Ransomware Attack Analysis

Leah Drew

The Attack

On October 20th, 2022, the private health insurer Medibank revealed that they had been the victim of a ransomware attack which leaked the data of 9.7 million customers. Medibank claimed initially that there was no evidence of customer data having been stolen, believing itself to have stopped the attack before the attackers had been able to access this sensitive information. However, Medibank was later contacted by the attackers, who revealed that they had in fact stolen data (Toulas, 2022). A Russian ransomware gang, REvil, are likely the group behind the attack. The attackers initially demanded a ransom of $10 million US dollars, which was lowered to $9.7 million after the insurance company refused to pay. The company stood by its decision not to pay the ransom over fears that paying the ransom would not result in the data being recovered or kept private (Whiteman, 2022).

Later, the stolen information was leaked by the attackers on the dark web, including "names, addresses, dates of birth, phone numbers, email addresses, Medicare numbers for ahm customers (not expiry dates), in some cases passport numbers for our international students (not expiry dates), and some health claims data" (Gatlan, 2022). However, the most sensitive information, such as financial information and identifying documents had not yet been leaked (Gatlan, 2022). The attackers claimed to have only leaked some of the data they had stolen and threatened to post the entire database on the dark web if Medibank did not pay the ransom (Kost, 2022). As of November 9th, 2022, several weeks after the initial attack, attackers were still negotiating with the insurance company over WhatsApp to attempt to get them to pay the ransom (Gatlan, 2022). On December 1st, 2022, the hackers posted one final leak of stolen information on the dark web, proudly stating in their post, "“Happy Cyber Security Day!!! Added folder full. Case closed” (Page, 2022).

In order to execute the attack, the attackers needed a way to gain access to the system. In this case, this was done by stealing the credentials of an employee with privileged access in the network. This information was sold on the dark web and purchased by an unknown party, presumably someone from REvil. While it is unknown how the credentials of this employee were stolen, it is likely that they were stolen through phishing—a type of social engineering that attempts to trick a user into providing sensitive information through a seemingly legitimate email or website (Kost, 2022).

By stealing the credentials of a privileged user, the attackers with REvil were able to skip some steps of a cyberattack; mainly, the privilege escalation step, because they already had everything that they needed to steal and encrypt the information they wanted. They could immediately execute the attack to steal the information and then encrypt and lock down the system. The attack was over much quicker than it would have been if the credentials that had been stolen were that of an ordinary user (Kost, 2022).

What is Ransomware?

Ransomware is defined by the Federal Bureau of Investigation as “a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return” (FBI, 2020). Ransomware infects a machine with a malicious file that is usually downloaded from a website, email attachment, or advertisement. After the file is downloaded, the attacker attempts to obtain root or admin privileges, which allows them to steal information. In a ransomware attack, the attacker will usually encrypt all of the files and lock the user out of their computer, forcing them to either pay a ransom to be able to decrypt their files and regain access, or refuse to pay the ransom and losing these files forever. Most users have no idea that they have downloaded a malicious file until they are already locked out of their computer, in which case, it is sometimes too late to do anything about it (FBI, 2020).

Ransomware can encrypt every type of file, from simple text files to image files to program files and critical system files. They can also affect any type of computer—personal computers, servers, enterprise networks, and government networks can all be victims of a ransomware attack (Microsoft, n.d.). Less commonly, ransomware can infect other devices such as phones and tablets. Aside from encrypting and denying the user access to their data, ransomware can be dangerous because it gives the attacker full access to sensitive information, including things like banking information that may be on your device (Chebac, 2022).

What Are the Effects of the Attack, and What Can be Done?

Fortunately, ransomware attacks are preventable with good computer habits. Keeping operating systems and applications up to date, running antimalware scans regularly, making backups of important information, and creating a continuity plan in case of an attack can all help an organization to respond and recover from a ransomware attack (FBI, 2020). Backups are critical for recovering from a ransomware attack as they can be used to fully restore the system, effectively undoing the effects of the attack. However, leaked data cannot be taken back from the attackers, so it is important to take steps to avoid downloading malicious files in the first place (CISA, n.d.).

Because ransomware attacks are preventable, organizations can face consequences for not taking adequate steps to prevent these attacks. Indeed, the Australian government, the country in which Medibank is based, has recently passed legislation allowing businesses to be fined up to $50 million for security breaches (Page, 2022). Medibank may face legal consequences for the breach, as the law firm Maurice Blackburn has announced that they have filed a complaint against the insurance company and have “the power to not only fine Medibank for privacy breaches but also to potentially order the company to compensate customers” (Janda & Ziffer, 2022).

Because this attack affected almost 10 million individuals, it has the potential to have serious effects on society. Privacy breaches are always dangerous, as it puts sensitive information in the hands of people who intend to use it for immoral or criminal purposes. Additionally, people have a right to privacy, which has been violated by a single act of poor judgement by an employee with privileged access to the system at Medibank (Janda & Ziffer, 2022). This serves as a reminder to maintain cautious and responsible actions when using the internet.

References

Chebac, A. (2022, November 17). Mobile ransomware on your smartphone: The next step for Cybercriminals. Heimdal Security Blog. Retrieved December 4, 2022, from https://heimdalsecurity.com/blog/mobile-ransomware-the-next-step-for-cybercriminals/

CISA. (n.d.). Ransomware guide. CISA. Retrieved December 4, 2022, from https://www.cisa.gov/stopransomware/ransomware-guide

FBI. (2020, April 3). Ransomware. FBI. Retrieved December 4, 2022, from https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

Gatlan, S. (2022, November 9). Medibank warns customers their data was leaked by ransomware gang. BleepingComputer. Retrieved December 4, 2022, from https://www.bleepingcomputer.com/news/security/medibank-warns-customers-their-data-was-leaked-by-ransomware-gang/

Janda, M., & Ziffer, D. (2022, December 1). 'case closed': Have the hackers just dumped the remaining stolen Medibank data? ABC News. Retrieved December 4, 2022, from https://www.abc.net.au/news/2022-12-01/medibank-data-leak-has-everything-been-released-now/101720028

Kost, E. (2022, November 17). What caused the Medibank Data Breach?: Upguard. UpGuard. Retrieved December 4, 2022, from https://www.upguard.com/blog/what-caused-the-medibank-data-breach

Microsoft. (n.d.). Protect your devices and data from malware. Microsoft Support. Retrieved December 4, 2022, from https://support.microsoft.com/en-us/windows/protect-your-pc-from-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3

Page, C. (2022, December 1). Medibank hackers declare 'Case closed' as trove of stolen data is released. TechCrunch. Retrieved December 4, 2022, from https://techcrunch.com/2022/12/01/medibank-case-closed-stolen-data-released/

Toulas, B. (2022, October 26). Medibank now says hackers accessed all its customers' personal data. BleepingComputer. Retrieved December 4, 2022, from https://www.bleepingcomputer.com/news/security/medibank-now-says-hackers-accessed-all-its-customers-personal-data/

Whiteman, H. (2022, November 11). Australia blames cyber criminals in Russia for Medibank Data Breach | CNN business. CNN. Retrieved December 4, 2022, from https://www.cnn.com/2022/11/11/tech/medibank-australia-ransomware-attack-intl-hnk/index.html