THE EUROPOL PODCAST

OFFICIAL TRANSCRIPT

Ransomware: Your Money or Your Files!

Introduction

Bogdan B., Europol

REvil is one of the most known cybercrime organised groups that started their criminal activity with a ransomware as a service project. They have coordinated and organised with the aim of recruiting affiliates and, through their affiliates to, in fact compromise computer systems of large organisations.

Catalin Z., Romanian Central Cybercrime Unit

When we first saw the GandCrab ransomware, it was something quite unique, something quite new at the time.

Europol Narrator

Welcome to the Europol podcast, the official podcast of the EU agency for law enforcement cooperation. In this series, we shine a light on some of the biggest operations Europol has supported, and how we continue to fight organised crime.

Ransomware - Your money or your files!

Cybercrime causes all kinds of havoc, from power outages to crippling financial losses. It's a top priority for police forces in the European Union, and for the investigators here at Europol as well. But nowadays, it's not only the tech-savvy criminals that law enforcement needs to watch for.

Cybercrime services can now be purchased by paying a user fee, a rental fee, or a percentage of the criminal profits. Cybercriminal networks offer tools such as malware, ransomware, and distributed denial-of-service (DDoS) attacks online, especially on the dark web. This business model is known as crime-as-a-service, and it makes criminal services easily available to anyone, lowering the level of technical expertise previously required to perform specific activities.

The crime-as-a-service model allows the developers and the affiliates to share the criminal profits. In this episode, we're going to talk about a cybercriminal network called REvil, and an operation that saw Europol and its partners take down several prolific affiliates who were using REvil's services.

What is REvil's Crime-as-a-Service model?

Europol Narrator:

REvil was a notorious ransomware group. And their ransomware-as-a-service business model was pretty straightforward.

Step one: REvil operators develop a type of malware called ransomware, which encrypts files until a ransom is paid.

Step two: REvil's affiliates then pay to use the ransomware, and begin their campaign to compromise computer systems/networks, exfiltrate valuable data and, in the end, dropping ransomware.

Step three: if the attack is successful, the victim's computer files are encrypted. Only the ransomware affiliates have the key that will unencrypt the files.

The victims are then told to pay a ransom fee, otherwise their files might remain stuck behind the encryption forever, or published online by the criminals. It's a nightmare for the victims, and law enforcement had to act to shut down the affiliates if they wanted to damage REVil's criminal business model and deter other would-be affiliates. Attacks of this nature, by REvil affiliates and other groups too, were reported in all kinds of places:

A major currency exchanger in the UK was attacked, knocking their systems offline and effectively halting online banking for several major British banks.

Elsewhere, a widely-used network computing solution was also hit, with the ransomware spreading downstream to their customers. Several worldwide organisations using their services had no choice but to shut down their business entirely while they dealt with the fallout.

Cybercriminals even managed to attack a major technology firm, stealing the confidential schematics for their upcoming smartphones.

In this episode, we will talk about an operation that led to the takedown of several affiliates of this ransomware group known as REvil, or Sodinokibi.

Europol's involvement

Bogdan B., Europol

My name is Bogdan. I'm a specialist working at AP [Analysis Project] Cyborg.

Europol Narrator

Bogdan is a cybercrime specialist working at Europol headquarters in The Hague. And he'd been monitoring REvil and their affiliates for some time as part of this investigation:

Bogdan B., Europol

REvil was one of the most known and at the time was I would say number one in relation to a number of the affiliates that they got in the platform and the high level of victims they had at the time. So in our opinion, were the first ones that made this business model a standard.

So that's something normal for this kind of business at this point; to run it as a criminal company and recruit affiliates. And they were doing also PR on the cybercrime forums. They were post that they are recruiting affiliates. They would mention their conditions and what they're offering. And one of the things that they were advertising is stability, credibility that they would offer everything that the affiliates would want.

So they would have their own monikers on the forums and they would provide the customer support to the affiliates. For example, they had some issues with payment and technical issues with the malware. Then they will receive customer support from the administrators of the platform.

Europol Narrator

So REvil's a busy enterprise. In fact, they were doing many of the things a legitimate company does – offering technical support, building their brand through public relations, and carrying out recruitment drives.

But of course, REvil was working for criminal and nefarious purposes. And following a notification from an EU Member State, Bogdan and his team began investigating REvil and its affiliates.

Bogdan B., Europol

Yeah, well, our work started as all our operations, we get a notification from one of the Member States that this and the specific situation was Romania. That has sent us an internal notification in relation to the ongoing investigation they had.

