A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities

Alexis M Pitney, Spencer Penrod, Molly Foraker and Suman Bhunia
Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio, USA 45056
Email: pitneyam@miamioh.edu, penrodsw@miamioh.edu, forakem@miamioh.edu, bhunias@miamioh.edu

***Abstract*—At the beginning of 2021 a massive amount of servers using Microsoft's Exchange program were breached by a foreign hacker group called HAFNIUM. This group discovered and exploited 4 different zero-day vulnerabilities which sent the entire cybersecurity community into a panic. Immediately after data breach was discovered, Microsoft and other governmental security agencies alerted all the users. Microsoft released multiple patches to safeguard the attack surface. This paper provides an in-depth analysis of the attack methodology, impacts and possible defense solutions. An estimated 400,000 Exchange Servers were affected by this attack, and a large portion of servers are still vulnerable today. Microsoft has released an effective security patch to stop the exploitation of the vulnerabilities.**

***Index Terms*—Backdoors, Microsoft Exchange, Data Breach, zero-day vulnerabilities, Serverside request forgery, HAFNIUM, File writing vulnerabilities**

I. Introduction

In January of 2021 there was a data breach in Microsoft Exchange Servers. A company called Volexity was auditing the security of Microsoft's servers when they noticed a presence within the network of the customer, downloading emails. After that caught the eye of the auditing team, they began to dig deeper into the server that the client was using and noticed some very unexpected requests. The requests that were being sent through were asking for very specific information from email accounts and files. Through this, the team began to uncover one of the largest breaches in Microsoft Systems. According to Adair, the head of the auditing company, this breach had been underway for almost three months, and he had never seen anything like this before [1]–[3].

The hackers exploited multiple errors within the code that created vulnerabilities [4]. The hackers had taken all of the vulnerabilities and in combination together used them to gain the initial access to Microsoft Exchange servers. After gaining this access Web Shells would be deployed allowing the hackers to steal data and use malicious practices against the server users. The hackers would also set up back doors into the system [5], in the case that the they could not access after patches, and updates were deployed by Microsoft, fixing the vulnerabilities.

Even with the day-one vulnerabilities other factors accounted for systems being breached. According to NPR [1], two conditions needed to be met in order for companies to be exploited: 1) They needed to be managed by the company's Internet security team locally, and 2) They needed to be connected to the internet as the hackers were not entirely local. Due to these two requirements Microsoft Cloud was not subject to the same type of attacks, it being on the cloud ensured that its' security is run by Microsoft directly. The Microsoft Threat Intelligence center took no time determining who the hackers were and how they infiltrated the company's software. At first the team thought that the hack was not very big as not much data was being taken and suddenly the hack started covering a wide range of companies rather than just a few. So much so that even the American government got involved as their information was also at risk.

The hackers that were concluded to be responsible by several agencies, is an organization that goes by HAFNIUM [6]. HAFNIUM is a group that operates allegedly from a foreign nation [1]. Their goal is to find information from industries, disclose, and compromise the information. It has been noticed previously by Microsoft, as early as June of 2020. The group is known as a nation-state hacker, and is backed by an adversarial government. The group has been known for doing similar attacks on victims that have internet-facing servers. They will usually gain access to these servers and then gain access to confidential information. The group is known to orchestrate these attacks from virtual private servers that they lease, which are typically hosted in the United States.

In this paper we describe multiple aspects of this attack, and what lead to the steady increase in compromised systems. In Section II the problems leading up to the attack, target victims, and the architecture of the system are discussed. Section III describes the vulnerabilities that were used to enter the system, and the process attackers would take in infiltrating, and exploit compromised systems. Section IV discusses the various ways of how this hack affected the community, and the ongoing problems faced by Exchange server owners. Section V offers up different solutions that Microsoft highly suggested to the responders of the systems that were hacked. Section VI describes reasoning for why the attacks were very effective.

