Everything We Learned From the LAPSUS$ Attacks

By The Hacker News

Published: 2022-05-12 · Archived: 2026-04-05 16:45:09 UTC

In recent months, a cybercriminal gang known as LAPSUS$ has claimed responsibility for a number of high-profile attacks against technology companies, including:

- T-Mobile (April 23, 2022)
- Globant
- Okta
- Ubisoft
- Samsung
- Nvidia
- Microsoft
- Vodafone

In addition to these attacks, LAPSUS$ was also able to successfully launch a ransomware attack against the Brazilian Ministry of Health.

While high-profile cyber-attacks are certainly nothing new, there are several things that make LAPSUS$ unique.

- The alleged mastermind of these attacks and several other alleged accomplices were all teenagers.
- Unlike more traditional ransomware gangs, LAPSUS$ has a very strong social media presence.
- The gang is best known for data exfiltration. It has stolen source code and other proprietary information and has often leaked this information on the Internet.

LAPSUS$ stolen credentials

In the case of Nvidia, for example, the attackers gained access to hundreds of gigabytes of proprietary data, including information about chips that the company is developing. Perhaps more disturbing; however, LAPSUS$ claims to have stolen the credentials of thousands of Nvidia employees. The exact number of credentials stolen is somewhat unclear, with various tech news sites reporting differing numbers. However, Specops was able to obtain approximately 30,000 passwords that were compromised in the breach.

The rise of cyber extortion

There are two major takeaways from the LAPSUS$ attacks that organizations must pay attention to. First, the LAPSUS$ attacks clearly illustrate that gangs of cybercriminals are no longer content to perform run-of-the-mill ransomware attacks. Rather than just encrypting data as has so often been done in the past, LAPSUS$ seems far more focused on cyber extortion. LAPSUS$ gains access to an organization's most valuable intellectual property and threatens to leak that information unless a ransom is paid.

A technology company could conceivably suffer irreparable harm by having its source code, product roadmap, or research and development data leaked, especially if that data were to be made available to competitors.

Even though the LAPSUS$ attacks have thus far focused primarily on technology companies, any organization could conceivably become a victim of such an attack. As such, all companies must carefully consider what they can be doing to keep their most sensitive data out of the hands of cybercriminals.

Weak passwords at play

The other important takeaway from the LAPSUS$ attacks was that while there is no definitive information about how the attackers gained access to their victim's networks, the list of leaked Nvidia credentials that was acquired by Specops clearly reveals that many employees were using extremely weak passwords. Some of these passwords were common words (welcome, password, September, etc.), which are extremely susceptible to dictionary attacks. Many other passwords included the company name as a part of the password (nvidia3d, mynvidia3d, etc.). At least one employee even went so far as to use the word Nvidia as their password!

While it is entirely possible that the attackers used an initial penetration method that was not based on the use of harvested credentials, it is far more likely that these weak credentials played a pivotal role in the attack.

This, of course, raises the question of what other companies can do to prevent their employees from using similarly weak passwords, making the organization vulnerable to attack. Setting up a password policy that requires lengthy and complex passwords is a good start, but there is more that companies should be doing.

Protecting your own organization from a similar attack

One key measure that organizations can use to prevent the use of weak passwords is to create a custom dictionary of words or phrases that are not permitted to be used as a part of the password. Remember that in the Nvidia attack, employees often used the word Nvidia either as their password or as a component of their password. A custom dictionary could have been used to prevent any password from containing the word Nvidia.

Another, even more important way that an organization can prevent the use of weak passwords is to create a policy preventing users from using any password that is known to have been leaked. When a password is leaked, that password is hashed and the hash is usually added to a database of password hashes. If an attacker acquires a password hash they can simply compare the hash to the hash database, quickly revealing the password without having to perform a time-consuming brute force or dictionary-based crack.

Specops Password Policy gives admins the tools that they need in order to ensure that users avoid using weak passwords or passwords that are known to have been compromised. Specops makes it easy to create a password policy that complies with common password standards, such as those defined by NIST. In addition to setting length and complexity requirements, however, Specops allows admins to create dictionaries of words that are not to be used as a part of a password. Additionally, Specops maintains a database of billions of leaked passwords. User's passwords can be automatically checked against this database, thereby preventing users from using a password that is known to have been compromised.

Found this article interesting? This article is a contributed piece from one of our valued partners. Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2022/05/everything-we-learned-from-lapsus.html