NVIDIA BREACH

Logan Ferguson

April 25, 2022

FACTS:

- February 25, 2022
- Lapsus$ ransomware gang
- Nvidia's internal systems compromised
- Minor ransomware attack
- Lapsus$ claimed they would leak customer data if Nvidia did not pay the ransom

WHAT WAS STOLEN

- Lapsus$ claimed to have stolen 1TB of data
- Password hashes
- Source code for new AI system still in development
- Designs for new graphics cards
- On February 28, the hacker group supposedly leaked the first batch of data, again asking Nvidia to pay the ransom

SOLUTION

- Nvidia refused to pay, so they decided to go on the offensive
- Lapsus$ reported that Nvidia had successfully “hacked back”
- Nvidia was able to remote into the group’s Virtual Machines and encrypt the data that had been stolen
- Information had been uncovered that has led to the arrest of a few Lapsus$ members

INFORMATION SECURITY VULNERABILITIES

- There is still little information about this attack since it only happened a few months ago
- We do know that Nvidia has “hardened” its information systems against further ransomware attacks
- Nvidia could have mistaken their own data loss prevention policies for a ransomware attack

IMPROVING CYBERSECURITY

- Ways to improve information security and prevent such attacks:

- Enable 2FA for all employee accounts
- Keep antivirus software running and up to date
- Frequent penetration testing on networks
- Ensure that employees are well educated on good cybersecurity practices

REFERENCES

Bannister, A. (2022, February 28). *Cyber-attack on Nvidia linked to lapsus$ Ransomware Gang*. The Daily Swig | Cybersecurity news and views. Retrieved April 20, 2022, from https://portswigger.net/daily-swig/cyber-attack-on-nvidia-linked-to-lapsus-ransomware-gang

Newman, L. H. (2022, March 15). *The lapsus$ hacking group is off to a chaotic start*. Wired. Retrieved April 20, 2022, from https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/