II. Background

The Exchange breach is an example of how even larger software companies can have vulnerabilities in the systems they create. The vulnerability that was in Microsoft Exchange came from multiple day one vulnerabilities, and the reason for the large scale coverage that came was due to the speed with which these vulnerabilities were discovered. HAFNIUM

Fig. 1: Exchange Data Breach Timeline (2021)

is believed to be the perpetrator of these attacks [6], [7]. The group has done attacks similar to this before. They targeted multiple internet-facing servers, and open-source frameworks such as Covenant. Microsoft has also seen Hafnium interacting with multiple Office 365 Tenants, in many of these cases they were unsuccessful, but it did help Hafnium prepare for the attack on the Microsoft Exchange servers. Microsoft speculates that a large reason for the success of this attack is due to the amount of surveillance, and data Hafnium has gathered on their network. The group also had the resources needed for such an attack, as they are believed to be a nation-state hacker.

A. Nation State Hackers

The idea of nation state hackers can be a complicated topic, the definition is a hacker, or a group of hackers that works with an adversarial government [8]. Their purpose is to commit cyber-crimes against opposite government or other ally countries. Due to the funding and backing from governments combating nation state hackers can be a difficult task [9], [10]. Due to the backing from governmental bodies the groups could be companies, small task forces, or even divisions in the countries military. The groups usually get a large amount of funding for projects, as well as have the resources to access systems. With the large amount of resources it is easier for these groups to gain access to a system, and accomplish the task they are given. Helping push the agenda of who they are working for. Since these groups can work for different governments the purpose of their attacks can not always inferred, and the intentions of these groups can change depending on which government or group is funding the hackers [9]. Hafnium is known to be a hacking group

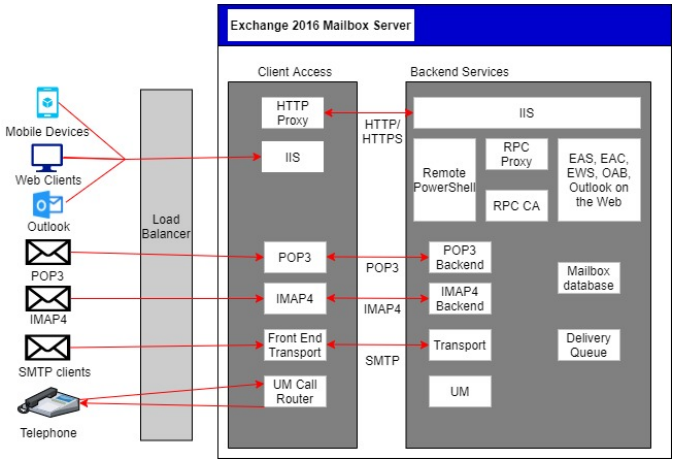

Fig. 2: Microsoft Exchange Server Architecture

backed by a foreign government, which has helped security specialists to infer what the purpose of these attacks could be. The government usually uses nation-state hackers to help retrieve information depending on what industries they would like to improve on [1]. It is believed that the reason for the attacks was to gather data that foreign governments could use to help expand AI development, which is one of the industries that foreign governments is currently working to expand in. It also would explain a large amount of the chosen victims, and information that was being taken.

B. Microsoft Exchange System

Fig. 2 depicts the architecture of a typical Microsoft Exchange Server that HAFNIUM infiltrated and Fig. 1 shows the timeline in which the events occurred. The Client Access section on Exchange servers are responsible for accepting all forms of client connections [11]. The front end services proxy connections to the back-end,due to this Clients do not directly connect to the back-end directly, but as will be described in III the zero day vulnerabilities found by HAFNIUM helped to bypass this design. This was possible because when a client would want to connect using HTTP, the server would use HTTP as a way to proxy a request to the server. This would be in a secured SSL using self-signed certificate, and the vulnerabilities that will be described in detail had the ability to circumvent this.

C. Victims of Attacks

The victims of many of these attacks were companies and people who were running their own local Exchange servers. Many of these companies were relatively small, and had either a small IT department or no IT department at all [4], [12], [13]. Since these companies were small, they had little need for extensive security. Due to this many of them had these servers connected to the internet, which allowed for Hafnium to gain access to these systems. In the beginning the amount of victims was small and as Tom Burt, vice president at Microsoft who manages the digital crimes unit states, *"At the time it was perceived as a relatively routine report of a couple*

TABLE I: Microsoft Exchange Exploit Definitions

Exploit	Definition
CVE-2021-26855	Server-side request forgery (SSRF) vulnerability in Exchange.
CVE-2021-26857	Insecure deserialization vulnerability in the Unified Messaging service. Insecure deserialization is where untrusted user-controllable data is deserialized by a program.
CVE-2021-26858	Post-authentication arbitrary file write vulnerability in Exchange.
CVE-2021-27065	Post-authentication arbitrary file write vulnerability in Exchange.

of vulnerabilities, it was in just a couple of dozen entities worldwide and just a handful in the U.S. We and the rest of the defender community see this activity happening all the time."

