NORTHWAVE
Intelligent Security Operations

TALES FROM THE TRENCHES II

THERE'S A NEW KID IN TOWN: TRUSTEX RANSOMWARE

SEPTEMBER 2020

ROELAND KLUIT, NORTHWAVE

NEVER WASTE A GOOD INCIDENT

Northwave believes that there is real opportunity in learning from cyber-attacks and their incident response cases. More adequate cyber security strategies can be developed by analyzing these cases. In our 'Tales from the trenches' series of whitepapers, we do just that.

This is the tale of a ransomware attack in which Northwave's incident response team encountered a new ransomware family we called Trustex

BAKERY IN THE HOT ZONE

On a Friday morning in September, employees of a Dutch industrial bakery are getting started for today's bakes. The startup is almost like any day; however, they seem not be able to access the desktop machine used to maintain the daily planning information. Coincidentally, the crew manager finished early yesterday and prepared the bakes for this Friday. Hence, today, production starts as normal.

At the same time, other employees find out that almost all computers in the planning and financial administration departments are unavailable. The computers have been shut down along with the Internet connection, after the IT Staff got indication that the company have been struck by a ransomware attack.

When the IT staff turns to their server platform to check the backups, they discover that all the drives, containing their backups, on their NAS systems are empty and files on the server systems are all encrypted. Their options to restore to normal operation are now limited. Today's production might be fine, but all other processes are down. And there is no planning prepared for next Monday...

INFILTRATING THE NETWORK

To dig a little into the source of the incident, Northwave's incident response team found out that the company's external bookkeeper routinely performs accounting tasks for bakery, he needed access to the Accounting software to do so. To make the bookkeepers life easy (and the entry very simple), a terminal server was put in place and connected to the Internet on a custom port.

An attacker found the open port where the terminal server was listening for incoming RDP connections. A brute-force attack harvested the (relatively weak) administrator account on this server. This was not too complex, as the administrator account was not renamed and all server system had the same simple password. One that resembled a custom written format of the Active Directory domain name.

A ransomware attacker usually wants to infect as many systems as possible to effectively halt the business process and urge the victim to pay the ransom. In this case, this was quite simple for the attacker as all the keys to the castle were basically handed over on a silver platter.

After some looking around on the network, using some off-the-shelf administrative tooling, the attackers identified the various systems on the network and identified the backup volumes. First, they erased the backup volumes. Next they used PSEXEC together with the administrator account to push the ransomware out to all endpoints. They activated the encryption process, and after a few hours, all the systems where encrypted by their ransomware...

WHAT SHOULD YOU CONSIDER?

