Ransomware Case Study

Nancy R. Mead,
Bastian Tenbergen

November 2021

Ransomware

Background

The ubiquitous availability of the internet from practically every computer, device, and many pieces of equipment – from ATM machines to farming equipment – gives rise to a new challenge in cyberattacks [1]. Ransomware attacks alone account for more than $100 million in monthly damages to the economy [2] and are a potential threat for companies, governments, and private citizens alike [3].

Case Study Overview

In this case study, we will explore the anatomy of ransomware attacks and look into recent examples to identify mitigation strategies. We also investigate the legal aspects of these kinds of attacks. The learner is advised to review CyBOK chapters 2, 3, and 6-8 prior to attempting this case study. Furthermore, a wealth of online resources such as [4], [5] (explicit language warning), [6], [7] are suitable introductions to the topic and may serve as hints to adequate solutions.

Student Instructions

Task 1:

Describe the anatomy of a ransomware attack. State the typical stakeholders and adversaries, and state the adversaries' goals and motivations. As you do so, be sure to describe the mechanism of how a ransomware attack infiltrates an organization, in other words, the "business model" behind an attack like this, and the risk to the attacked organization.

Task 2:

In popular scientific literature as well as news articles, you will find a plethora of examples of ransomware attacks. Find a new example that wasn't discussed as part of this course and summarize the attack from the source(s) you found. Cite the sources properly. Finally, for each of your descriptions of stakeholders, goals, motivations, attack vector, business model, and organizational risk (see your solution to Task 1), identify them in the example you found.

Task 3:

In this task, you take the role of a security administrator in an insurance underwriting agency. Your office branch takes in insurance applications from potential customers, solicited and sent to you by local insurance brokers. Your office is in charge of ensuring that incoming applications are filed properly, checking them against eligibility criteria, evaluating the risk to the insurance company, and if all criteria are satisfied, approving the coverage. You specifically are in charge of data and network security.

You have been asked by your superiors to develop a risk management and governance plan to keep your office branch safe from ransomware attacks and keep all your office data secure. Your plan should specify policies, actions, and procedures for the following levels of the organization:

- Individuals (e.g., policy clerks, supervisors, managers)
- Departments (e.g., underwriting dept., application dept., network administration)

- Organizational management (e.g., branch management, insurance company at large)

Feel free to be creative, but explicit, on how your fictitious office operates.

Task 4:

Explain in your own words why it is regulatorily problematic to:

a) Prosecute ransomware attacks
b) Make ransomware payments.

Instructor notes

This case study may be assigned as a formative homework assignment, whole or in part, for individual students or small student teams. It is also possible to use this case study as an in-class exercise. Assessment is at the discretion of the instructor.

Example solution

Note that this exercise requires some creativity on part of the student. Solutions may therefore take dramatically different forms. The following can be seen as an example of a minimally acceptable solution.

Task 1:

There are essentially three main actors: the attacker, the victim, and the target organization. The attacker intends to extort money from the target organization. This is done by sending malware to a victim and somehow motivating them to run it on their computer. The malware is designed to encrypt all files and possibly the operating system of the computer, and possibly other computers on the network, thereby effectively rendering the machines useless and locking the victim and other members of the target organization out of their own files. In the case of private citizens, the target organization is the same as the victim.

The attacker promises to remotely decrypt the locked files in exchange for money, typically in the form of anonymous payment methods such as prepaid credit cards or cryptocurrency. The target organization is immobilized and unable to execute their daily business since they are locked out of their IT infrastructure and files.

Task 2:

The example of the Colonial Pipeline Hack from May 2021 comes to mind [8]. In this case, rather than send malware by email (which is the typical vector of malware in company networks), a password to a VPN network account that is no longer used but was meant for a former employee to work from home was leaked and compromised by attackers from a hacking group called "DarkSide". The attackers gained access to the internal infrastructure of Colonial Pipeline Co. and rendered the billing system inoperable. In their ransom note, they claimed to be able to make it functional again in exchange for cryptocurrency payment. Since the company was no longer able to bill their business partners, they began shutting down the entire pipeline, hence protecting them from financial loss, while shifting the loss and burden to the general public [9]. The company eventually paid $4.4 million.

Task 3:

The following measures could provide some protection against ransomware attacks, specifically a VPN intrusion using inactive accounts, like the example from Task 2:

- Individuals (e.g., policy clerks, supervisors, managers)
  - Only allow certain individuals remote access
  - Require multi-factor authentication for all network access
  - Limit access, e.g., through role-based access control
  - Only allow email-attachments of certain file-types or none at all
  - Disallow thumb drive usage on employee workstations
- Departments (e.g., underwriting dept., application dept., network administration)
  - Terminate accounts of former employees immediately
  - Set access boundaries between departments
  - Maintain department-wide backups
- Organizational management (e.g., branch management, insurance company at large)
  - Maintain organizational backup systems
  - Clearly mark email-attachments from external sources as such
  - Hire an external company for network monitoring and security management
  - Perform readiness drills and penetration tests

Task 4:

Explain in your own words why it is regulatorily problematic to:

a) Prosecute ransomware attacks:
   Some countries provide safe-havens for attackers.
b) Make ransomware payments.
   It does not deter future attacks. The same company may be attacked again using the same mechanism by the same attacker. It also makes prosecution impossible once payment is made, since the attackers will "lay low."

References

1. Dosset, Julian, "A timeline of the biggest ransomware attacks." Online resource available at „„https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/, accessed 21 November 2021.

2. Brooks, Chuck, "MORE Alarming Cybersecurity Stats for 2021!" Online resource available at https://www.forbes.com/sites/chuckbrooks/2021/10/24/more-alarming-cybersecurity-stats-for-2021-/, accessed 21 November 2021.

3. Fruhlinger, Josh, "Ransomware explained: How it works and how to remove it." Blog article available at https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html, accessed 21 November 2021.

4. European Union Agency for Cybersecurity, "Threat Landscape for Supply Chain Attacks." Online resource available at https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, accessed 21 November 2021.

5. Last Week Tonight, "Ransomware." Online resource available at https://www.youtube.com/watch?v=WqD-ATqw3js [explicit], accessed 21 November 2021.

6. Birsan, Alex, “Dependency Confusion: how I Hacked Into Apple, Microsoft, and Dozens of Other Companies.” Blog article available at https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610, accessed 21 November 2021.

7. Bridgwater, Adrian, “Forget the users, the threat starts in the software supply chain.” Blog article available at https://www.idginsiderpro.com/article/3611543/forget-the-users-the-threat-starts-in-the-software-supply-chain.html, accessed 21 November 2021.

8. Turton, William; Mehrotra Kartikay, Hackers Breaches Colonial Pipeline Using Compromised Password.” News article available at https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password, accessed 21 November 2021.

9. Campbell, Ian Carlos, “Colonial Pipeline CEO confirms company paid $4.4 million ransom it wasn’t supposed to pay.” News article available at https://www.theverge.com/2021/5/19/22443933/colonial-pipeline-ransom-4-million-hack-gas-shortage, accessed 21 November 2021.