Intro

In 2021, Microsoft suffered a cybersecurity attack by multiple groups of hackers on their Microsoft Exchange server. There were more than 10 hacking groups that exploited the vulnerability that led to the attack (ESET, 2021), with some of them having ties to the Chinese government. The Microsoft Exchange server " includes calendaring software, email, and a place to manage your contacts. Many small, medium, and large organizations use Exchange and some email providers have Exchange accounts for home and personal accounts (Microsoft, 2021)." With Microsoft being such a large company, there were thousands of victims in the 2021 Microsoft Exchange Server data breach, mainly small businesses and governments. There were at least 30, 000 organizations that were victims of this attack (Krebs, 2021) in the United States alone. There were more victims of this attack across the globe.The scale of this attack makes it an interesting one to learn about, such as how the breach works, the technologies used to perpetrate the attack, the devices that can be attacked, what applications can be attacked, and how it affects today's society.

How did the breach work?

The data breach worked by exploiting four zero-day vulnerabilities within Microsoft's code that would lead to Remote Code Execution, which allows an attacker to "run malicious code on organization's computers or network (Cloudflare,)". Remote Code Execution can lead to many different kinds of attacks such as data breaches, privilege escalation, and ransomware (Imperva,). The four vulnerabilities are used in conjunction with each other to execute the attack. They are CVE-2021-26855, 26857, 26858, and 27065 (zdnet). All of the vulnerabilities affect port 443. The first vulnerability, 26855 has a remote attack vector that uses the network stack, and will allow attackers to view and change data heavily compromising confidentiality and

integrity. It is also known as a Server-side request forgery (Kost, 2023). A Server-side request forgery " causes the server-side application to make requests to an unintended location" (Port Swigger). After attacking the application with a Server-side request forgery, other technologies are open for the attacker to do what they want. This could be things like escalation of privileges, stealing data, manipulating files, and many other things. When using a Server side request forgery to attack a server, the application layer in the internet protocol stack is used in the form of HTTP requests. The attacker modifies information in the URL portion of the HTTP request to get information they normally would not be able to (Port Swigger) . By first exploiting this vulnerability, the attackers are able to then exploit the next vulnerabilities. The other three vulnerabilities all share the same attack vector and impact on the CIA triad, denying confidentiality, integrity, and availability to those affected by the attack. Those three require local access through either remote access like SSH or through local access of the keyboard or console(Microsoft, 2021). The second vulnerability, CVE-2021-26857 will then escalate the attackers privileges, allowing them "execution privileges as system (Kost, 2023)". CVE-2021-26857 "is a deserialization vulnerability in Exchange Server's Unified Messaging (voicemail) service (AttackerKB)." Serialization is when an object is changed in a way that makes it able to be transported to another place. Deserialization is reverting that change once it gets to its destination. An insecure deserialization vulnerability is when attacker controlled data gets deserialized by the server(Synk Learn). By using a deserialization vulnerability, an attacker can do things like cause errors and exceptions that will allow them an opportunity to use different attacks, such as remote code execution. The third and fourth vulnerabilities, CVE-2021-26858 and CVE-2021-27065, are both similar in that they are both arbitrary file write vulnerabilities (narang, 2021). Arbitrary file write vulnerabilities are another vulnerability that

lead to even more privilege escalation. What they do is give control over file and path permissions, and they can be exploited in different ways with different targets to attack. An arbitrary file write vulnerability can lead to an attacker gaining control of a file path and changing where things are uploaded to, but they may not be able to change the contents of a file in the path. An attacker may also gain control over the contents of a file, heavily compromising the integrity of data. An attacker can have control over the contents of a file, but that does not mean that they have control over both the contents and file path, but there are cases where an attacker has control over both(Schmitt & Stella, 2023). In summary, the attack was perpetrated through four different vulnerabilities. The first vulnerability,CVE-2021-26855, grants access to the server using a Server Side Request forgery. The second vulnerability, CVE-2021-26857, escalates the attacker's privileges by exploiting an insecure deserialization vulnerability. The last two vulnerabilities, CVE-2021-26858 and CVE-2021-27065, allow the attacker to create and change files wherever they want to in the server. This is the attack chain that led to thousands of victims that were using Microsoft Exchange Servers in 2021.

What were the technologies used to perpetrate the attack?

The technologies used to perpetrate the attack were the four zero-day vulnerabilities as described above to do things like remote code execution and creating backdoors. The technologies were from 2021 and have since been patched.

What applications are affected by the attack?

The applications affected by the attack were applications that were connected to the Microsoft Exchange Server. Typically those applications were things that used Microsoft's calendar, e-mail, and other communication applications that could access your contacts. For example, a device using Microsoft outlook would have been vulnerable to this attack.

How does the attack affect today's society?

This cyberattack was massive and one of the largest data breaches of 2021. It targeted one of the largest technology companies, Microsoft, and the people who use their Microsoft Exchange Server. There were other governments and organizations worldwide that suffered repercussions from this attack due to Microsoft being so large. With so many organizations and by extension, people being affected by this attack, it was bound to have effects in today's society. For one, it would be bad for the economy with businesses getting reputational and financial damage from losing valuable data and the trust of their customers, especially the smaller organizations. Data breaches are costly and in 2021, the global average cost of a data breach was 4.24 million dollars (IBM, 2021). Another factor that would change how this cyber attack would affect society is the circumstances during which this attack took place. A lot of countries at this time were still recovering from or actively handing the COVID-19 pandemic. Many organizations may have had most of their employees working remotely, which is bound to have changed the way that organizations conduct their business. They may have reconsidered how much of their budget they relegate to cyber security. They may have also changed the way they interact with their employees, implementing things like more cyber security training and employing more cyber security professionals. The attack could have served as a wake-up call or a warning for companies to start investing in their cyber security capabilities. Another way this affects our society is by instilling fear and distrust among the victims of the attack. This could lead to more caution when it comes to securing vital customer information. It could possibly lead to organizations not wanting to use Microsoft's services anymore due to fear of becoming a victim of another cybersecurity attack even though Microsoft already patched the vulnerabilities. This is one of the reputational costs of a cyber attack, and it can result in a loss of customers

