Data Breach Case Study

Microsoft

By,

P Sairam Sekhar

Data breach

On March 2nd, 2021, Microsoft reported it was the victim of a state-sponsored cyberattack from the Chinese hacking group called Hafnium. Microsoft explained in their notification that the group “primarily targets entities in the United States for the purpose of exfiltrating information from a number of industry sectors.”

On 5 January 2021, security testing company DEVCORE made the earliest known report of the vulnerability to Microsoft, which Microsoft verified on 8 January. The first breach of a Microsoft Exchange Server instance was observed by cybersecurity company Volexity on 6 January 2021. By the end of January, Volexity had observed a breach allowing attackers to spy on two of their customers, and alerted Microsoft to the vulnerability. After Microsoft was alerted of the breach, Volexity noted the hackers became less stealthy in anticipation of a patch. The attacks came shortly after the 2020 United States federal government data breach, which also saw the compromising of Microsoft's Outlook web app and supply chain. Microsoft said there was no connection between the two incidents.

New nation-state cyberattacks - Microsoft On the Issues

Attack Category : Mailing Servers

Provider: Microsoft

On March 2nd, 2021, Microsoft reported it was the victim of a state-sponsored cyberattack from the Chinese hacking group called Hafnium. Microsoft explained in their notification that the group "primarily targets entities in the United States for the purpose of exfiltrating information from a number of industry sectors."

The attack affected over 30,000 organizations across the United States, including local governments, government agencies, and businesses. It is the eighth instance of a nation-state cyberattack against civil organizations and businesses Microsoft has reported in the last 12 months.

The Microsoft breach was carried out through a sophisticated zero-day hacking campaign that targeted hundreds of thousands of on-premise servers running Microsoft's Exchange software. Hafnium gained access to on-premise servers through a combination of stolen passwords and previously undetected vulnerabilities. Then, Hafnium created a web shell around those servers that provided them with the access they needed to steal email data remotely. Hafnium operates from China, and this is the first time we're discussing its activity. It is a highly skilled and sophisticated actor.

The attacks included three steps. First, it would gain access to an Exchange Server either with stolen passwords or by using the previously undiscovered vulnerabilities to disguise itself as someone who should have access. Second, it would create what's called a web shell to control the compromised server remotely. Third, it would use that remote access – run from the U.S.-based private servers – to steal data from an organization's network.

The latest details about the affected data are available here.

Timeline

Microsoft Exchange Attack

1 Hackers have exploited the vulnerabilities to spy on a wide range of targets, affecting an estimated **250,000** servers. The attack affected over **30,000** organizations across the United States, including local governments, government agencies, and businesses.

2 On 2 March 2021, the Microsoft Security Response Center (MSRC) publicly posted an out-of-band Common Vulnerabilities and Exposures (CVE) release, urging its clients to patch their Exchange servers to address a number of critical vulnerabilities.

3 On 15 March, Microsoft released a one-click PowerShell tool, The Exchange On-Premises Mitigation Tool, which installs the specific updates protecting against the threat, runs a malware scan which also detects installed web shells, and removes threats that were detected; this is recommended as a temporary mitigation measure, as it does not install other available updates.

4 Microsoft released updated tools and investigation guidance to help IT Pros and incident response teams identify, remediate, defend against associated attacks

5 Automatic on-premises Exchange Server mitigation now in Microsoft Defender Antivirus.

6 Approximately **952.8M** active email records were exposed.

Vulnerabilities

Overall Summary

- As of 9 March 2021, it was estimated that 250,000 servers fell victim to the attacks, including servers belonging to around 30,000 organizations in the United States, 7,000 servers in the United Kingdom.
- Web shells were installed on more than 5,000 unique servers in over 115 countries.
- **Acer** reportedly suffered data exfiltration and was hit with a demand to pay a ransom of $50 million

China Chopper - Backend Cookie - CVE-2021-26855

This vulnerability is a server-side request forgery that would allow an attacker to send requests to the server and bypass the need for authentication. An attacker would only need to know details about the Exchange server itself and the email address it hosts.

DearCry- Unified Messaging-CVE-2021-26857

This vulnerability allows for insecure deserialization within Exchange's Unified Messaging service. Serialization is when code objects are persisted to disk for use or transmission elsewhere. In this instance, HAFNIUM had shells and scripts – exploitation tools – prepared. Once in an exchange server with forged authentication, they would run deserialization commands while in exchange servers to import and run their tools. Ransomware known as DearCry was subsequently installed on vulnerable on-premises Microsoft Exchange servers.

Revil- ECP Application Pool-CVE-2021-26858

This vulnerability is for arbitrary file writing after successful authentication into an exchange server. These allowed HAFNIUM to write files to a path on the server, either duplicating valuable information or using a backdoor to extract. The REvil ransomware was also deployed on other vulnerable systems, as was the Black KingDom ransomware.

Crypto-mining - OAB Application Pool-CVE-2021-27065

This vulnerability is also for arbitrary file writing after successful authentication into an exchange server. Crypto-mining malware, such as Lemon Duck and the Monero-mining component of Prometei, was deployed in some systems.

Costs

- The average cost of a data breach is $200,000
- Between tens of thousands to more than 250,000 victims worldwide, particularly small businesses and governments, as of 6 March 2021.
- As of 9 March 2021, it was estimated that 250,000 servers fell victim to the attacks, including servers belonging to around 30,000 organizations in the United States, 7,000 servers in the United Kingdom.
- Web shells were installed on more than 5,000 unique servers in over 115 countries.
- Acer reportedly suffered data exfiltration and was hit with a demand to pay a ransom of $50 million.

Prevention

- The Exchange Server team released a script for checking HAFNIUM indicators of compromise (IOCs) – **04:March:2021**
- To aid customers in investigating these attacks, Microsoft Security Response Centre (MSRC) has provided additional resources, including new mitigation guidance: Microsoft Exchange Server Vulnerabilities Mitigations – **05:March:2021**
- Microsoft released a new one-click mitigation tool, the Microsoft Exchange On-Premises Mitigation Tool, to help customers who do not have dedicated security or IT teams to apply security updates for Microsoft Exchange Server – **15:March:2021**
- Microsoft released updated tools and investigation guidance to help IT Pros and incident response teams identify, remediate, defend against associated attacks. Microsoft Defender was also updated to detect and remove the DearCry ransomware. – **16:March:2021**
- The US Federal Bureau of Investigation, the Australian Cyber Security Centre and the UK National Cyber Security Centre each coordinated national responses against the exploits.