Microsoft's 6 Biggest Hacks

Microsoft has certainly been a household name since its inception, but its history is far from flat. Over the years, Microsoft has suffered from a long list of security incidents, many of which have put user data at risk.

So what is the biggest Microsoft hack of the 21st century? And does the tech giant need better security?

1. Exchange server breach in 2021

In early 2021, on January 3, Microsoft's Exchange platform servers began to be compromised through four zero-day software vulnerabilities.

It was not until March of the same year that the scale of the attack became apparent, with more than 30,000 US-based organizations being attacked due to these software flaws in Microsoft Exchange's code. In total, more than 250,000 individual Exchange servers were attacked, of which 7,000 are based in the UK. Other countries, including Norway and Chile, were also affected.

The data stolen in this attack included the email addresses and passwords of the server users. Additionally, attackers can add more backdoors to exploit in the future.

It didn't take long for Microsoft to release the necessary patches, but this attack highlights how easily vulnerabilities can lead to massive attack campaigns.

2. The leak of 250 million people's customer records

In early 2020, it was discovered that Microsoft had accidentally leaked more than 250 million customer records. This major leak happened because the database was not password protected.

Much of the exposed data included conversations between users and customer support representatives, which took place between 2005 and 2019. However, more sensitive information was revealed in some cases. certain, including the email address and IP of the client.

It took Microsoft only 24 hours to secure the database, but by now it was too late.

3. Hotmail 2016 Credential Leak

In May 2016, multiple press outlets started reporting on a major hack that resulted in the leak of user login credentials from Google, Yahoo, and Microsoft. More than 270 million account information has been stolen and sold on illegal markets in Russia. 33 million of them are credentials for Hotmail, an email service purchased by

Microsoft in 1997.

Fortunately, the hacker who originally owned the credentials sold them to a disguised security company, rather than another malicious individual looking to exploit them.

4. Lapsu$ data breach in 2022

In March 2022, Microsoft confirmed that they were attacked by a well-known hacker group called "Lapsu$". This international hacking organization has made a name for itself by targeting many big names, including Nvidia and Samsung.

While Lapsu$ used to target organizations in South America and the UK, they have since targeted other victims, including those in the US. This blatant hacking group shifts its focus to Microsoft in early 2022.

In this case, Lapsu$ (which Microsoft officially calls "DEV-0537") managed to compromise a Microsoft employee account and access parts of the Bing, Bing Maps, and Cortana source code.

Microsoft's confirmation comes after Lapsu$ published the stolen source code in a torrent file. However, Microsoft alleged in a blog post related to the incident that the theft and leak of the source code did not pose a security risk to the company or its users.

5. 2010 Zero-Day Violation

In late 2009, Microsoft discovered a critical zero-day security vulnerability. The company did not take any action until the following year, when companies like Google and Adobe began to become targets of cybercriminals through this vulnerability.

This vulnerability allows an attacker to deploy malware on the target company employee's device. Malware will then be used to access private information from Google and Gmail.

This breach caused Microsoft to be considered particularly bad because of the way the company handled the issue of remedies. It was not until January 2010, 3 months after learning about this vulnerability, that Microsoft released a patch. What's worse is that Microsoft originally planned to release the patch a month later, in February.

6. Storm0558 Attack of 2023

In 2023, about 25 organizations, including government agencies, were attacked through two Microsoft security vulnerabilities. The malicious actor, based in China and known as Storm0558, managed to steal data from customers using Outlook Web Access and Exchange Online.

Microsoft claims that the threat actor has espionage goals. The company further confirmed that the attacker obtained the signing key of the MSA consumer to carry out the attack.

According to Wiz's investigation, not only Outlook Web Access and Exchange Online were affected by the hack. Wiz reported that other Microsoft services, including Teams, OneDrive, and SharePoint, can also be

exploited with a compromised MSA key.

Does Microsoft need better security?

Microsoft is not lax in terms of security at all. The company ensures that its products have a solid level of user protection, including two-factor authentication, encryption, anti-spam filters, firewalls, and login alerts.

Of course, the presence of these features will depend on the Microsoft product you are using. For example, Windows operating system comes with default antivirus software but Outlook does not.

The majority of the attacks listed above are caused by software vulnerabilities, so it looks like more code testing might be what Microsoft needs to do. The company has gone through audits, be it on their software or business, but it seems a large amount of vulnerabilities are still being missed.

It can also be wise to release security patches as soon as a vulnerability is identified, even if the vulnerability has not yet been exploited. This eliminates the possibility of Microsoft or Microsoft users falling victim to attacks caused by software exploits.

However, these activities will require a lot of personnel and resources as Microsoft currently has close to 400 software products.