Uncensored Interview with REvil / Sodinokibi Ransomware Operators

cybleinc.com/2021/07/03/uncensored-interview-with-revil-sodinokibi-ransomware-operators/

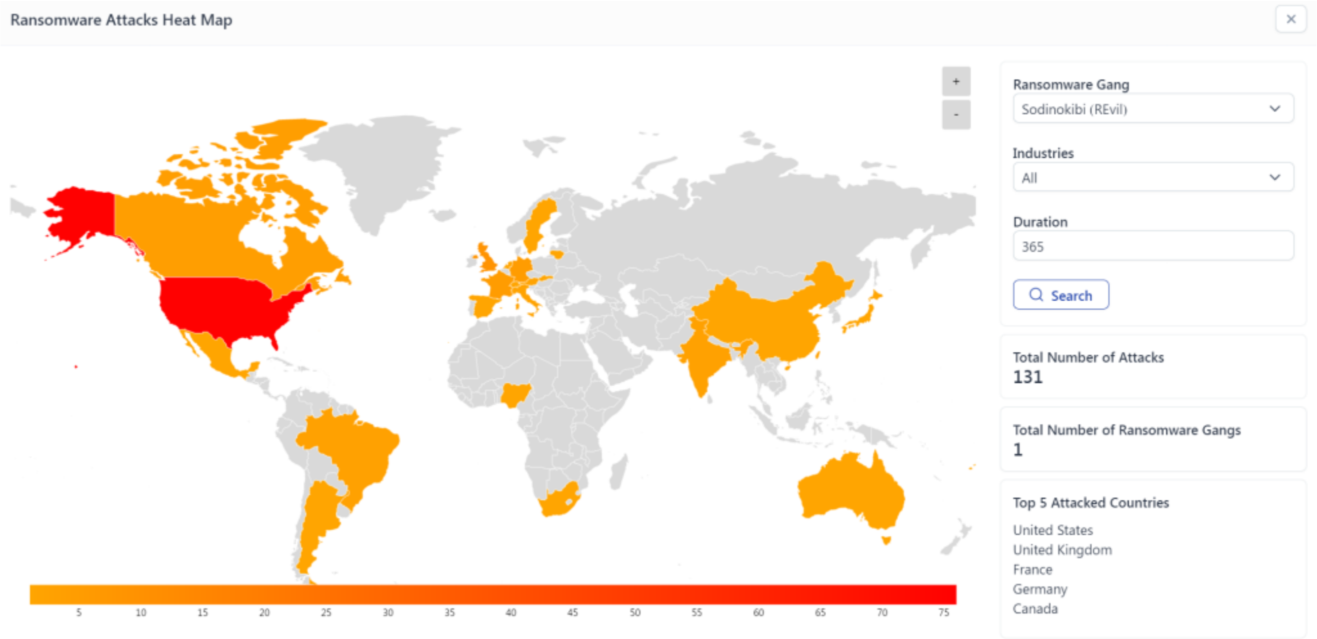
July 3, 2021

An **uncensored** interview between the Russian OSINT and REvil operator has popped up in one of the hacking forums today. This is an unedited interview, which was originally released on October 23, 2020, by the Russian OSINT on their YouTube channel.

Here are some of the interesting insights –

- Per the operators, it meant Ransom Evil and was derived from Resident Evil.
- REvil is an encryptor written in C. The encryptor also requires to liquidate backups and merge information as much as possible for a successful attack. They support elliptical cryptography and a “triple” scheme (file key – system key – affiliate key).
- Malware developers keep 20-30% of the share, while distributor takes the remaining 70%
- WannaCry was unmanageable and called “stupid.”
- The top three attacks were – Travelex, Grubman, and Texas 23 counties
- The REvil mentioned that some paid them on behalf of Alan Grubman as they had access to tax evasion schemes.
- REvil makes over $100M a year.
- They have a penetration testing group with over ten individuals working for them.
- They operate as a “closed” family. The selection process is rigorous. They don’t communicate with each other directly.
- Per REvil, they compromised Grubman and Travelex through known Pulsar and Citrix vulnerabilities. They also boasted about how they owned the network in under 3 minutes.
- 33% of deals with the group are unreported or secret
- Their favorite targeted as IT providers, Insurance, Legal firms. Manufacturing
- Monero is the preferred mode of payment due to the difficulties in tracking transactions
- REvil is inspired by SunCrypt ransomware, i.e., DDoSing the site as well to add extra pressure. They are working on it.

