Ransomware and DigiNotar case analysis

Casini Lorenzo Tommasini Martino

01.10.2020

1 Ransomware analysis

Among the malware that could infect devices, in the last ten years an increase in attacks has been noted (2). These take the form of a specific kind, called *ransomware*. The etymology behind the word (1) suggests us that our files are held hostage and a ransom is requested to get them back. Still, to clearly understand these kind of attacks it is important to have a proper definition of them. We can take into consideration the definition given by *""I was told to buy a software or lose my computer. I ignored it": A study of ransomware"* (6):

> "Ransomware is a particularly pernicious form of malware that restricts an individual's access to their computer [...] and demands payment to restore functionality."

Although it feels generic, this definition includes all families of ransomware, without the need to get too specific. It is important to note though that the definition given here refers only to "computers", whereas we know that not only computers but also phones (2) (3), databases and servers (2) could be targeted regardless of the installed OS (1) (3) (6) or whether they are a business or private devices. The most attractive targets are businesses and organizations of all size, which highly rely on the availability of data and where team members need to make quick decisions. But also colleges, universities, government agencies, hospitals, energy and finance companies can be targeted due to the sensitive information they store or the critical services they provide.

As described into (2), ransomware comes in the form of *locker-ransomware* and *crypto-ransomware*. The former locks the device, denying the access to the owner. There is no encryption involved but instead, the device's user interface is locked due to malicious changes operated by the attacker (e.g. modifying the boot procedure, the partition tables or assigning the shell to himself (1)). This malware leaves the target with very few capabilities such as allowing the victim to only communicate with the attacker and to pay the ransom (5).

Crypto-ransomware instead actively looks in specific places to encrypt most common used file types (such as those with extension $.txt$, $.jpeg$, $.pdf$ or $.doc$) (1). They also come in the form of modifying registry entry or encrypting or even deleting restore points and backups, so to nullify eventual recovery plan based on these (3). Since directly encrypting a large number of files with the private key is computationally expensive, the attacker typically uses a hybrid approach. Once the target machine is infected, the malware generates a large random symmetric key which is used to encrypt the data. Then it uses the public key of the attacker to encrypt the symmetric key. This hybrid approach allows to have an efficient encryption scheme together with the guarantee that the user will not be able to decrypt the data without paying the ransom. The resulting asymmetric ciphertext is shown to the victim along with instructions on how to

pay the ransom. Usually, a deadline is fixed by the attacker and a missed payment within the established date could lead to a higher money request or to a permanent loss of data (7).

Ransomware is often spread through phishing emails that contain malicious attachments or through links in web-based instant messaging applications. The victim is tricked into opening links or attachments from apparently trusted or known sources, which then give to the attacker free access to device. *Drive-by download* is another common way users can be infected. This ransomware is installed on the victim's machine when they visit a compromised website, without even the need to click anything on it. Moreover, a ransomware can be embedded in a pirated software or in an official software previously corrupted. More advanced variants of ransomware have self-propagating mechanisms that permit them to move laterally to other devices on the network. An entire organization, thus, can be infected by a single compromised machine. *Malvertising* (malicious advertising) is also becoming an increasingly popular method of ransomware delivery (4).

The main reason for the wide success of ransomware as a malware attack vector is its effectiveness and ability to generate money for cyber-criminals. The requested amount is transferred to the attackers in a way that is difficult to trace. Bitcoins are frequently used since they offer an easy and anonymous method to collect the ransoms.

1.0.1 How ransomware can affect me as an individual

As described, ransomware can affect me, as an individual, by taking hostage my files, or my whole device, by preventing me to access useful or important information. Files such as photos and videos may have a huge personal and emotional value, which could be painful if lost.

On a professional level, a ransomware could prevent me to access important work-related resources or preventing me to do my work completely. Moreover, if the network to which I am connected is not secure, the ransomware may be able to infect other devices on the same network, thus creating more problems for which I could be held responsible.

From a broader point of view, a ransomware could attack a hospital in which I am hospitalized, thus preventing the doctors to know my data and take proper decisions.

1.0.2 Preventive, detective and corrective measures

Risk is the interpretation of the probability and impact of a ransomware attack. Different approaches and solutions should be taken when considering how to reduce the risk of infection.

