Justin Healey
07/25/2022

NVDIA Ransomware Incident & Impacts

In February 2022 the world's largest semiconductor chip company experienced a cyberattack via an increasingly common method – ransomware. NVDIA confirmed that the ransomware group, Lapsus$, started leaking employee credentials and personal information online.[1] The attack lasted two days. According to NVDIA, the company's commercial activities were not affected and remained fully operational as the attack unfolded and in the aftermath.[2] Even though NVDIA's customers were not directly affected, over 71,000 employees' sensitive information was compromised and Lapsus$ claims to have stolen over 1 TB of information. The group threatened to publish the data in five phases if NVDIA did not pay an unknown amount in ransom. Ironically, Lapsus$ was also hit with ransomware in the following days. The group outwardly blamed NVDIA for the attack on Twitter, but NVDIA never publicly claimed responsibility. It is not unlikely, however, that a talented, revenge seeking NVDIA employee targeted the group purely out of spite and hatred; alternatively, if NVDIA did target Lapsus$, this could suggest that the data is very valuable. Lapsus$ said on Twitter:

> "TODAY WE WOKE UP AND WE FOUND NVDIA SCUM HAD ATTACKED OUR MACHINE WITH RANSOMWARE…… LUCKILY WE HAD A BACKUP BUT WHY THE FUCK THEY THINK THEY CAN CONNECT TO OUR PRIVATE MACHINE AND INSTALL RANSOMWARE!!!!!!!!!!"

The security community laughed at this comment, but it does show that even black hat hacking groups can be compromised, even with the same methods they use on their victims. Lapsus$ also had some interesting demands in return for the data decryption key and to not leak the data online. The group demanded that NVDIA release the source code for their GPUs and remove the LHR (lite hash rate) limitation, which would be a huge benefit to the cryptocurrency mining and gaming communities.[3]

NVDIA stated on multiple occasions that the attack did not interrupt any of their public operations; however, there are likely still some considerable economic impacts. Number one, the semiconductor chip shortage has not improved much since it begun in the second quarter of 2020. NVDIA, the largest semiconductor chip manufacturer in the world, plays a crucial role in pulling the industry out of this hole. This incident could impact the public's trust in the company and potentially extend the shortage due to a decrease in revenue and thus manufacturing. Second, the incident proved that Lapsus$ possesses the ability to compromise one of the largest companies in the world, which poses the question as to whether small and medium sized businesses have the resources to adequately defend themselves against similar attacks. According to Ahmed Sharaf, CTO and founder of Xband Enterprises out of Massachusetts explains, "Simply stated, they are outmanned and outgunned to address such challenges and cyberattacks."[4] Many cybersecurity experts follow suit in their predictions. It has become clear that black hat hacking groups are becoming increasingly skilled in their craft, posing a real threat to both private and government entities alike.

Justin Healey
07/25/2022

The NVDIA ransomware incident opened a lot of eyes to the growing threat of ransomware and the importance of integrating cybersecurity practices, including backups. In this case, if NVDIA had backups of the data, they likely would not need to even consider complying with Lapsus$'s demands. They could have mandated a password reset for all employees, which they did, and then wipe and restore their systems to prevent advanced persistent threat scenarios. There are many lessons to be learned, and even 5 months later it is unclear just how powerful these black-hat hacking groups have become. This incident also poses the important question, is any company is "unhackable?"

Sources:

1. *Cyber Management Alliance*, "5 Major Ransomware Attacks of 2022." June 15, 2022. https://www.cm-alliance.com/cybersecurity-blog/5-major-ransomware-attacks-of-2022.

2. Gatlan, Sergiu; *BleepingComputer*, "GPU giant NVDIA is investigating a potential cyberattack." Feb. 25, 2022. https://www.bleepingcomputer.com/news/security/gpu-giant-nvidia-is-investigating-a-potential-cyberattack/.

3. Newman, Hay Lily; *Wired.com*, "The Lapsus$ Hacking Group Is Off to a Chaotic Start." Mar.15, 2022. https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/.

4. Ghosh, Soumik; *Bank Info Security*, "How Lapsus$ Data Leak May Affect NVDIA and Its Customers." Mar. 1, 2022. https://www.bankinfosecurity.com/how-lapsus-data-leak-may-affect-nvidia-its-customers-a-18636.