When we saw the initial infections, we started the coordination at Europol, with all the countries that had active investigations at the time, European from the United States and some of them actually also from other countries in Asia. So we started the investigation and then we started to coordinate law enforcement at international level and provided constant support.

For this operation we had in place operational action plan, which targeted three main areas of the organised crime group. First was to identify, geo-locate and arrest the suspects. Second, to identify, disrupt and take down the infrastructure. And the third one was to follow the money trail and identify their financial assets and see.

So that is the standard procedure, I would say, investigative procedure that we implement in these kind of cases. And of course, how we actually implement them and how we do it, that's up to our investigative teams and their methods that are reinforcement for of us.

Europol Narrator

We'll hear more about the investigation from Bogdan later. But first, let's take a look at where and how this specific 'ransomware-as-a-service' business model came about.

GandCrab

Europol Narrator

REvil's efficacy was the result of experience. REvil was in fact a second iteration of a ransomware-as-a-business outfit called GandCrab, and they took the lessons from GandCrab forward when they formed REvil.

Catalin Z., Romanian Central Cybercrime Unit

I think with GandCrab, things went to a totally different level and I think they had quite a successful affiliation model and I think they also were keeping very well track on the activity of their clients so they'd be efficient and produce a good number of victims.

Europol Narrator

That's Catalin Zetu, a senior police officer from Romania.

Catalin Z., Romanian Central Cybercrime Unit

So my name is Catalin Zetu and I am currently working for a Romanian central cybercrime unit.

Europol Narrator

Catalin is responsible for investigating the types of criminal activity we're discussing in this episode.

Catalin Z., Romanian Central Cybercrime Unit

So working in the cybercrime field, obviously this is one of our mission and job is to look for new threats that are affecting Romanian systems. And during that kind of activities, we got reports first on GandCrab that a Romanian citizen or his systems were defective or infected with GandCrab ransomware. So basically I would say that's where everything began, getting a press report of the crime.

Europol Narrator

GandCrab ransomware was being rented out based on the ransomware-as-a-service model we described earlier - and it was being used for all kinds of attacks. But law enforcement eventually disrupted GandCrab's business model:

Catalin Z., Romanian Central Cybercrime Unit

So, at some point or during the investigation, multiple decryption tools were released or for the victims of GandCrab to recover encrypted files. And I think with those decryption tools, somehow the victims were more aware that the possible solution to that problem may be available to them.

Europol Narrator

Law enforcement had successfully released tools that beat GandCrab's ransomware, called decryptors – clever pieces of software that can unencrypt files and unblock systems. That meant victims infected by GandCrab could use a decryptor, instead of paying ransoms to criminals.

Catalin Z., Romanian Central Cybercrime Unit

So they were not being anymore because their activity was not too lucrative anymore. And also I think it was quite a big hit for the affiliates in the same time because they were also not doing any profit. And with each decryptor for the name of the gun club, the group was speaking, I would say a big hit.

So they went dark through a very bold, let's say, public statements saying that they have made the billions and they now look good to retired. But at the same time we had the feeling that this is not necessarily accurate and most probably, uh, a rebranding will follow.

Emergence of REvil

Europol Narrator

Catalin's suspicions of a rebranding would prove right, when the REvil group emerged and affiliates began using its ransomware for very large-scale attacks.

Catalin Z., Romanian Central Cybercrime Unit

I think there were also a lot of reports, security reports that they think this some similarities within the code and functionalities of the malware. But we didn't really rush into conclusions at first. We consider it like being separate, separate investigations.

We start noticing some overlaps with the actors involved. And for us with the Romanian investigation, we see it like our affiliates transiting from gang capital to it took that over passport.

Europol Narrator

GandCrab's ransomware-as-a-service business model was being refined by this new group. Like GandCrab, this new group had customer support helplines, making it easier for affiliates to get up and running using the ransomware. This new group, REvil, was also running recruitment drives on hacker forums. It looked like the expected rebranding had come. Catalin and his team started exploring leads, but this isn't an easy task in ransomware cases.

Catalin Z., Romanian Central Cybercrime Unit

So in the first term, I would say that we need to put all the pieces together. And when we're talking about ransomware, it's pretty difficult to collect usable evidence. So, you know, in investigations, you would need to gather evidence in order to attribute specific attacks. So with ransomware, there are very few pieces that can be followed up, and that's why there is in need of a specialised, very specialised and skilful people that can efficiently trace and attribute to a specific attack.

