CYBER HERMES

Cyber Hermes:

Ransomware Negotiation

Case Study

January 2022

Executive summary

Cyber Hermes: Ransomware Negotiation Case Study provides an anonymized view into a successful negotiation process when the negotiator was able to reduce the price eightfold while regaining access to all files.

Key figures:

- It took roughly a month to come to an agreement
- The initial demand of $4M was lowered to $0.5M
- The files were successfully restored, and the provided report helped to fix the root cause and improve security posture against future attacks

Detailed view

A US-based company in the entertainment industry with a revenue of $50M+ was infected with a prominent ransomware variant in the beginning of December 2021. Upon following the ransomware note and contacting the group, the initial message received was as follows:

> Due to poor security of your networks, we have downloaded your critical information with a total volume. This information includes personal data of your customers, employees, and vendors, as well as your legal, financial HR, IT, audit, and compliance directories (among other files). We obtained personal documents, phone numbers, contact information, consolidated financial statements, payroll, and banking statements.

The offenders offer a decryption tool, a security report of how the intrusion took place, and a promise to delete the leaked data in exchange for $4,000,000.

As this is a routine procedure, they additionally describe how the victim could verify the veracity of their claims:

> We will first give you a file tree to demonstrate which files we downloaded from your network. Then, you can chose certain file names from this listing and we will provide you with these files to prove that we have them. Then we transfer all the files that we have back to you and delete them from all our

> hustings and servers, making sure that you are the only one who has access to them.

To sound more persuading, the operators draw a picture of the potential risks associated with the publication of stolen data as a nasty “bonus” to previously encrypted files:

> At this point, all off your files are about to get public on our blog and will be available for anyone, including darknet criminals who are eager to abuse your information for their own evil purposes like social engineering attacks against your customers and vendors, spamming, and other bad actions. Your customers, vendors, employees, and investors (lists are available from you inner documentation) will also be notified by us about the breach. This way then can know what to do, since their private data is getting public. It goes with out saying that this privacy violation will lead to long-term legal, regulatory, financial, and reputational damages, including lost contracts and class action lawsuits from those whose info was exposed.

Finally, the initial message concludes with reassurance of their care of reputation and a promise to keep their word:

> THERE IS NO WAY that we will not fulfill our promises after you pay. To put it simply - the chances that Hell will freeze are higher then us misleading our customers. We are the most elite group in this market, and our reputation is the absolute foundation of our business and we will never breach our contract obligations.

At that stage, the *Ransom Negotiation protocol* comes into play. Upon meeting with the Executive team, reviewing what’s known at the moment, and outlining the constraints and the impact of either scenario, a reservation price (the one which the company is actually willing to pay) is defined.

Then, two parallel activities begin:

- internal initial preparation for the payment, such as putting aside the budget and setting up a financial infrastructure to convert the money into cryptocurrencies; and
- first contact with the hackers.

The client expresses interest in reaching the agreement and uses counter-anchoring technique by offering $25,000. While it is obvious that the hackers won’t accept this offer, it helps to establish a dialogue and provide a lower limit of the negotiation window.

The ransom operators respond with more threats and try to show how public release of the data will bring reputational damage to the company:

```
Do you think your clients and employees will be happy about it? Even if they will, the GDPR guys will not. There is a million regulatory acts and govt bodies that punish for data exposure. And on our side we will make sure to make it as public AF.
```

They furthermore share a private blog post with a portion of sensitive data that "*will become public unless you pay ASAP*".

At this moment, the victim conducts a so-called "proof-of-life" by asking to decrypt a few files and confirms the validity of the published data. After a few days to review the files and agree on the next steps, the negotiator offers the second non-monetary benefit: *willingness to close the deal quickly*.

The attackers agree to reduce the price by 25% and reiterate their promise to provide the decryptors, delete the files with a proof, and guarantee that the gang will no longer attack the company.

Couple of days later, the victim again expresses a desire to reach an agreement and declines the offer, citing their financial situation and the nature of the business. This triggers an extra 25% drop, to $2,000,000:

```
Given the Christmas holidays and your small company we can make you 50% discount and our price now for you $2,000,000. You must do the payment until 12.31.2021. After that all your data will be published and we will not get the decryptor.
```

The negotiator politely thanks them for the discount and finally counters with a $100,000 offer. This, combined with a virtual promise to pay, places the ball on the ransom operator's side. A week later, after "*taking several loans*" and firmly standing on $200,000, the hackers yield yet another $500,000 decrease. An important technique here is reiterating the price of the data *for the attackers* and insisting on the business nature of the deal.

Even though this might seem counterintuitive, in most cases, *time works in favor of the negotiators*. Going back and forth for another week and rejecting

offers above the reservation price finally leads to the acceptable price of $500,000.

At that stage, instead of simply accepting the offer, the negotiator requests the decryption of extra files and explicitly clarifies the terms of payment. The gang confirms what happens next:

```
After the payment:
1. You receive decryptors (windows and linux OS).
2. Your hided page will be totally deleted from the blog.
3. ALL your data will be deleted.
4. Consequently, you will receive a full deletion log.
5. You will get penetration report and recommendations how to avoid such a situations in future.
6. You receive a guarantee that anyone of our cartel will not NEVER attack you again.
```

Finally, after the successful payment, the hackers provide the decryptors, confirm the deletion and send an intrusion report that involved such techniques as phishing and business email compromise as the entry point. This information was included in the *Executive Negotiation Report* along with all the gathered evidence for an official claim.

Conclusions

Comprehensive preparations, keeping the negotiation professional and not allowing emotions to enter in play help to successfully negotiate significant discounts and many times allows quick recovery after the breach with minimized impact.

Cyber Hermes recommends to avoid paying the ransom whenever possible, and to focus instead on preventing the unfortunate event from happening. We offer a premier service **Virtual CISO** tailored to the needs of your business, and conduct a rapid **Breach Preparedness Assessment** to ensure the most common security failures are fixed before it's too late.

If payment is your only option, **consider ransom negotiation** as an effective mechanism for lowering the price while ensuring an unbiased professional approach to maximize the chances of successful recovery.

About Cyber Hermes

Cyber Hermes OÜ is an Estonian cybersecurity company specializing in cyber crisis management, and specifically ransomware research, negotiation and prevention.

We assist businesses in developing their first security programs, preparing for a security incident, and minimizing the impact of the breach if the worst-case scenario has already occurred.

Headquarters

Sepapaja tn 6, Tallinn, 15551, Estonia
Email: info@cyberhermes.com

In a cyber emergency?

Our 24/7 response team:
urgent@cyberhermes.com

Follow us

Linkedin: https://www.linkedin.com/company/cyberhermes
Twitter: @cyberhermescom