REvil’s Ransomware Attacks Summary is below (Source: Cyble Vision):


Ransomware Attacks Heat Map

Ransomware Gang: Sodinokibi (REvil)

Industries: All

Duration: 365

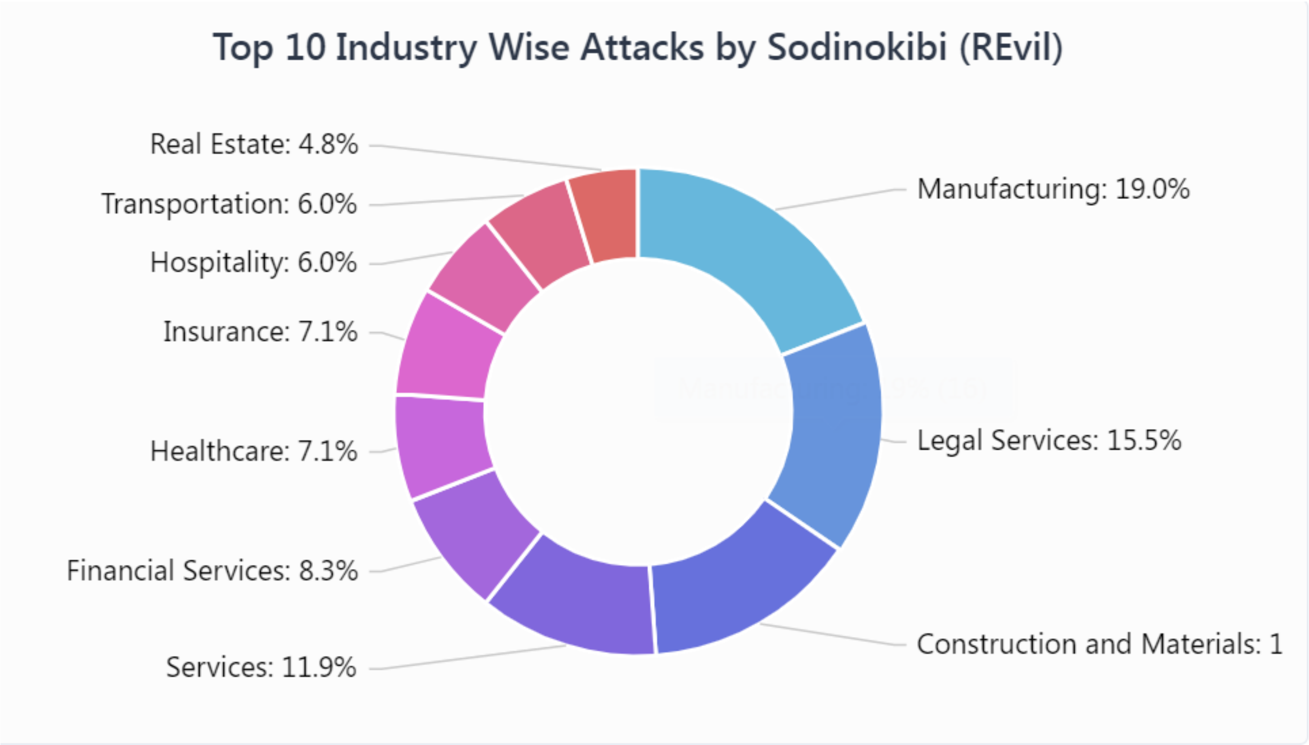
Search

Total Number of Attacks
131

Total Number of Ransomware Gangs
1

Top 5 Attacked Countries
United States
United Kingdom
France
Germany
Canada

Ransomware Attacks Heat Map (REvil)