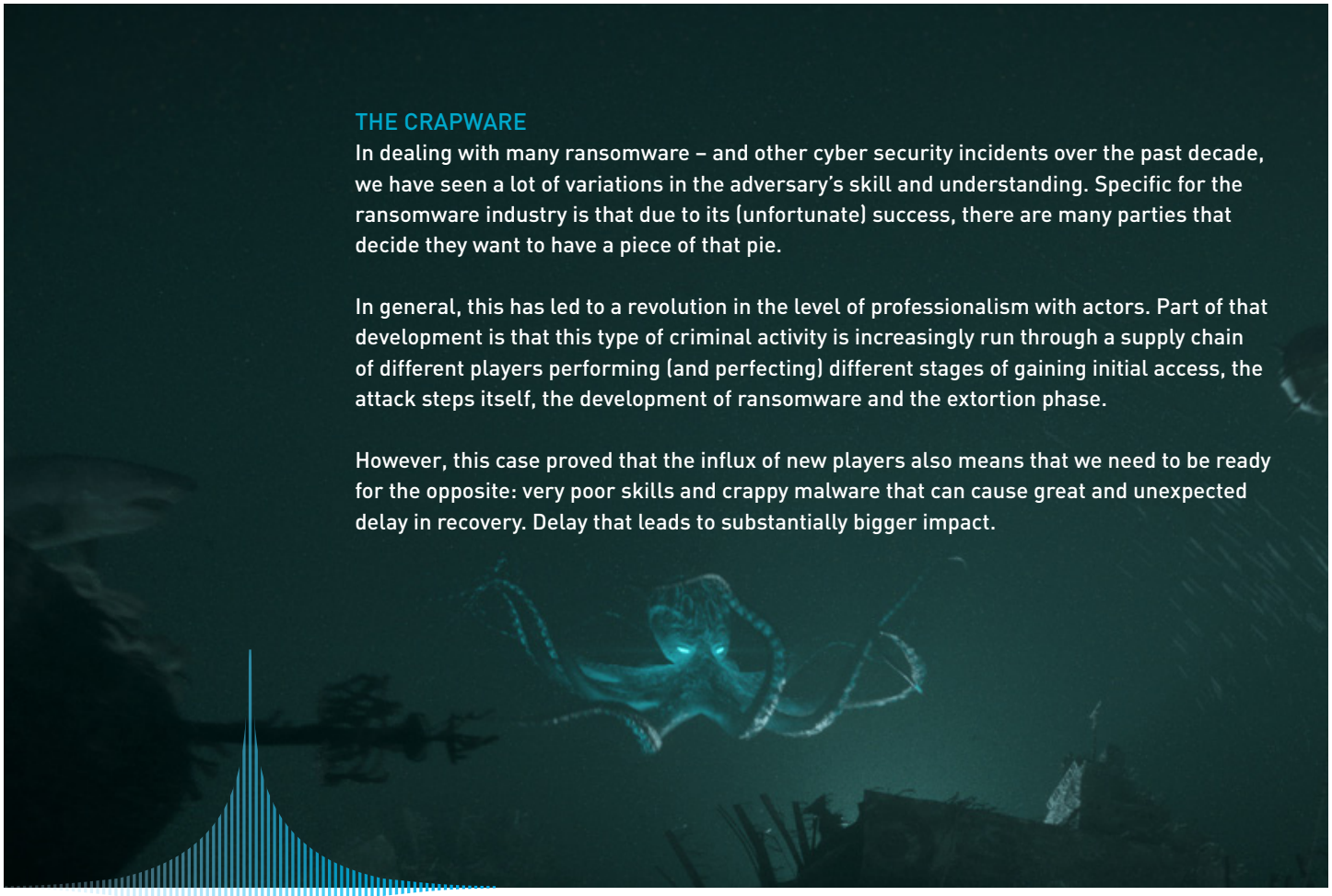
When an organization is hit by ransomware there are a lot of thing to consider. It is most commonly not as simple as to pay or not to pay. Businesses must do their day to day work to keep processes and production running. But there are ethics involved too. When considering steps to take when your organization is under attack, it is not just about the amount of money

the attacker is asking. Even if the ransom is payed there is no guarantee your data will be recoverable, and the attacker will delete the copies they created. Some companies refuse to pay ransomware regardless of the price because they do not want to support crime. They accept the data-loss, data exposure and additional cost to get the organization back into business.

Besides the main question about ethics, you must consider the amount of money you are willing to pay for the data encrypted. The effort that is needed to do the recovery is mutely important: are systems rendered unbootable or do machines have unique encryption keys, this will all increase the effort and time needed to return the systems back to operational state.

When the ransomware is from a known family, you can navigate on the knowledge from companies like Northwave, the known common pitfalls and shortcomings. However, when there is a new variant, unpredictable challenges can occur. Do look for red flags like the previously mentioned per-machine encryption keys, boot configuration corruption and brand-new unknown attacker groups

