are enough competitors, they will go to them.

We always have high demand and everyone is satisfied.

**Interviewer:**

When you are preoccupied with what you are preoccupied with, is it possible to go on trips (meaning to travel the world)?

**Answer:**

Of course not, there are no other options here.

**Interviewer:**

Now I will ask not so serious questions, can be answered with humor.

How to identify a "lumberjack" who wants to make friends with you (referring to intelligence agents)

Answer:

He very stubbornly asks to enter your "sweet" system with all permissions. In other words - egoist.

**Interviewer:**

As a REVIL member, try to describe your life in one word.

**Answer:**

More and always more.

**Interviewer:**

What does your sweetest dream look like?

**Answer:**

Billion, then two billion. If there's a mood then five billion dollars.

**Interviewer:**

My followers want to know where you live. At some metro station, street and house number.

**Answers:**

Nikita Kubikov or Nariman Namazov.

Somewhere in the middle between them the place.

**Interviewer:**

How did you come to such a life?

**Answer:**

Once when I was little I installed CHLENIX and loved it.

**Interviewer:**

What can you advise a new company?

**Answers:**

Eat more and eat good but drink Vodka

Seriously it is better to learn, to try, everything will succeed, everything is possible.