Lucas Esquivel

CS 462

CS 462 Term Paper

As the tech field continues to grow so does the number of cyber-attacks. One type of attack that has become more popular lately are ransomware attacks. In late September of this year, a cyberattack occurred to Optus as 2.1 million pf their user’s IDs were exposed. Out of all those numbers, at least 150,000 passports and 50,000 Medicare numbers were stolen. They also identified that out of the 2.1 million affected users, 900,000 of them were stolen ID numbers from expired documents. Optus says the stolen data includes names, email addresses, postal addresses, phone numbers, dates of birth, and for a portion of the affected customers, identification numbers including passport numbers, driver’s license numbers and Medicare numbers. After the attack, a ransom threat was made. An Internet user published data samples on an online forum demanding a ransom of one million dollars in cryptocurrency from Optus. The threat was that if the ransom wasn’t paid within a week, all their data would be sold off in batches.

So, who was responsible for attacking Optus? Optus themselves have stated that it was the target of a “sophisticated attack”. The only person to come forward since, claiming to have the data is a user that goes by the name “OptusData” on a data breach forum. This is the same person who threatened to sell the data if Optus didn’t pay up a ransom of one million in cryptocurrency. The user then later posted what was allegedly 10,000 user records before deleting the posts and apologizing. Nothing else is known about this person other than what is posted on that forum, so it is still a mystery as to if this OptusData user was really the person responsible for the attack or not. This leads to another problem. Who has the data? We know that someone out there has all these data records and just the fact alone is a scary situation for people. People’s privacy and safety are in stake at the hands of someone out there that know one knows about. In their apology post the user “OptusData” stated that they had deleted the only copy they had of the data. There is no way to verify this, and I personally wouldn’t trust whoever is behind this user.

Ransomware attacks are attacks designed to deny a user or organization access to their files by encrypting the files and demanding for a ransom payment for the encryption key. This places an organization in a position where it’s cheaper to pay the ransom to gain the files. Ransomware has quickly become the most prominent and visible type of malware. Recent ransomware attacks have impacted different services from places like hospitals and banks. The attackers also threaten to sell the organization’s data to a third party if the ransom isn’t paid within a certain timeframe. In Optus’s case that user “OptusData” gave them a week to pay one million dollars in cryptocurrency to get the encryption key. This one was executed a little differently than traditional ransomware attacks. Usually in ransomware attacks the attacker wants to keep as low of a profile as possible to avoid any suspicions. In this case, the attacker went public by leaking 10,000 user records on a public forum, usually the attacker would rather not leak data as it could also leave a possibility of a vulnerability the company can use to get their data back without paying the ransom. This is one of the reasons the user OptusData apologized after, the hacker claimed there were “too many eyes” so he took back his essential plan of selling the data to someone else. I believe that the preparation phase of a cyber operation is very important, if your systems are not properly installed and prepared with things like anti-virus software and firewalls than put yourself at higher risk of getting attacked. It’s better to be safe than sorry.

This is Australia’s biggest and most serious data breach. A lot of angry people sent messages to Optus asking for an explanation. Quickly following the breach there was a rise of phishing attacks and fraud attempts. Many of the users whose IDs were stolen got a text or a call from a sketchy number trying to scam them. These people were told by Optus to watch out for identity theft and scammers. Optus is now facing a class action lawsuit as a result of the breach, with two legal companies investigating them. Optus also offered a 12-month subscription to credit monitoring and identity protection service Equifax Protect to reduce the risk of identity theft for those who had their data accessed in the breach. Someone claiming to be the hacker told Australian news press that they had “accessed an unauthenticated API endpoint” meaning that they did not have to log in to access the data and that it was “all open to internet for anyone to use”. The federal government is looking at urgent reform, including making it easier to alert banks to which of their customers may have been compromised. It is also considering large fines for companies that allow such a breach to occur.

This is an important topic to talk about especially today because technology is a field that continues to grow and expand, and the number of attacks continues to grow as well. Optus is Australia’s second largest telecommunications company with around 10 million users. A data breach attack to a company with this many users leaves a lot of risk when something like this occurs. There are companies like Facebook, Netflix, and Twitter that have hundreds of millions of users, and it will be a big safety threat if those companies get breached. Therefore, cybersecurity is such an important topic of discussion in today’s society and why it’s the best investment these companies can make to protect their data from outside enemies. As we move forward into the future newer devices and technologies like crypto and the metaverse will present new vulnerabilities and areas hackers can expose, it is important for the public’s safety and security that big companies make sure they make cybersecurity a priority to keep people’s information safe and secured.

Sources:

Jnguyen. “Ransomware Attack - What Is It and How Does It Work?” *Check Point Software*, Check Point Software, 29 June 2022, https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/.

“Optus Australia Satellite and Telecommunications Company in Australia.” *Skybrokers*, 5 Dec. 2021, https://sky-brokers.com/supplier/optus-australia/.

“Optus Data Breach: Everything We Know so Far about What Happened.” *The Guardian*, Guardian News and Media, 28 Sept. 2022, https://www.theguardian.com/business/2022/sep/29/optus-data-breach-everything-we-know-so-far-about-what-happened#:~:text=know%20so%20far.-,Who%20is%20the%20attacker%3F,of%20a%20%E2%80%9Csophisticated%20attack%E2%80%9D.&text=The%20only%20person%20to%20come,US%241m%20in%20cryptocurrency.

Powell, Olivia. “IOTW: Everything We Know about the Optus Data Breach.” *Cyber Security Hub*, 5 Oct. 2022, https://www.cshub.com/attacks/news/iotw-everything-we-know-about-the-optus-data-breach.

Turnbull, Tiffanie. “Optus: How a Massive Data Breach Has Exposed Australia.” *BBC News*, BBC, 29 Sept. 2022, https://www.bbc.com/news/world-australia-63056838.