- **DO I HAVE BACKUPS?**
  The first thing to ask yourself is, do I have ransomware resistant backups. If you do not have such backups, it probably is not possible to regain access to your data and files other than to pay the ransom. Otherwise you have to accept the loss of data.
- **CAN WE RESTORE THEM IN TIME?**
  More and more organizations are returning to tape-backup in case a ransomware attack hit the organization. When doing so, they find out that restoring the data of their tapes takes weeks or even longer. They do not have procedures and software in place to perform the restore - this pushes the start of the restore even further back. An unacceptable timeframe for most businesses.
- **HAS THE ATTACKER EXTRACTED ANY DATA?**
  In more and more ransomware cases the attacker also extracts a lot of data from the organization. When you do not pay the ransom, they will either auction off your data or publish it on the Internet.
- **HAS DATA BEEN MODIFIED?**
  When the attacker intruded into the network, did they leave anything behind to regain access at a later stage? Did they modify any data in the network? These are important questions that might impact your organization for a long period of time as you will need to consider rebuilding systems, checking integrity, and keeping a close look on the environment for suspicious behavior.
- **IS THE ATTACKING PARTY KNOWN TO ACT IN 'GOOD FAITH'?**
  In some case the attacker does not actually provide recovery keys. Commonly there is some sample decryption of some files to prove they possess the decryption keys before a payment is made. Even if they demonstrate their ability to decrypt your data, you have absolutely no guaranty if the attackers will provide the key and subsequently delete all copies of the data they might have after you have paid the ransom.
- **DOES THE DECRYPTION ACTUALLY WORK?**
  Sometimes the quality of the ransomware is very poor – an example will be addressed further on in this document – and will cause permanent damage to the data. Even after paying the ransom and running the decryptor, you will not be able to go back into business immediately. Fixing corrupted database files and inaccessible machines will need a lot of additional tooling and technical know-how to get them back into a working state.
- **WHO AM I PAYING?**
  When a ransom is payed, you are actively supporting criminals. Are you paying some foreign hacker who wants to pay his new car using your ransom money? Or are you paying money to something more disturbing like a terrorist group that is using ransom money to fund their offenses. In any case, you probably will not be doing it with your Mastercard.
- **HOW DO I GET THE CRYPTOCURRENCY NEEDED?**
  When you have to pay the ransom, the payment itself can be challenging. When you have to pay 1.5 million dollars in bitcoin, you cannot just go to your bank and order some. You probably need some help on how to buy them and how to transfer them to the attacker. Due to new more stringent monitoring on cryptocurrency laundering fraud this becomes more challenging each day.



THE CRAPWARE

In dealing with many ransomware – and other cyber security incidents over the past decade, we have seen a lot of variations in the adversary's skill and understanding. Specific for the ransomware industry is that due to its (unfortunate) success, there are many parties that decide they want to have a piece of that pie.

In general, this has led to a revolution in the level of professionalism with actors. Part of that development is that this type of criminal activity is increasingly run through a supply chain of different players performing (and perfecting) different stages of gaining initial access, the attack steps itself, the development of ransomware and the extortion phase.

However, this case proved that the influx of new players also means that we need to be ready for the opposite: very poor skills and crappy malware that can cause great and unexpected delay in recovery. Delay that leads to substantially bigger impact.

To get back into the case of the Bakery, they had no other option than paying the ransom to get back to their data. Their data got encrypted and the attacker deleted the backups.

TRUSTEX

When we performed initial triage on the ransomware note and encrypted files, we found no relations with known ransomware, nor any options to decrypt the files without a paid decryptor at this time.

The attacker had to be contacted through email, as stated in the ransomware note. After some negotiation about the price, the ransom was paid. The decryption process could now start. However, this turned out to be far from trivial and intrinsically less user friendly then in other cases... Apparently, this 'modern piece of art' generated a unique key for each time the encryptor it executed. Resulting in the need of a readme.txt file (containing the Key ID) and an encrypted file to be send to the attacker to generate a decryptor for each machine.

To make matters worse the ransomware also encrypted the boot volume resulting in unbootable systems. After a manual process of booting the system into Windows PE we could collect both a readme.txt and encrypted file - for each machine in the company. Quite some time after sending the collected files to the attacker, we finally received the decryptors. As all the systems were rendered unbootable, we had to start over the process of booting the systems one-by-one.

At encryption time, the ransomware did also encrypt the boot partition. The attacker probably improved their code after the encryption. When running the decryptor, the boot partition was not decrypted. We added extra steps to the recovery process to force the decryptor to include the decryption of the boot volumes which solved the issues for the UEFI machines. However, even rebuilding and fixing the boot settings did not brought BIOS machines back to a bootable state.

But this was not the worst of the issues that we encountered. After decrypting the MS SQL databases, which are part of their business applications, the SQL services refused to start. The database logging files were corrupted. During the process of the ransomware performing encryption on the SQL transaction log the file was modified by the still running SQL service. This resulted in permanent file corruption. Without a valid log file, you cannot start the database. With the use of professional recovery software, the supplier managed to recover the data. However, at a significant extra cost.

And there are more of them: on the Domain Controllers, the Active Directory services did no longer function due to corruption. Complete partitions on the fileserver did not decrypt due to multiple executions of the ransomware encryption software and on other systems random files did not decrypt at all, even after multiple attempts...

