Million-dollar deposits and friends in high places: how we applied for a job with a ransomware gang

By Cybernews Team

Published: 2021-04-21 · Archived: 2026-04-15 02:01:52 UTC

During an undercover interview, a CyberNews researcher tricked ransomware operators affiliated with Ragnar Locker into revealing their ransom payout structure, cash out schemes, and target acquisition strategies.

From a relatively rare threat just a few years ago to one of the biggest moneymakers for cybercriminals today - the meteoric rise of ransomware has cast a shadow of anxiety across businesses of all sizes.

And with the introduction of ransomware-as-a-service, the barrier of entry for getting in on the action has been lowered even further. So much so, in fact, that ransomware groups are now trying to solve their 'labor shortages' by recruiting new members on hacker forums, which are frequented by veteran and up and coming cybercriminals alike. But cybercriminals are not the only ones there.

Security researchers - us at CyberNews included - also routinely visit hacker forums for threat intelligence. And as we found out during this investigation, such visits can result in unexpected consequences for everyone involved.

Back in June 2020, while gathering intelligence on a popular hacker forum, we stumbled upon a peculiar recruitment ad seemingly posted by a ransomware group. To glean valuable insights into the ransomware operators' perspective, we decided to pose as a Russian cybercriminal and answered the ad in question.

To our surprise, we were invited to a private qTox chat room for a 'job interview' with people who claimed to be associated with an infamous ransomware group. There, we met the threat actors who were allegedly responsible for running a ransomware affiliate operation for more than 10 years.

What follows is the story of how we answered the partnership posting and what we found during our interview with an affiliate group of the REvil and Ragnar Locker ransomware cartels.

About this investigation

To conduct this investigation, one of our security researchers answered a ransomware affiliate ad on a popular hacker forum, posing as an experienced cybercriminal. By conversing with the potential partners in crime, the researcher attempted to learn about the structure and techniques used by the threat actors, as well as their past and future targets.

Ransomware cartel looking for partners in crime

In June 2020, a user called 'Unknown' submitted a rather peculiar post on a popular Russian hacker forum, looking for people to join their 'affiliate program.' In the world of crimeware-as-a-service, an 'affiliate' is a person

who uses malicious tools provided by another threat actor to commit cyberattacks against individuals or organizations of their choice - in return for a cut of the profits.

What made this particular posting stand out from your typical crimeware-as-a-service ads, was the fact that it seemed to be coming from REvil - also known as Sodinokibi - one of the most notorious ransomware groups in the world.


Ransomware collaboration advertisement on a forum

REvil is infamous for being the very first ransomware-as-a-service cartel to use the so-called “double extortion” tactic, whereby the group (or one of their ‘affiliates’) attacks and locks a company out of their own files, and then gives the owners an additional incentive to pay the ransom by threatening to sell or even auction the stolen data off to other cybercriminals.

Interestingly, it was sometime in June 2020 - the time when this story takes place - when REvil first used the double extortion tactic as it began auctioning off data stolen from a Canadian agricultural production company that refused to pay a ransom.

The terms of the deal

The potentially big name behind the posting wasn’t the only thing that piqued our interest. The terms of the offer seemed rather tempting as well. According to the ad, the affiliate, if accepted, would get up to 70-80% of any successfully paid ransom, while REvil themselves would keep the other 20-30%.


The terms of the deal

Clearly, the offer was good. Perhaps, even too good to be true. So how could potential partners in crime be sure that the ad was posted by an actual representative of the REvil cartel, and not by a scammer, a security researcher, or an undercover Interpol agent? Well, money talks, and it seems that the author of the post spoke it fluently:

> *To prove that the job posting was legitimate, the recruiters publicly deposited $1 million worth of bitcoin into their forum wallet.*

Prior to the massive deposit, the posting had our curiosity. Now, it had our attention.

-Are you gangsters? -No, we’re Russians

Surprisingly, having the right skills and experience was only part of the application process. The recruiter was adamant about the fact that the potential partner also had to be a native Russian speaker.

To weed out impostors, the ransomware gang would ascertain the candidates' identity by quizzing them about Russian trivia, including Russian and Ukrainian history, and folk/street knowledge that "cannot be googled." Naturally, we took up the challenge.

So, could we successfully pose as an experienced Russian threat actor? Could we ace a job interview with a group of cybercriminals? What could we learn about this ransomware affiliate operation?

Needless to say, we couldn't wait to find out.

Getting in

Note: *Original communication with the ransomware operators was conducted in Russian and has been translated to English for the purpose of this article.*

Having decided to answer the ad, we posed as a person interested in working with the ransomware operators. We sent them our contacts on qTox - a chat app popular among hackers for its use of a peer-to-peer chat protocol over Tor - and waited.

A couple days later, we received a message from an unknown user:


Message from unknown user

They asked us whether it was us who had posted the reply on the hacker forum, and asked us to add them as a friend. After we accepted their friend request, we were added to a group conversation that had one other person present in the chat.