Preventive measures are taken before a ransomware attack takes place both to limit attack surface, reduce the risk of getting infected and to help mitigate it in such eventuality (see *Correctives measures*):

- Be prepared for an incident by following the latest news on how a ransomware may occur;
- Keep operating system, software and applications current and up to date, to avoid known vulnerability to be exploited;
- Data should be regularly backed up. Those backups should be stored in a different location from the device they refer to. It is also ideal to have the backup location online during backup time only and offline otherwise, to avoid the malware to spread and thus infect the backup copies as well;
- Install antivirus and anti-ransomware software on your computer, if you don't already have them, and update them regularly;
- Don't open links or attachments in suspicious emails or from unknown sources;
- Don't visit alleged malicious websites or click on miraculous advertisements or pop ups;

- Enforce strong password security;
- Install a firewall to stop traffic from untrustworthy sources to access into your network.

Detective measures are taken in order to detect an intrusion or an attack. Some of them are purely technical, while others are related to good practices:

- Regularly scan your infrastructure. The scan can be done either by anomalies or by pattern-detection;
- Analyze the alarms given by the antivirus and treat them as soon as possible;
- Some tools can be installed in the compromised device in order to identify the specific ransomware you are infected by. Once the ransomware is recognized, the tool can give a good indication whether the data can be decrypted or not.

Corrective measures are taken in order to recover from a ransomware attack:

- Isolate the infected system from all the others, both physically and virtually (network). There must not be any contact points between the infected device and other devices in the system;
- Don't pay the ransom because this is what feeds the attacker's business and you don't have any guarantee that the data will be correctly decrypted;
- Restore the backups only once the device is free from the ransomware, to avoid the possible encryption of the backup system. A clear installation of the operating system can get rid of the ransomware (most of the times).
- Analyze what went wrong and learn from your mistakes. This must not happen again.

1.0.3 Measures taken as individuals

The following practices were put together based on what both of us do to avoid incurring in a ransomware or mitigating the hassle in such an eventuality.

If a ransomware were to happen on our phones it wouldn't be much of a problem, even if the ransomware was able to delete the Android default backups. Almost all the apps in use are either cloud based or provide an automatic backup on a cloud service. Nevertheless, we take for granted that, as long as all apps are up to date and our accounts are protected, we are doing the best we can. In case the possibility to install apps from unknown sources (e.g. $.apk$) was enabled for development or any other reason, it is done at our own risk and it is a good practice to disable it as soon as possible. Ideally, a separate device for "development purposes" would be much more secure.

Moreover we have subscribed to some hacking newsletters, podcasts and feeds to constantly stay informed about the latest vulnerabilities and techniques used by the attackers. We are careful about not visiting malicious websites or opening links whose source we are not sure about. The antivirus installed on our computers is kept up to date and performs full scans of the device regularly. Since the data on our computers is not critical and the availability of it is not an issue, the offline backups are planned monthly and they target the most used directories. In addition, a double backup of the most important files is stored in the cloud. A pool of different password is used in order to have diverse login credentials across multiple services.

How would you rate the residual risk that ransomware poses to you?
Since the impact of an attack would not be high and considering the controls implemented in the above paragraph, the residual risk is rated as low. Although additional measures could be taken in order to prevent or mitigate a ransomware attack, an excessive number of controls would not be justified by the current usage of the aforementioned devices.

2 DigiNotar case analysis

2.1 10 lessons learnt

Technical

1. Due to an incorrect or a poorly configured structure of the architecture to make its component segregated, the attacker was able to navigate the network once inside. Always ensure and verify the segments' segregation.

2. The investigation points out the fact that there are limited logging facilities, as well as the fact that logs are kept for a small period of time or deleted every time the system was turned off. This informs us to the fact that it was not a practice to archive or backup such log files in case of future need and that the retention period was relatively short. Considering the role of DigiNotar as Certificate Authority and the fact that the investigation went back in time for only a few months, this is a big oversight.

3. Malicious software, which could normally be detected by an anti-virus, was found on the most critical servers. No anti-virus software was present at the time of the attack.

4. At least two web servers were running outdated versions of the software. Keeping software updated is a well known and highly suggested best practice. Exploitation of known vulnerabilities was the way with which the attacker gained first entry in DigiNotar's network.

5. The log files were generally stored on the same servers monitored, making the logging system useless in case the given machine was compromised. Log files should be stored separately to preserve their integrity.

Security management

6. By leaving the smart-cards inserted in the netHSM network, the Certificate Authorities were continuously operational since the corresponding private keys were always activated. In this way, the high security provided by the needed physical access was made useless. It is important not to step over the security measures and to ensure that they are actually respected.

