Nov 12, 2021 08:09 GMT

“We wait, because we know you” Inside the Ransomware negotiation economics

Authors: Pepijn Hack & Zong-Yu Wu

An organization hit by a ransomware attack finds itself in a nightmare.

Business operations come to a standstill, systems are shut down, data is inaccessible.

Action must be taken immediately.

What exactly happened? Is there any information left to secure? Who should inform whom? Can we do it ourselves or do we need a specialist?

And then the next moment the message arrives, in which the attacker announces the amount of money that is to be paid to obtain the key to recovery.

To make matters worse: in more and more cases not only are whole systems encrypted, but sensitive data has also been exfiltrated and the attackers threaten to publish or sell it if payment is not made. An additional means to reinforce the extortion.

And then the dilemma: to pay or not to pay?

Paying a ransom or negotiating with criminals is problematic to say the least. Still, a significant percentage of ransomware-affected businesses see no other option than to negotiate and in the end pay the ransom. But not much is known about the economic backgrounds of digital extortion and about the negotiation strategies in the case of digital extortion.

That gap prompted us to investigate negotiations that take place after the decision has been made to pay a ransom after a successful ransomware attack.

More than 700 cases

Our researchers looked at how opponents use economic models to maximize their profits and also examined the victims' position during the negotiation phase and what strategies ransomware victims can use to level the playing field as much as possible. For this, more than seven hundred attacker-victim negotiations were collected between 2019 and 2020.

The ransomware groups investigated were among the most notorious. The researchers had access to the negotiation process between these groups and their victims and, in addition, a large amount of data was examined. The negotiations under investigation were partly done by a negotiator and partly handled by the victim itself. In many cases, however, it was not clear, a negotiator does not always indicate that he is from an external party.

Unlevel playing field

All companies or institutions that fall victim to a ransomware attack are completely in the firm grip of the attacker. Not only because the organization and its operations are completely shut down due to the attack, but also because in most cases the attacker has learned a lot about the victim. So much so, the research shows, that in most cases attackers have a good idea of what amount will ultimately be paid (if paid). The attacker knows a lot more about the victim, while the victim knows almost nothing about the attacker. And the attackers have much more experience in negotiating than the victim. If the attacker does well, they always win.

Still, the playing field is not as uneven as it may initially appear. Criminals are after money and a victim who pays less than the amount originally requested is still better for the criminal than a victim who does not pay at all. The latter would be a waste of time, effort and money - after all, the attacker will have to invest time in launching the attack. Hence, criminals negotiate with their victims. Moreover: the attackers are people and people can be influenced and make mistakes.

More than 50% 'discount'

Negotiations should yield maximum profit for the attacker, while the victim is after paying as little as possible. The researchers have seen that after negotiating, the victims managed to get between 10% and 90% in a 'discount' - the term used by the attackers. In two thirds of the cases examined, this discount is more than 50%.

Once payment has been made, the ransomware groups investigated have in all cases adhered to the agreements made. However, in one of every two cases, the decryptor that was sent was not very efficient, which led to calling on an external specialist to build a better one.

We also found that the same attackers (at least until now) have not come back to try again. What was found was a rare case where two groups had gained entry at the same victim at the same time and these two agreed to divide the loot.

The importance of time

In addition to money, time is also of the essence to both the victim and the attacker. The attacker wants to collect the ransom amount demanded as soon as possible. The victim needs time to map out exactly what happened and what sensitive data may have been obtained by the attacker. But the victim also needs time to collect the ransom (in bitcoins) and the attacker knows that too. Pressure the opponent to pay as soon as possible. For example, by threatening to leak documents or by threatening to double the ransom if payment is not made before a certain deadline. In many of the cases investigated, the attacker remained willing to extend the deadline. This is to the advantage of the victim and provides more time to map out the situation and work out different strategies.

Double extortion

The research findings also apply to negotiations in case of other forms of extortion - the 'double extortion' – where there is not only encryption of data, but also the threat of publication or selling of stolen data. In that case, the attacker has a stronger trump card than with ransomware alone, which in principle could be recovered. During most of the negotiations that were investigated, threats were also made to publish data in order to put pressure on the victim. If it is only a matter of publishing data (see SnapMC for example), the factor time plays a very different role. After all, the company is not out of business during this negotiation, which can lead to a much longer negotiation.

Not powerless

The research shows ransomware gangs have successfully developed their own negotiation and pricing strategies to maximize their profits. This is done based on the financial position of their potential victims, which they can map out before activating the ransomware and exfiltrating data. This leads to an unlevel playing field, as can be expected from criminals.

Perhaps the most important outcome of the study is that despite the unlevel playing field, victims are not completely powerless. The research report provides a comprehensive overview of the strategies victims can follow to minimize some of the adversary's advantages as well as practical tips about the negotiation process itself, all illustrated with examples from practice.

Never attractive

We hope that by making this investigation public, it will strengthen the defensive side of the cyber security landscape. With good negotiation tactics, in most cases 50% or more of the ransom can be recovered. This raises the question of whether the publication of the findings of the investigation and the negotiating tips will make it more attractive to pay a ransom.

For starters, paying ransom is never attractive. It always comes with a lot of stress and even half the ransom can be quite a drain. Moreover, the ransom that is ultimately paid is only a (small) part of the total damage that an organization incurs from a successful attack. A more significant effect of the research is that in those cases where victims consider paying, they have better chances of paying less to criminals.

We advise not to pay a ransom (ransomware, data leakage) because this maintains a criminal industry. We can however imagine that organizations may have to make a different assessment. Each case will have to be assessed on its own merits by affected organizations: pragmatic considerations can outweigh principles and we support customers in the consideration process with regard to factors that may influence the decision (whether or not to pay).

Society might get tired of ransomware

Looking ahead to the future of ransomware, it looks like we're not quite there yet. We think that as more and more companies become victims of ransomware, society will grow tired of it. We may then witness a development that companies will pay less often, which in general would of course be better. On the other hand, criminals could become more aggressive in their extortion, or lower their ransom amounts enough to make payment much more attractive. But even then, negotiation will still benefit the victim.

A bit of hope comes from some recent successes by law enforcement agencies. In November 2021 Romanian authorities arrested multiple individuals suspected of deploying the REvil ransomware on victims' systems as part of operation GoldDust. This operation included authorities from 17 countries which joined efforts with Europol, Eurojust and Interpol. Similarly, in October 2021, another police cooperation between eight countries led to the arrest of twelve suspects that allegedly were part of a worldwide ransomware network. During this investigation multiple companies could be warned that ransomware was about to be deployed on their systems preventing millions of dollars of damages.

Interested in reading the full research report? It is available here

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750