CS 462 Report
Ragnar Locker Ransomware

In December 2019, a couple of months before the start of a global pandemic, ransomware was released, targeting high-value targets. Multiple corporations and companies were hit, most of which contribute a significant portion of the world economy. This ransomware is known as Ragnar Locker, a complex system of attack designed to cause as much damage and confusion as possible. In this report, we will analyze the damages caused by this ransomware, how, where, and why it was used, as well as the effect this attack had on our world amidst an international lockdown due to the COVID-19 pandemic.

In an era marked by rapid digitalization and technological advancement, an industry as old as the age of sailing stands at the center of innovation and vulnerability. While the integration of digital technologies has revolutionized the efficiency and connectivity of the maritime field, it has also exposed it to unforeseen cybersecurity threats. Many improvements arose in the maritime field from the advancement of technology, allowing ships to carry heavier freight over greater distances, sometimes toward fairly remote locations. All of this improvement allowed for greater flexibility in the international market, stretching beyond what we thought could be possible. However, all of this fancy technology is still at risk, the risk of a cyber-attack crippling the system, thus the ship, just as piracy was during the age of sail. In our case, the Ragnar Locker ransomware was responsible for crippling the international shipping company CMA CGM, interrupting their entire activity for the month, causing a significant blow to their revenue and, as a result, the global economy.

Ragnar Locker is the name of a ransomware, a type of malware designed to take control of certain assets, intending to extort money from the victim, designed specifically to target high-profile organizations. The goal of this ransomware was to target remote desktop protocols, more specifically, the CVE-2017-0213 vulnerability in Windows. This vulnerability allows the attacker to elevate their privilege within the system, meaning that if they successfully infiltrate the system, they can give themselves permission to roam it freely. To initially gain access to the system, the attacker had to use a brute-force attack in order to get credentials, gaining access to confidential information.

The ransomware was specifically targeting Windows systems, as the attackers knew they could exploit the CWE-2017-0213 vulnerability. After successfully infiltrating the system, they ran VMs using Windows XP to avoid detection. Using the virtual machines carefully crafted for this kind of attack, meaning it was operating silently, they were able to scan the system for further vulnerabilities. From there, they gained access to sensible information, encrypted it, and then locked the system, requiring a key to decrypt it. The encryption used masked its path, allowing the host machine to recognize it as trusted. Furthermore, all antivirus and countermeasures were disabled, allowing the attacker to remain silent and steal the sensitive data. At this point, companies lost control of their system, and only one solution could resolve the problem: pay the ransom. While the information and system were locked, the attacker remained in control of the data, extracting it for further gain. It is unclear what their intent was, but we could speculate that they were willing to sell the data to malicious corporations or rivals of the company victim of the attack. If the ransom was not paid in time, the victims would not be able to gain access to their system, and their data would be sold to the highest bidder.

To remain undetected, the ransomware was carefully crafted and protected with obfuscation techniques. The code of the malware was filled with encryption, as well as junk code, rendering it hard to understand to the untrained eye. This technique allowed the ransomware to stay dormant in the systems until the attacker deemed it was time to activate it. It also allowed for data to be extracted and encrypted without anyone noticing.

As seen before, the attacker ran a small virtual machine within the system of the infected company using a Windows XP shell. The older version of Windows allowed for the virtual machine to not be detected. From there, they installed the ransomware, encrypted and stole the file, and set the malware to be dormant for a certain period. It is important to notice that none of the systems flagged the Windows XP virtual machine as hostile, proving a certain flaw in the security systems of the victims.

To encrypt the files, the software used hardcoded strings, which ran through all of the services on the infected system, locking them. The encryption was targeting text, database, and email, meaning that all text files, emails, and documents were encrypted. This makes sense when we know how valuable emails or a text file containing a client list can be to a company. Using the RSA-2048 public key, a system of encryption allowing for great security of the encrypted message, the attacker generated special keys to be used as decryption methods. When activated, Ragnar Locker commences the encryption process in 64 simultaneous threads and uses their special encryption algorithm, Salsa20, to fully encrypt the data. A message would be prompted in a special file on infected machines, ordering the victim to come in contact with the attacker to pay the ransom, which would, in theory, release the key, thus decrypting the data.

The attackers adopted a double-extortion method, meaning that not only did it disable systems, but it also extracted a large amount of sensitive data that could be sold for an increased profit. The malware had a long dormant period during which it analyzed how it could infect the system for maximum damage. Ransoms going up to $11 million were requested for the control of the system to be returned. It is rather unclear what exactly the attackers want to do with the stolen data. It is safe to assume that by keeping it, they want to sell it, even when they already obtain a significant amount from the victims themselves. Another reason they did this was simply for the chaos it would cause. Human nature is very much unpredictable in this sort of situation.

In our case, the shipping company CMA CGM was already trying to recover from the unprotected hit it took from the international lockdown following the COVID-19 pandemic. The situation was already as chaotic as it could get, and adding a major cybersecurity breach to the muddle was surely not planned by the management. The ransom itself was already a large sum that the company ultimately paid, but the lack of movement for the ships, spread across months, also significantly reduced the income of this one. Not only was the company impacted, but so was the world economy. The system being down meant the ships would not be able to deliver and pick up goods around the world. This shortage crippled multiple sectors, even if they were not a direct victim of the ransomware. Such a breach is proof that all of our systems rely on good security and that one attack could cripple the entire world economy. Adding to the already burning fire that was the global lockdown, this attack was a good demonstration of what could happen in the worst scenario.

A case like the Ragnar Locker is proof that, first, no field is spared by cybercrime, and such crime can lead to a decrease in growth for the economy. Any damage done by ransomware can be devastating for a company, thus making safety measures even more important. A good understanding of how, when, and where an attack might happen is a good way to mitigate potential damages. Here, the company's victim of the attack could have prevented the initial breach by ensuring that no vulnerability is left unguarded. Furthermore, some extensive employee training should be required to ensure that no openings are found. In our case here, the CWE-2017-0213 was not patched on the company computers, meaning that anyone knowing about it would have been able to elevate their privileges. This is the kind of inattention that causes such an attack to happen. Some penetration could have been executed prior to the attack, where the pen tester would have potentially found the vulnerability and then reported it to the capable technician. Moreover, a brute force approach would not have worked if the password policy had been revised. Password in the company’s victim of the attack should not only be strong but should also expire after a certain time, and a double authentication system should be implemented. This would ensure that no outside agent or password cracker gains access to the system. The possibility of an inside threat is also probable, which, in this case, audits would be required to investigate where and when accessibility was compromised.

Amidst all precautions taken by a company, it is always a good thing to remember that the human factor has a huge part in every attack or major breach. Cybersecurity is everyone’s affair when the stakes are this high. Quality training and a good awareness of the situation are good ways to mitigate damages by any potential attacks.

Source:

https://nvd.nist.gov/vuln/detail/CVE-2017-0213

https://www.sentinelone.com/anthology/ragnar-locker/

https://www.acronis.com/en-us/blog/posts/ragnar-locker/

https://doi.org/10.1109/MITP.2023.3297085