So at first, we as a Romanian Central Cybercrime Unit, we have built up partnership, solid partnerships at the international level with different other law enforcement agencies, but also at the national level or with different private partners.

But we also engaged with Europol that somehow made also the law enforcement cooperation. From Europol we got in touch with multiple other international law enforcement agencies and start deconstructing our cases and also sharing actionable intelligence so we can bring all the pieces together in order to have a successful operation.

Europol Narrator

The investigation was expanding as law enforcement built up a picture of the REvil ransomware group and its affiliates. As more agencies and experts got involved, it was only a matter of time before a breakthrough came and it would be time to act.

The breakthrough

Europol Narrator

Sure enough, a breakthrough came as the international cooperation progressed. Here's Bogdan again:

Bogdan B., Europol

That was a breakthrough moment of the investigation. I cannot provide more details, but I would say that we received intelligence from law enforcement agencies where it gave us a very good understanding how the organised crime group was operating and who was part of the affiliation group. And that intelligence was used further, also from the Europol side, to enhance it with our data sets that we had here.

And we managed to identify the suspects in a longer timeframe. It was something that we worked constantly since 2019 until 2021. So it's a lengthy process because there were a lot of affiliates.

Europol Narrator

Armed with solid intelligence and over 2 years of careful investigation, Europol and our partners on the case had been able to geo-locate several REvil affiliates, responsible for several serious cyberattacks. Bogdan was now ready to coordinate an Action Day from Europol HQ that would take these REvil affiliates, and any remaining GandCrab actors, offline.

Bogdan B., Europol
The law enforcement doing the operation targeted affiliates mainly and those affiliates were responsible for infecting thousands of victims and also responsible for receiving large sums of money from the ransom paid by the victims, so by stopping the affiliates, we actually stop some of the criminal activity. These are the ones that are infecting the victims. These are the ones that are compromising computer networks and then deploy the malware.

Europol Narrator
In November 2021, the partners were all lined up and ready to act in unison.

Bogdan B., Europol
In relation to the operation to the action day. We had 17 partners, 17 participating countries from all over the world and we had participating organisations such as Eurojust and Interpol. The arrests happened and in Romania we saw REvil as a continuation of GandCrab. So when we did the takedown, we had the actions in different countries that also targeted GandCrab.

And those actions were done in South Korea, Kuwait. Also, a suspect was arrested in Poland. And those operations were coordinated from Europol. We had the virtual command post set up which kept us in contact with the activities in the field. And of course before that we had multiple coordination calls and meetings with all the partners in this investigation.

Each country did their own house searches based on their own internal procedure, and of course, they seized the devices used by the suspects, found evidence of their criminal activity. Seize assets also.

Europol Narrator
So on the Action Day, a total of seven ransomware affiliates - suspected of being responsible for thousands of attacks - were taken in by the authorities.

As well as this action, a longer-running investigation into the people behind REvil itself was ongoing:

Bogdan B., Europol
Of course, the target for this operation was to identify an arrest in the field, but also to identify and arrest the administrators. I would have to also say that this is also ongoing operation. We had an operation in last year. But then it's not something that it's finished. It's something that law enforcement is still looking into and investigating further.

Europol Narrator
And the intelligence gained from the Action Days will be fed into this ongoing investigation.

Bogdan and his team at the Europol are investigating major threat actors across the European Union, and they conduct action days like this all year round as part of their work keeping the digital communities of Europe safe.

No More Ransom campaign

Europol Narrator

The arrest of affiliates is a key part of the action when it came to disrupting ransomware campaigns and preventing the attacks; but that's not the end of the story in this episode.

The "No More Ransom" website is an initiative by the National High Tech Crime Unit of the Netherlands police, Europol's European Cybercrime Centre, and a group of private sector IT security companies. No More Ransom helps victims of ransomware retrieve their encrypted data, but without having to pay ransoms to criminals.

Since its launch in July 2016, No More Ransom has helped more than 10 million people. The resources are available in 37 different languages, and it offers more than 136 tools capable of decrypting over 165 different types of ransomware.

When Europol and our partners took action against REvil, No More Ransom was a key component of the effort. As well as taking action against the criminals, law enforcement wanted to give support for the victims. And that's where private cybersecurity companies can play a key role in public safety. One partner in the REvil case was a provider called Bitdefender.

Bitdefender

Alex C., Bitdefender

My name is Alex Cosoi, and I'm the senior director for the investigations and forensics unit within Bitdefender.