7. DigiNotar was unable to provide any proof that the private keys were not always active. This means that no measures had been implemented to record the smart-card usage implying a generic lack of access control to track physical access to and usage of high security assets.

8. A user name and password in clear text was found in a $web.config$ file on the external $Main - web$ server. These credentials were misused by the attacker to gain access to the internal network. It was also proved that the Administrator password could be easily brute-forced, meaning that the password in use was relatively weak. This leads to question the whole password policy in use at DigiNotar. A strong password security should be enforced. In addition a different authentication approach should have been considered where the $web.config$ file was needed.

9. As a Certificate Authority, DigiNotar was a trusted party. By not making this information open to the public from the very beginning, DigiNotar didn't meet the expected responsibility level. Moreover, organizations such as the Dutch Government, which rely on such third parties, should carefully choose who to trust only after a detailed analysis.

10. According to some retrieved emails, some employees knew about the outdated software on the web servers, the dual network interface of the BAPI workstation and the temporary fail of some routine checks that could have immediately detected the issue of rogue certificates. Still no one was directly appointed to solve these issues. To make sure that the security procedures are enforced, it is fundamental to assign the responsibilities of the systems.

2.2 Relation to ISO 27002 chapters

Technical

1. Architecture structure not segregated:
   Chapter 13 - Communications security, 13.1 - Network security management

2. Poor logging facilities and retention:
   Chapter 12 - Operations security, 12.3 - Backup & 12.4 - Logging and monitoring

3. Missing antivirus
   Chapter 12: Operations security, 12.2 - Protection from malware

4. Software update
   Chapter 12 - Operations security, 12.6 - Technical vulnerability management

5. Segregation of device from log output
   Chapter 12 - Operations security, 12.4 - Logging and monitoring

Security management

6. Smart-card inserted in netHSM network
   Chapter 9 - Access control, 9.1 - Business requirements of access control

7. Missing traced procedures for smart-card usage
   Chapter 12 - Operations security, 12.4 - Logging and monitoring

8. Password in clear text and easy password
   Chapter 9 - Access control, 9.3 - User responsibilities

9. Late public notification
   Chapter 16 - Information security incident management

10. No appointed personnel to solve the issues
    Chapter 6 - Organization of information security, 6.1 - Internal organization

2.3 Attackers gained access to the Secure network

The attackers exploited some vulnerabilities in the external web servers and used them as stepping stones to gain access to the internal *Office* network and bypass the firewall. The BAPI workstation production was located in the Secure network, thus protected by a firewall. However, the workstation contained two network cards and was therefore connected to both the Office network and the Secure network. Because of the dual network interface, the traffic was not blocked by the firewall and the attackers could gain a foothold in the Secure network, where the CA servers were located.

References

[1] A. Ali. Ransomware: A research and a personal case study of dealing with this nasty malware. 7:87–99, 2017. doi: 10.28945/3707.

[2] A.K. Maurya, Neeraj Kumar, Alka Agrawal, and Prof. Raees Khan. Ransomware evolution, target and safety measures. *International Journal of Computer Sciences and Engineering*, 6:80–85, 01 2018. doi: 10.26438/ijcse/v6i1.8085.

[3] P. Lindskog D. Monika, Zavarsky. Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, 94:465–472, 08 2016. doi: 10.1016/j.procs.2016.08.072.

[4] Panzerit. How ransomware spreads, 12 2019. URL `https://panzerit.com/how-ransomware-spread/`. Accessed on September 21st, 2020.

[5] Panda Security. Ransomware: Screen lockers vs. encryptors, 01 2018. URL `https://www.pandasecurity.com/mediacenter/malware/ransomware-screen-lockers-vs-encryptors/`. Accessed on September 29nd, 2020.

[6] Camelia Simoiu, J. Bonneau, C. Gates, and S. Goel. "i was told to buy a software or lose my computer. i ignored it": A study of ransomware. In *SOUPS @ USENIX Security Symposium*, 2019. URL `https://web.stanford.edu/~csimoiu/doc/ransomware.pdf`.

[7] A. Young and Moti Yung. Cryptovirology: extortion-based security threats and countermeasures. In *Proceedings 1996 IEEE Symposium on Security and Privacy*, pages 129–140, 1996. doi: 10.1109/SECPRI.1996.502676.