Microsoft was working on a patch to fix these vulnerabilities while it was still small scale, but then the hack went viral. Microsoft security reports have shown that before a patch could be deployed HAFNIUM had decided to ramp up the identification of vulnerable servers, which allowed for the number of compromised systems to spike. Microsoft believed that now other foreign actors from foreign governments were targeting these systems, and had to change their approach now that the situation had escalated [14].

III. Attack Methodology

When hacking into any system the first step is to gather information. When HAFNIUM scanned the servers for Microsoft Exchange, they were able to pin-point 4 zero-day vulnerabilities that they can exploit. Table I lists the four common vulnerabilities and exposures (CVE). A zero-day vulnerability is a weak part of the system that had not been known to the company that made the software [4]. These vulnerabilities allowed the hackers to access the servers that were only located on-site, in other words, the servers that were not connected to the cloud. After accessing these servers, they begun to steal emails, company data, passwords and usernames in order to escalate their privileges within the server to gain more data and this enabled them to maintain their access within the vulnerable server.

A. Server-side Request Forgery

The first of the four zero-day vulnerabilities is called CVE-2021-26855 [4]. This specific attack is a vulnerability that allows for server-side forgery (SSRF). Through this weakness, the hacker group was allowed to send arbitrary HTTPS requests to the server, and then say that the messages were real messages sent to the server. This weakness is especially concerning as anyone could access the server in this manner and it would not have to be a trusted source.

B. Deserialization vulnerability

The second vulnerability was called CVE-2021-26857 [15]. This particular vulnerability dealt with the Unified Messaging service within the Microsoft Exchange servers. This particular service allows users to make and access calls made across the server [16]. The messaging service allowed for data

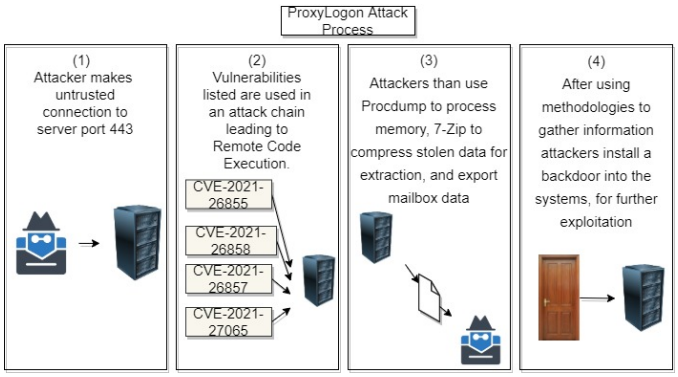

Fig. 3: Attack Process Used by HAFNIUM

to be deserialized in an insecure manner. Insecure deserialization makes a system vulnerable to Denial of Service attacks (DoS attacks), or bypass authentication [17].Standing by itself, this vulnerability does not appear to do much besides make the service unusable. Used with the other three vulnerabilities, this is a very good weapon for the hackers.In combination with the other weaknesses in the system, the hackers are able to pass data into the system that could harm the system as a whole.

C. First File Write Vulnerability

The third vulnerability was called CVE-2021-26858 [15]. This vulnerability dealt with an arbitrary file write. This means the hackers could have easily written random files within the server with information or even with programs to run [18]. The thing about this weakness is that the attacker would need to be able to authenticate who they were within the system. With the first vulnerability that was mentions, this is not a difficult task for the hackers.

D. Second File Write Vulnerability

The final vulnerability that was a main part of the Microsoft Exchange breach was called CVE-2021-27065 [15]. This vulnerability is very similar to the third one mentioned in that it also deals with arbitrary file writing within the server after the hackers were authenticated. The hackers could and did use both of these to write files to any path within the server. The hackers used this also to create a web shell within the servers they exploited. Web shells are commonly used to escalate and maintain access within the system that was hacked [19]. This shell cannot perform any other actions except maintain access within the system after the hack is performed so it is always the next step to monitoring the system for hackers [19].

