Attack Case Study

Microsoft

Swipping Attack

On 5 January 2021, security testing company DEVCORE reported a vulnerability to Microsoft, which Microsoft verified on 8 January. On 6 January 2021, cybersecurity company Volexity observed a breach allowing attackers to spy on two of their customers, and alerted Microsoft to the vulnerability. On 2 March 2021, ESET reported multiple attackers besides Hafnium exploiting the vulnerabilities. On 10 March 2021, security researcher Nguyen Jang posted proof-of-concept code to GitHub on how the exploit works, totaling 169 lines of code. On 13 March, another group independently published exploit code, with minimal modification to work. The attacks came shortly after the 2020 US 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.

The global wave of cyberattacks and data breaches began in January 2021 after four zero-day exploits were discovered in on-premises Microsoft Exchange Servers, giving attackers full access to user emails and passwords, administrator privileges, and access to connected devices. 250,000 servers fell victim to the attacks, including those belonging to 30,000 organizations in the US, 7,000 servers in the UK, and the European Banking Authority, Norwegian Parliament, and Chile's Commission for the Financial Market. On 2 March 2021, Microsoft released updates for Microsoft Exchange Server 2010, 2013, 2016 and 2019 to patch the exploit, but this does not retroactively undo damage or remove any backdoors installed by attackers. Small and medium businesses, local institutions, and local governments are the primary victims of the attack, as they often have smaller budgets to secure against cyber threats and outsource IT services to local providers that do not have the expertise to deal with cyber attacks. Microsoft announced on 12 March 2021 that a new family of ransomware was being deployed to servers initially infected, encrypting all files and making the server inoperable and demanding payment to reverse the damage. By 22 March 2021, 92% of Exchange servers had been either patched or mitigated.

Timeline

Microsoft Attack

1. **The hackers were able to exploit four different zero-day vulnerabilities that allowed them to gain unauthorized access to emails from small businesses to local governments.**
2. For three months, hackers took advantage of a few coding errors to allow them to take control of vulnerable systems.
3. They only needed two conditions to break into each individual company's email servers: Connection to the internet & On-premises, locally managed systems
4. Once they were in, they could request access to data, deploy malware, use backdoors to gain access to other systems, and ultimately take over the servers.
5. Since the requests looked like they came from the Exchange servers themselves, many people assumed it was legitimate and approved.
6. Though Microsoft was able to patch the vulnerabilities, if the owners of the individual servers didn't update their systems, attackers would be able to exploit the system flaw again.

Vulnerabilities

On 11 March 2021, Check Point Research revealed that the number of exploitation attempts on organizations it tracks tripled every two to three hours. The United States was the most attacked country. The attack was discovered after attackers were discovered downloading all emails belonging to specific users on separate corporate Exchange servers. On march 12, 2021 DearCry was deployed to servers, encrypting device contents, and demanding payment to recover files. it was estimated that 250,000 servers fell victim to the attacks.

Zero-day Vulnerability

Hackers exploited four zero-day vulnerabilities to compromise Microsoft Exchange servers' Outlook Web Access, giving them access to victims' entire servers and networks.
With that, a second vulnerability can then be exploited, escalating that user access to administrator privileges.

Using Web shell

Attackers then install a web shell to provide a backdoor to the compromised server which gives hackers continued access to the server as long as both the web shell remains active and the Exchange server remains on. Attackers used a script to return to addresses to drop a web shell.

Ransomware

Attackers downloaded emails from servers, added users, added backdoors, accessed other systems, and installed ransomware. As patching the Exchange server against the exploit does not retroactively remove installed backdoors, attackers continue to have access to the server until the web shell, other backdoors and user accounts added by attackers are removed.

Costs

- REvil has demanded a $50 million U.S. dollar ransom, claiming if this is paid they would "provide a decryptor, a vulnerability report, and the deletion of stolen files", and stating that the ransom would double to $100 million U.S. dollars if not paid on 28 March 2021.

Prevention

- 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.
- Microsoft patched the vulnerabilities and the Microsoft Defender antivirus was updated to automatically mitigate them. However, these patches and mitigations do not remove existing infections, such as web shells and backdoors that have already been installed.
- Microsoft Defender was also updated to detect and remove the DearCry ransomware.