ACER RANSOMEWARE ATTACK Case Study

ACER INDIA

RANSOMEWARE

- On **13 October**, a user on a popular hacker forum posted the below screenshot, claiming credit for the 60GB attack, referencing the March breach and offering both video evidence of the haul, as well as releasing the records of 10,000 Acer clients.

- **The REvil ransomware group claimed the attack and demanded a $50 million ransom**, one of the highest reported at the time. Acer offered to pay the group $10 million, which was rejected by the hackers.

- **The REvil hackers** shared that they had broken into Acer's system, and they had files and pictures as proof. The leaked images contained the company's financial documentation as well as bank balances and bank communications.

- According to BleepingComputer, REvil, announced their ransomware strike on Acer on their data leak site last Friday. It was revealed that Acer was breached through some released images of files that they stole as proof of their involvement that included financial spreadsheets, bank balances, and bank communications.

- With a workforce of 7,000, annual revenue of $7.8 billion in 2019, and $3 billion in earnings in Q4 2020, Acer ranks among the most popular brands to fall victim to ransomware attacks.

- The group said it plans to attack supply chains and cause "disorder and chaos" that affects as many people as possible.

Timeline

Acer ransomware attack

1. Taiwanese computer manufacturer Acer is facing a ransomware attack from the REvil group.
2. Bleeping Computer reports that REvil offered Acer a 20% discount on the payment it was looking to extort out of the company if the money was transferred by Wednesday, March 17
3. According to Bleeping Computer(Opens in a new window), REvil is demanding a $50 million sum from Acer. The company reportedly has until March 28 2021 to send the funds before any alleged stolen data is leaked.
4. Acer offered to pay the group $10 million, which was rejected by the hackers.

Vulnerabilities

Overall Summary

Acer's Attack is the Largest Known Ransom Demand

This attack on Acer is the largest known ransom demand—even offering Acer a 25% discount if they made their payment by this past Wednesday. Being that REvil announced the attack on Friday, it can be presumed that payment to the group has not been made.

Vulnerability

Though there are few details on what fully transpired, there is some information on how it could have happened.

The group may have pulled off the attack by way of the "Hafnium" vulnerability in Microsoft Exchange. Data from Advanced Intel's Andariel cyberintelligence platform was able to link the possible breach to the Microsoft Exchange hack issue. Though Microsoft had been working to release a simple patch for the issue, that doesn't mean it's been erased entirely. The software giant explained that the patch would only work against attacks that had already happened and might not be a panacea to resolve future hacks.

Costs

- 50 million ransom, one of the highest reported at the time.
- "Acer is a global network of vulnerable systems. We no longer have access to their India servers. This is all we can reveal now," the hackers said in a follow-up message.

Prevention

- Putting money into the training and education of staff members.
- Maintain a consistent patching schedule for all workstations and servers.
- Establish a strong infrastructure for working remotely using managed devices.

REFRENCES

1. 1.https://www.zdnet.com/article/acer-confirms-second-cyberattack-in-2021/

2. 2.https://www.cpomagazine.com/cyber-security/acer-reportedly-suffered-a-revil-ransomware-attack-attracting-the-highest-ransom-demand-in-history-of-50-million/
3. https://www.zdnet.com/article/acer-confirms-second-cyberattack-in-2021/
4. https://cyolo.io/blog/ransomware/5-ransomware-attacks-from-2021/#:~:text=Acer%20%E2%80%93%20%2450%20Million%20and%20Financial%20Data%20Leaking&text=Then%2C%20they%20demanded%20that%20the,(see%20CNA%20attack%20below).
5. https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php