The quality and support of the ransomware was rubbish. A lot of extra damage has been caused by creating difficulties both before and after the decryption. Also, a lot of effort was needed to restore the corporate database servers and other systems back into production. Some of the data was even lost forever due to encryption or decryption errors.

MANAGING A RANSOMWARE CRISIS

When considering steps to take when your organization is under attack it is not just about the amount of money the attacker is asking. Even if the ransom is paid there is no guarantee your data will be recoverable, and the attacker will delete the copies they created. Some companies refuse to pay ransomware, regardless of the price, because they do not want to support crime. They accept the data-loss, data exposure and additional cost to get the organization back into business.

Besides the main question about ethics, you have to consider the amount of money you are willing to pay for the data encrypted. The effort that is needed to do the recovery is mutely important: are systems rendered unbootable or do machines have unique encryption keys, this will all increase the effort and time needed to return the systems back to operational state.

Dealing with a cyber crisis means thinking in scenarios and separating assumptions from facts. Here are some key points taken from many incidents, including this one, that you can feed into your scenarios. In a life situation, or in a cyber crisis exercise. They will also proof valuable in evaluating and strengthening your security controls.

DEFENDING YOUR ORGANIZATION

For a company it is important to defend themselves to cyber-attacks like ransomware. When your company is hit by such an incident the attackers do not hesitate to ask enormous amount of money. Northwave has seen ransom demands for many millions of dollars. This besides the cost off lost production and recovery. Imagine if you would have only invested half of that money into defense. To protect your company, there is not a simple silver bullet solution. The protection of your company must be achieved over multiple layers. Not only the technical aspect should be addressed. We list some of the options you should address:

- **SHIFTING FOCUS**

  Management within organizations are commonly not deep into security. Messages about technical issues are not understood and filtered out in reporting to higher management. Management should actively manage security in the organization. Make sure you get the right security maturity information on your IT landscape. Also encourage the company to continuously improve the security posture.

  For users it is good to train them on cyber incidents, much like a fire drill. For instance, you can open a document you should not have opened or click on a link that you probably should not have. Management should create a culture where reporting such incidents is easy and never backfired at the person who made the mistake or reported it.

- **HAVE GOOD, RANSOMWARE RESISTANT AND QUICKLY RECOVERABLE BACKUPS**
  Make sure the backup solution you have in place is protected against deletion by an attacker. Ensure to test the restore of backups with the assumption the entire IT environment is unavailable. Implement the correct data policies to be able to meet the RTO and RPO as agreed in any SLA.

  When implementing a backup strategy, do not forget your online and outsourced services. These can become compromised too. Does the vendor take care of the backups or is that something the outsourcing company is responsible for?

- **SEGREGATE NETWORK AND CREDENTIALS**
  Most commonly attackers compromise a single account in the environment. This account is used a starting point to harvest other credentials. When using accounts only in predefined silos, the possibility for an attacker to steal such credentials, is reduced. You can take the Microsoft tiering model as a reference or starting point. To strengthen this defense, adding additional barriers in the network configuration, makes attacking the environment more difficult.

- **LOGGING AND MONITORING**
  Ensure to enable security logging and monitoring in the environment. Configure security events to be collected centrally. Check for unusual behavior. Is an account suddenly logging in to multiple systems? Are there a lot of failed logon attempts? Do we have detections in our antivirus? And so on. Use predefined rules in security tooling where possible. Do not forget to include your cloud environment.

- **IMPLEMENT UPDATES AND LIFECYCLE MANAGEMENT**
  The management should dictate a good lifecycle management and ensure there is capacity and money to keep the IT environment up to date and current. Vulnerabilities in software are one of the easiest ways in for an attacker.

- **USE MULTI FACTOR AUTHENTICATION**
  When an attacker is trying to enter your systems by guessing usernames or passwords there is not a lot you can do. Blocking their IP address is possible, but they change addresses often. When using multi factor authentication, compromising the account just by password guessing is not enough. They will also need an additional factor. When implementing multi factor authentication do not skip certain access paths or users. If you do so, these will become the target.

CLOSING WORDS

Based on incidents like this, it shows the need for having your security controls and procedures ready. When having to live with the mercy of an attacker, it will only cost you a lot of money. A good implementation of protective and detective controls will help you and your organization to reduce the cost of attacks. An unfortunate fact that we see happening every day. Hopefully your organization is prepared.