Both were using vague, unidentifiable nicknames (one of which was just an emoji) that divulged as little information about the people behind them as possible: a time-honored tradition among cybercriminals whose communities are known for their culture of mistrust and suspicion.

From the conversation that followed, we were able to gather that these people belonged to one of the hacker groups affiliated with REvil and Ragnar Locker groups.

The threat actors explained that they were working with Ragnar Locker - a popular ransomware suite deployed against devices running Microsoft Windows - and that the team already had four active members. If we were able to ace the interview, we'd become the fifth member of this team.

After complimenting our fake portfolio, Emoji tried to wow us by bragging about the group's supposed biggest ransom payout: a whopping $18 million. Once Ragnar Locker took their 30% cut, the group divided the remaining

70% of the massive ransom, with each member taking about $2.5 million home.

According to the other threat actor, the group has had a long and storied 11-year-long career, backed by a “flawless reputation.”

The conversation went on for some more time as we discussed various technicalities and the skills we would provide as the new member of the team. We won’t bore you with all the little details.

In short, the threat actors were interested in whether we would ‘clear the coba’, which meant that they were using Cobalt Strike in post-intrusion exploitation stages. Cobalt Strike is a legitimate threat emulation toolkit used by penetration testers and red teams to assess vulnerabilities and test their systems.

On the other hand, Cobalt Strike is also famously used by cybercriminals, including ransomware operators and their affiliates, due to its flexibility and ease of use. The toolkit has so-called beacons that offer an attacker a number of functionalities such as remote code execution, privilege escalation, lateral movement over the network, and more.

Cashing out

With the technical side of things covered (for the time being), our conversation with the threat actors turned to money. Namely, how we were to receive the crypto from successful extortion attempts (bitcoin accounts for about 98% of ransomware payouts due to it being harder to trace) and how we could then turn that crypto into traditional currencies.

Apparently, the cybercriminals had an insider contact at a cryptocurrency exchange who specialized in money anonymisation and would help us safely cash out (and maybe even launder) our future ransom payouts.

We were told that if we wanted to easily cash out our future ‘earnings’, we were to open an account on that crypto exchange, deposit our ransom payouts there and convert them to USD in multiple ‘small’ instalments of 1$ million. This would be done so as to not raise suspicion or affect the price of bitcoin on cryptocurrency markets that could negatively react to sudden large sell-offs.

Once the full multi-million ransom payout was transferred to the crypto exchange and sold for USD, the insider contact could then convert it to cash and deliver it anonymously to a place of our choosing - for a 4% fee.

Interestingly, the recommended cash out amount was also a manageable $1 million per delivery, which would weigh about 10 kilograms (~22 lbs). According to the threat actors, anything heavier than that would be rather inconvenient, not to mention incredibly unsafe, to transport in person.

During our lengthy back-and-forth, we also attempted to obtain some information about the group's past escapades. When asked about former targets, however, Emoji was tight-lipped and did not want to divulge anything incriminating.

Having failed to goad Emoji into revealing the group's past crimes, we then continued our discussion about the specifics of cashing out our future 'earnings' from the group's insider contact at the crypto exchange.

As the interview drew to a close, we decided to see if our interviewers weren't lying about their ransom cash out scheme. After a brief visit to the exchange indicated by the threat actors, we came to a chilling conclusion: they must have been telling the truth.

...The end?

Following our visit to the crypto exchange, the threat actors had started discussing several potential targets for ransomware deployment and asked us to help them carry out attacks against them. Needless to say, we wouldn't do that.

Before we ceased all communication with the group, we managed to glean several takeaways about these threat actors:

- They carefully select their targets over a long period of time, prioritising companies whose day to day operations the attacks would affect the most.
- The group conducts exceptionally thorough preparation before attacking, including researching their victims' financials and estimating how likely they are to pay the ransom.
- The threat actors usually begin their attacks on Friday nights after the personnel of the target company leaves the office. These attacks continue throughout the weekend, when the probability of being detected is much lower due to the absence of cybersecurity staff or network administrators on the premises.

Protecting against ransomware attacks

In light of these findings, our main recommendation to businesses that wish to avoid being targeted by ransomware gangs is to employ a zero-trust security policy by verifying any and all incoming connections inside or outside the company.

Another crucial best practice is making sure to regularly back up company data so that business operations aren't interrupted by ransomware attacks.

However, passive countermeasures are only part of the solution. Businesses will also need to take a proactive strategy that includes:

- Blocking malicious websites and filtering allowed file types to prevent malware from being delivered to company devices
- Keeping software up-to-date, enabling 2FA, and using a secure VPN to protect devices with remote access
- Patching VPNs, firewalls, antivirus, devices and infrastructure, keeping obsolete platforms segregated to prevent the spread of malware through the company network.

context-specific and locally validated to ensure that we are not perpetuating health inequities," Elish explained.