Europol Narrator

Alex is a cybersecurity expert who works at the company Bitdefender. He leads a core team of expert analysts in Bitdefender's Investigations and Forensics Unit, who can offer technical expertise and other support for law enforcement investigations.

And like the victims of Gandcrab, law enforcement wanted to give REvil victims a way to unencrypt their files without paying a ransom to cybercriminals.

Europol Narrator

So they needed to make a decryptor, and this is where Alex and his team came in.

Alex C., Bitdefender

So basically when your files are encrypted, they are encrypted with the key, and they can only open to it with some other key. So they have that key. And the only way to decrypt your files is to obtain that key from the criminals. Usually you pay the ransom and they'll provide you with just the key or a decryption tool that contains that particular key.

But in other cases, you have to have a huge investigation, find the key and then create the decryption tool.

Europol Narrator

THIS was NOT easy – it took major inter-agency and international cooperation – but eventually law enforcement were able to get the Bitdefender experts what they wanted.

Alex C., Bitdefender

I think the total was 19 countries that actually participated. But in terms of organisations we were about 23. So one of them provided us with the decryption keys. So basically we quickly created the decryption tool based on those keys, and helped the victims out there.

Europol Narrator
With the tool developed, it was now time to get it deployed. But law enforcement need to act fast if they want to stay ahead of the criminals:

Alex C., Bitdefender
I think maybe a larger discussion would be whether if the ransomware group is still active, when you release decryption tool, they can actually change the keys or they can improve their ransomware, which means that that tool will not be useful for the new victims.

Europol Narrator
To factor for this, the operational teams knew that if they could get the tool onto a public space and announce it quickly, many victims could take action to get their files back. The tool went onto the No More Ransom Website, and it was time to disrupt the ransomware affiliates who'd been extorting businesses and organisations all over the world.

Alex C., Bitdefender
So basically, we have to do a public communication saying that there is a tool available. It can be downloaded either from the normal ransom initiative or from our website. Other partners that were involved in investigation. They also did similar press releases in their countries, some social media.

And then we started to see victims coming into to download the tool. If they had trouble with the tool where there were cases where the files were actually encrypted by two different ransomware families. So for them, it was a bit more challenging. So once we release a tool, there's usually communication, direct communication with the victims whenever they have some issues, for instance.

Europol Narrator
And the results speak for themselves:

Alex C., Bitdefender
We helped out 1400 organisations to decrypt that their computers. And if they would have paid that would have sum up to half a billion dollars. So it's a very lucrative business for ransomware. It affects people and organisations all around the world especially when we talk to let's say critical infrastructure and it's a business that it's not going to go away.

Europol Narrator
And as for the people behind the cyberattacks:

Alex C., Bitdefender
So they stopped attacking anybody and then they reappeared and so on. So there was definitely a disruption because once the tool was out, they disappeared for a while. And now we see that several arrests follow the investigation throughout the world, actually.

Conclusion

Europol Narrator

Taking down these cybercriminals and affiliates is a major priority for Europol and our law enforcement partners. And Alex can explain why this malware is so dangerous for victims and lucrative for cybercriminals:

Alex C., Bitdefender

So basically, we actually did a study like a year ago or two years ago, and we asked about a thousand CISOs if their company would pay, whether their infrastructure gets affected with ransomware or not.

NARRATOR: A CISO is a chief Security Officer, and they're senior execs at companies and organisations who are responsible for all the cybersecurity.

Alex C., Bitdefender

And they stated that 50% of them they actually will pay. The reality is about 70% of them actually pay. So if seven out of ten companies pay, obviously criminals will stay to continue just business for them and will still make a lot of money. I mean, GandCrab stated that they made the 2 billion.

Europol Narrator

Europol's Serious and Organised Crime Threat Assessment, found that the number of ransomware attacks and the level of their sophistication is increasing. What's particularly notable is there is a growing number of attacks directed at public institutions and large companies. So law enforcement will continue to hunt down these cyber criminals and do its best to protect the individuals, organisations and businesses targeted by criminals.

To learn more about how to protect yourself from ransomware, visit the Europol website and search 'ransomware' for brochures, links and how-to guides on the topic.

And of course, there's the website for No More Ransom - NoMoreRansom dot org. Whether you're already a ransomware victim, or you're looking for ways to avoid ransomware attacks, the campaign has materials and software that can help.

Thanks a lot for listening, we hope you enjoyed hearing about this case. If you did, be sure to subscribe, rate and review the show on whatever platform you're using, and tell your friends about it on social media. We'll see you in the next episode.