Industries Targeted by REvil Ransomware Operators

Here is the original interview (as published on a cybercrime forum):

Russian OSINT: *” REvil deposited a million dollars on a hacker forum. ” ” Thus, hackers want to prove to potential partners that they are serious about the matter, ” Maria Nefyodova wrote in the article. As an ordinary person, together with the audience, it is interesting to know what REvil is or what is it called Sodinokibi? Do I understand correctly that the encryption program Revil used to obtain ransom from organizations in the event of a successful attack?*

Revil: *REvil (or as it is called by the information security vendors of the sodinokibi) is an encryptor written in C. Yes, the program encrypts user files, thereby restricting access to them. For a successful attack, it is also necessary to liquidate backups (NAS and TAPE storages for example) and "merge" as much information as possible to yourself. Very often they pay not for the fact of encryption, but for the fact that these files do not get into public access. An example of how not to do it is Travelex. In my memory, as a result of our attack, they simply went bankrupt due to the fall in shares.*

Russian OSINT: *As journalists write, Revil operates on the RAAS model (Ransomware-as-a-Service, "Ransomware-as-a-Service"), as part of this agreement, affiliates and ransomware developers share the proceeds from the ransom. Is it true that with such a "division of labor", malware developers get a 20-30% share, while distributors get 70-80% of the ransoms received?*

REvil: *Yes it is. Distributors do most of the work, and software is just a tool. I think this is fair.*

Russian OSINT: *Please explain for viewers and subscribers how REvil differs from other ransomware programs, for example WannaCry?*

REvil: *REvil is not meant to be massive. WannaCry was a very stupid experiment, and unmanageable. To make such a rustle and get less than $ 100k is very funny. At the very least, we do not have the RCE exploit, as WannaCry had, so it does not automatically infect other computers, like a worm. On the external internet. Within the network, of course, the software itself will connect external media and systems for maximum effect.*

Russian OSINT: *How did REvil come about, is there a background to the creation of the project?*

REvil: *Nothing special. We used similar software as advertisers earlier – the software eventually ceased to exist. We bought its source code and wrote our product for our purposes.*

Russian OSINT: *What are the main competitive advantages of your product in comparison with other TOP-5 ransomware? Why do your so-called partners choose you?*

REvil: *An encryption system. Neither Maze nor Lockbit have elliptical cryptography, no "triple" scheme (file key – system key – affiliate key). But they come to us rather because of our competent work on receiving payment (envelope) and technologies. Maze and we, in principle, set the vector of the direction of the ransoms as a whole as branches. We treat our competitors quite neutrally and are always ready for dialogue (very often this happens when 2 lockers encrypt 1 company at the same time. If you don't agree, both will be left without money).*

Russian OSINT: *What does the R prefix in the word Revil mean? Is that the word Reborn? I.e “*

REvil: *Ransom Evil. The thought came from Resident Evil.*

Russian OSINT: *When I was preparing for the release, I must admit that I did not fully realize how serious Ransomware is and, in particular, Revil is involved in a number of high-profile scandals, it is mentioned by such authoritative media as Forbes, Wallstreet Journal, BBC, Security Lab, Xakep , Cyberbeast, even in Wikipedia … ..What TOP-3 public attacks of REvil do you think are the most resonant?*

REvil: *Travelex, Grubman and Texas 23 counties. This is for a moment. There will be one more very loud attack, but we will not advertise it for now. I will just say that she is connected with a very large game developer.*

Russian OSINT: *Some media reported that in May 2020, you demanded $ 42 million from US President Donald Trump. It was alleged that you deciphered the elliptic curve cryptography that the firm used to protect its data. How did the story end, did the US authorities make a deal with you by paying the ransom?*

REvil: *No no, we wished the NSA, the FBI and the US Secret Service the best in decrypting the data. Not Trump, but Alan Grubman. Money paid for the data. Who bought them – I will not say. The data was related to tax evasion schemes by companies affiliated with Trump.*

Russian OSINT: *The deposit of a million dollars is about 77 million rubles at the current exchange rate, it seems to me, for you it is mere pennies .. if it’s not a secret, what is the approximate annual revenue of REvil for 2019 and 2020 in comparison?*