should they lose trust in the company that was attacked. It could also be speculated that the attack would have had an influence over the federal cybersecurity policies that are being made in the years after the attack. This attack is highly speculated to be perpetrated, or at least sponsored by the Chinese government. “After months of investigation, the UK’s National Cyber Security Centre has now declared it “highly likely that Hafnium is associated with the Chinese state (Hern, 2021) .” In 2023, the Department of Defense released a summary of their cybersecurity policy in which they identify threat actors and determine how they are to be dealt with. In that cybersecurity policy, it is no shock that China and hacking groups related to the Chinese government were listed as some of the major threats to the United States’ cyberspace. Cyber attacks like the Microsoft Exchange Server data breach set precedents in cyberwarfare. It shows who is a threat and will alter the severity with which the United States will respond to cyberattacks. For example, the Department of Defense stated in their 2023 cybersecurity policy that they will start “Defending forward” and launch disruption campaigns against cyber threats with the goal of making it more costly to attack the United States critical infrastructure than it is to defend their own (Department of Defense, 2023).

Sources

"2023 DOD Cyber Strategy Summary." *Media*, U.S Department of Defense, 2023, media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF. Accessed 14 Apr. 2024.

"Cost of a Data Breach Report 2021." *IBM*, 2021, info.techdata.com/rs/946-OMQ-360/images/Cost_of_a_Data_Breach_Report_2021.PDF. Accessed 14 Apr. 2024.

"CVE-2021-26857." *AttackerKB*, 2021, attackerkb.com/topics/hx6O9H590s/cve-2021-26857. Accessed 14 Apr. 2024.

Hern, Alex. "What Is the Hafnium Microsoft Hack and Why Has the UK Linked It to China?" *The Guardian*, Guardian News and Media, 19 July 2021, www.theguardian.com/world/2021/jul/19/what-is-the-hafnium-microsoft-hack-and-why-has-the-uk-linked-it-to-china. Accessed 14 Apr. 2024.

"Insecure Deserialization: Tutorials & Examples." *Snyk Learn*, learn.snyk.io/lesson/insecure-deserialization/. Accessed 14 Apr. 2024.

Kost, Edward. "Critical Microsoft Exchange Flaw: What Is CVE-2021-26855?: Upguard." *RSS*, 1 Aug. 2023, www.upguard.com/blog/cve-2021-26855. Accessed 14 Apr. 2024.

Krebs, Brian. "At Least 30,000 U.S. Organizations Newly Hacked via Holes in Microsoft's Email Software." *Krebs on Security*, 5 Mar. 2021, kr bsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/. Accessed 14 Apr. 2024.

"Microsoft." *Microsoft Support*, Microsoft, 2021, support.microsoft.com/en-us/office/what-is-a-microsoft-exchange-server-account-48f92dec-72d5-440b-97a0-3e1bad044e91#:~:text=Exchange%20Server%20includes%20calendaring%20software,for%20home%20and%20personal%20accounts. Accessed 14 Apr. 2024.

Narangh\, Satnam. "CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065: Four Zero-Day Vulnerabilities in Microsoft Exchange Server Exploited in the Wild." *Tenable®*, 30 Oct. 2023, www.tenable.com/blog/cve-2021-26855-cve-2021-26857-cve-2021-26858-cve-2021-27065-four-microsoft-exchange-server-zero-day-vulnerabilities. Accessed 14 Apr. 2024.

"Number of Apt Groups Exploiting the Latest Exchange Vulnerabilities Grows, with Thousands of Email Servers under Siege, Eset Discovers." *ESET*, 10 Mar. 2021, www.eset.com/int/about/newsroom/press-releases/research/number-of-apt-groups-exploiting-the-latest-exchange-vulnerabilities-grows-with-thousands-of-email-s/. Accessed 14 Apr. 2024.

Osborne, Charlie. "Everything You Need to Know about the Microsoft Exchange Server Hack." *ZDNET*, 2021, www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/. Accessed 14 Apr. 2024.

"Remote Code Execution (RCE): Types, Examples & Mitigation: Imperva." *Remote Code Execution*, Imperva, 20 Dec. 2023, www.imperva.com/learn/application-security/remote-code-execution/. Accessed 14 Apr. 2024.

Schmitt, Maxence, and Lorenzo Stella. "A New Vector for 'Dirty' Arbitrary File Write to RCE." *A New Vector For "Dirty" Arbitrary File Write to RCE · Doyensec's Blog*, 28 Feb. 2023, blog.doyensec.com/2023/02/28/new-vector-for-dirty-arbitrary-file-write-2-rce.html#:~:text=Arbitrary%20file%20write%20(AFW)%20vulnerabilities,(RCE)%20on%20the%20server. Accessed 14 Apr. 2024.

"What Is Remote Code Execution?" *What Is Remote Code Execution?*, Cloudflare, www.cloudflare.com/learning/security/what-is-remote-code-execution. Accessed 14 Apr. 2024.

"What Is SSRF (Server-Side Request Forgery)? Tutorial & Examples: Web Security Academy." *What Is SSRF (Server-Side Request Forgery)? Tutorial & Examples | Web Security Academy*, portswigger.net/web-security/ssrf#:~:text=Server%2Dside%20request%20forgery%20is,services%20within%20the%20organization%27s%20infrastructure. Accessed 14 Apr. 2024.