REvil: *More than $ 100 million a year. If we talk about rubles, then already well over a billion.*

Russian OSINT: *Aren’t you afraid of losing 1 million if the forum gets hacked or private keys leak into the network? As you yourself hint in your posts, Western intelligence services are hunting you.*

REvil: We’ll *earn more. Money comes and goes.*

Russian OSINT: *Does it take more than 10 people to service a complex product like REvil?*

REvil: *If we talk about the development group, less than 10 is enough. But about the pentest group, more than 10, of course.*

Russian OSINT: *Why did you decide to work according to the Ransomware as-a-Service model, and not do everything yourself from start to finish: hack, secure, encrypt, demand a ransom and launder money?*

REvil: *We work* **anyway** *. According to the RaaS model, it is more profitable. More profit is obtained.*

Russian OSINT: *Does the RaaS model allow you to scale your business faster?*

REvil: *Undoubtedly*

Russian OSINT: *What service options do you provide to your partners today?*

REvil: Negotiations, pressure on the organization. Well, the software itself. Receiving a ransom, providing a decryptor.

Russian OSINT: *Once again, I want to capture an important point for viewers: when a partner asks you to provide him with your service, do you lease REvil to him? That is, the partner does not control the encryptor and does not know how its filling works … he only uses the finished product. Right?*
REvil: *We provide software and our own negotiation services. The partner's task is to infect the network and kill backups. Download files. Everything. The rest is our concern.*

Russian OSINT: *If an organization pays a ransom, does the money go to you first, and then you distribute it among the partners?*

REvil: *Immediately automatically distributed by the system. But the original wallet is of course ours.*

Russian OSINT: *Were there any cases of conflicts with partners, can you give one memorable case and how you managed to resolve it?*

REvil: Honestly, *I don't remember. We have our own "closed family". The selection is very strict and inadequate personalities, we do not even add to ourselves in the means of communication.*

Russian OSINT: *Who is hunting you today? CIA, NSA, FBI, Interpol?*

REvil: *The US Secret Service, Europol and cybersecurity companies around the world. This is normal. The project was designed under such pressure.*

Russian OSINT: *Have there been any cases when, under the guise of partnership, agents from the Secret Service, NSA or CIA tried to get into the trust of you?*

REvil: *Yes. But they are pouring in on the "general political and social" issues of the CIS countries. There were also Russian-speaking people, but when we talk about the specific specifics of work, a person swims. Also immediately denied.*

***Russian OSINT:** Do you have a funny story from practice when they tried to recruit you? Share a memorable experience.*

***REvil: Recruit**? I don't know to recruit. We are apolitical. I doubt the practical use of us as a special apparatus. If you remember Trump, there is purely money. No politics. We don't care who is the president. We have worked, we are working and will continue to work.*

***Russian OSINT:** Have your "partners" tried to hack you through phishing links, malware, some complex schemes for the purpose of deanon?*

***REvil:** There are no partners, but cybersecurity experts are. The most striking example is <script> alert ('hello') </script>; and info.php in the chat app. They try to break it every day. It's hard to actually break what you don't know. I'm sure the experts don't even know which OS builds are on the servers, which web server. They just attack for luck. There is a separate respect for shell.exe. The product was created for this scale and is capable of holding such a defense.*

***Russian OSINT:** How do you feel about the well-known information security journalist Brian Krebs, how objectively does he write about you?*

***REvil:** Read it. Neutral.*

***Russian OSINT:** In early September 2020, BancoEstado, one of the three largest banks in Chile, was forced to close all branches following a ransomware attack. They wrote that the incident occurred due to the fact that one of the bank employees opened a malicious Office document received by mail. The allegedly malicious Office file installed a backdoor on the bank's network, and on the night from Friday to Saturday, hackers used it and spread the ransomware across the financial institution's network.*

It is reported that initially the bank's specialists expected to quickly cope with the attack, but the damage turned out to be more serious than they thought, since the ransomware encrypted the vast majority of internal servers and workstations of employees. Details of the attack were not disclosed, but a source close to the investigation said the bank's internal network was attacked by REvil (Sodinokibi). Was it really or a fictional story?

***REvil: It** really was. Our handiwork. Very often, companies keep silent about the source of the attack. The reputation is the same. Falling stocks.*

***Russian OSINT:** Recently, Tyler Technologies paid a large ransom for Ransomware (approximately $ 10 million). Are there any other interesting cases known when ransomware took advantage of vulnerabilities in the systems of large technology companies? Can you give specific examples when savings on information security led to large losses?*

REvil: *Grubman and Travelex. Both are hacked through the old Pulsar and Citrix. This is really stupid. We got access to the entire network in 3 minutes. Just because of 1 vulnerability, which is healed by the patch.*

Russian OSINT: *In how many% of cases large companies go with you to a secret deal and pay a ransom so that there are no publications in the media or they are not threatened with hate for negligent attitude to security*

REvil: *In 1/3 of cases*

Russian OSINT: *How honestly do you negotiate with companies in the event of a successful attack? If a company pays the ransom in good faith, how can they be sure that you don't double the amount and demand the amount again?*

REvil: *Our reputation is dear to us – it affects the envelope (% of payments). There have never been any deceptions on our part and there never will be. This is the foundation. There will be a bad envelope, people will leave. Reputation in such a business is No. 1.*

Russian OSINT: *Have you ever had problems when it was not possible to decrypt encrypted files after receiving a ransom? That is, something went wrong and you yourself could not do anything.*

REvil: *Yes. If you have previously tried to use third-party data recovery software. If at least 1 bit of the file is modified, the key will be lost. Especially often this happens with antivirus – it simply deletes notes, and they contain keys. I say openly – such cases are extremely rare. I remember only 12 for the entire time of work. And, of course, we never took money. The note contains a warning to the victims. If they don't read it, their difficulties.*

Russian OSINT: *Which industries are currently the "fattest" for Ransomware attacks? Where is the most profit?*

REvil: *IT-providers, insurance, legal firms. Manufacturing, especially, oddly enough, the agro-industrial complex.*

Russian OSINT: *You don't do any hacking and fixing into the infrastructure with your own hands … your partners do it, right?*

REvil: *We have our own "flying squad", and we also have partners. We do this and that.*

Russian OSINT: *A recent report from Microsoft said that 2 extremely effective attacks for introducing Ransomware are brute-force and RDP hacking, how do you think, will attack vectors change over time?*

REvil: *Brute force has been alive for 20 years. And he will be alive. RDP is the best vector. Especially the fresh BlueGate vulnerability will hit him very hard.*

Russian OSINT: *Are there Android and iOS Ransomware today? Is it profitable to do this? Let's say we encrypt the phone memory or cloud storage of CEOs of companies … will there be any movement in this direction?*

REvil: *You have to be absolutely repulsed to do this. I am totally against it. Android and even more so iOS is ideal for working out the banking sector. What to encrypt? Photos of you eating matzo? Very bad damage, yes.*

Russian OSINT: *In your post on the forum you write"Our software has been repeatedly tested by Europol, Interpol, FBI, CIA, NSA, US Secret Service and other law enforcement agencies and intelligence agencies of countries around the world. Our software has been used all over the world and has passed a government security audit. Top-notch teams trust our software and have been able to significantly expand their budget and improve the arsenal to work with. Together with us, newbies who just downloaded the free version of msf switched to licensed cobalt strike in just a month, and after 6 months they already had 0day lpe / rce exploits at their disposal for successful work. And such examples are enough "*

Based on your text, as I understand it, supports help and train newcomers, that is, you have built a whole hierarchy and division of labor…. Do newcomers really earn so much?

REvil: Supports *will only help in negotiations. They learn the technical details themselves. Yes, they can really do that quickly. Before my eyes, 1 team with redemptions of 20-30k dollars rose to redemptions of 7-8 million for 1 goal. For half a year. Hierarchy is unlikely. Competent division of labor. We don't have the main ones. What I am answering now is purely my personal opinion. All decisions are made collectively. I really appreciate and respect that.*

Russian OSINT: *To prevent young people from rushing for easy money , I want to ask a question related to the risks of such an activity: what are the timing of newcomers for doing this activity and how high are the stakes in your game?*

REvil: *Seriously, taking the realm of extortion, I wouldn't be surprised if I get killed. I will understand that. None of our topic will ever fly to the United States and similar countries, and since there is no justice for us, it is quite an option to kill. We create serious problems and are virtually elusive. Timing? 2 for life.*

Russian OSINT: *Considering that the NSA and the CIA are after you, Tox or Jabber?*

REvil: *My* ***own*** *OS build, personally tested and compiled (Gentoo for example). Also with software. I advise the paranoid to decentralization.*

Russian OSINT: *Monero Still Cannot Trace?*

REvil: *I guess so. The most obvious trace is that on exchanges it is rarely accepted; its large number raises questions. Therefore, Monero is only a transit means of payment.*

Russian OSINT: *Do you do charity work? For example donating to various open source foundations, the Tor Project, the Electronic Frontier Foundation?*

REvil: *Possibly.*

Russian OSINT: *As Naked Security by Sophos writes: your favorite attacks on entering the company's infrastructure are exploit kits, exploitation scan techniques, RDP servers, installation files with backdoors. What type of attack do you think is the most effective of the above?*

REvil: *I don't know how to get into the infrastructure through a bunch of exploits, for example, RIG. It is written somehow incorrectly. The best method, for me personally, is to catch the authorization data of the drocher sysadmin from a regular stealer and get full access to the MSP of the entire organization. I'm not telling it out of thin air – this was in practice. The organization was serious, the ransom with 6 zeros. And so RDP and exploits. For a very important purpose – ringing spam mailings.*

Russian OSINT: *How do you think the Ransomware market will change in the next 2-3 years? What global movements or changes will there be in the market?*

REvil: *Yes. Everything is moving towards merging files, not encrypting them. Encryption is just a nice touch. Personally, I liked the idea of SunCrypt – the ddos of the site and infrastructure, together with encrypted files and the threat of their publication – very strong pressure. We are developing this idea.*

Russian OSINT: *When you make enough money, do you think you can stop at the right time? Or the process associated with great risk and money is like a drug, addictive … ..*

REvil: *Speaking about myself, it would be high time to stop. There will be enough money for more than one hundred years. But there is never a lot of money – there is always not enough money.*

Russian OSINT: *The funniest resume / autobiography that you have come across from candidates / partners during your entire work …*

REvil: *There are actually a lot of them. The most average – I buy Dedicated files in a shop and I want to work with you. Rarely do really talented people actually write. I think everyone who has already been assigned to affiliate programs. Therefore, I personally think to rely on young people. Give them a chance to prove themselves. And if he does not show it – there are plenty of competitors, our demand is always high – no one is offended.*

Russian OSINT: *Is it possible to travel with what you do?*

REvil: *Impossible – definitely*

Russian OSINT: *How to recognize "Drovoruba" who wants to make friends with you? (sarcasm about the name of the rootkit)*

"The NSA has issued a warning about Russian intelligence (GRU) spy operations using a previously unknown malicious Linux kernel-based OS toolkit called" Woodcutter "

REvil: *He is very insistent on invading your sweet system with maximum rights. Egoist.*

Russian OSINT: *Describe your life in one word*

REvil: *More*

Russian OSINT: *Do you have a secret dream?*

REvil: *Billion dollars. Then 2 billion. If you are in a good mood – 5.*

Russian OSINT: *Where do you live: what metro station, street, house number?*

REvil: *Nikita Kuvikov or Nariman Namazov. Something in the middle of their habitats.*

Russian OSINT*: How did you come to such a life?*

REvil: *Once, when I was little, I installed a joint. And I liked it. Everywhere.*

Russian OSINT*: What advice do you have for beginners?*

REvil: To *eat more often, but better to drink. But seriously, study, read, try. Everything will work out, everything is real.*