E. The Process

As shown in the Fig 3 HAFNIUM would use the first and second vulnerabilities to enter and destabilize the system, HAFNIUM then used the last two vulnerabilities to create web shells within the servers. After the web shells were planted within the systems to act as back doors, the hackers used a program called Procdump to dump the Local Security Authority Subsystem Service Process. Procdump is a standard

program developed by Microsoft to assist in monitoring CPU spikes and creating a crash to help determine the cause of the spike [20]. The Local Security Authority Subsystem Service Process is an process that is used to run Windows operating systems and authenticate users [21]. Using these two programs, the hackers were able to overload the system and then infiltrate it.

Once the vulnerabilities the hackers were using became public, there was mass panic. This panic drew a lot of attention to what they were doing, making it more difficult for HAFNIUM to take files from the systems they were hacking quickly. To solve the issue of the speed of exfiltration, they started to encrypt the data they were taking and using a 7-zip to compress the files and take them quicker. The next step that they did was to install and use a program called Exchange Powershell to export data that they were taking from emails. Exchange Powershell is is a command line based interface that is used to automate administrative tasks [22]. The next step for these hackers was to use Nishang Invoke-PowerShellTcpOneLine reverse shell. Nishang is a tool in Linux that enables the usage of payloads to run post exploitation tests [23]. The final thing that these unethical hackers did was download PowerCat, a powershell that can generate payloads and transfer files [24], to open a connection to a remote server.

With all of these steps followed the hackers were able to take emails, company data, passwords, and usernames from the companies that they had infiltrated. Once the hack went public the hackers started to encrypt data, install ransomware and malware onto the systems. Through this the hackers were able to take a lot of information.

IV. Impact

The impact of the attack started small, but as this section will explain the attack grew into a large-scale crisis due to multiple factors. The first indication of a vulnerability being found in Microsoft Exchange servers was suspected to be found in early January with a small number of clients being compromised [14]. HAFNIUM being the first organization to exploit this vulnerability was a large reason why this had started as a smaller number of compromises [1].

In the beginning the vulnerability was seen as routine. The number of reports coming in about vulnerabilities was typical for a new patch [1]. The months of February, and January had little instances of servers being compromised, and seemed relatively manageable [14]. The hack was not being shared and deployed at an alarming rate, but this soon changed. The amount of reports coming in changed from a couple a day to thousands a day. Microsoft had set a date for "Patch Tuesday", but had to escalate the progress of development as the attacks had become a crisis. The patch was deployed on March 2nd, and Microsoft had now officially announced the vulnerabilities that were found.

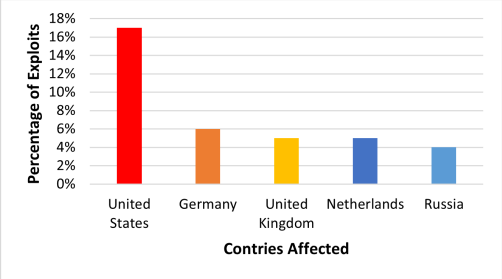

Fig. 4: Countries With Most Attacks

A. Public Announcement Leads to Larger Surge

The announcement led to a large surge in attacks [25], as now it was public that there was something wrong. This with HAFNIUM releasing the hack that was implemented to the public created a chain reaction of more servers being compromised [14]. HAFNIUM, other groups, and amateur hackers now started to scan for more compromised Exchange Servers and started to install back doors on as many of them as possible. The thousands of compromises a day grew. This had all happened within 3 days of the patch and announcement by Microsoft [26]. Even with the speed of the remediation the impact was very high. According to KrebsOnSecurity [27] on March 5th at least 30,000 servers were compromised within the United States, and it is estimated that hundreds of thousands of servers worldwide have had backdoors installed. This is an estimation of the scope of the attack, and is believed to be even larger than this estimation. As of March 9th Microsoft had confirmed that 100,000 servers were still not patched [28], and these systems were still being exploited at this time, and as of the most current report from Microsoft on March 12th there are still 82,000 servers not patched [29].

B. Attacks Deployed on Compromised Servers

Many of the servers that have been compromised fell victim to ransomware attacks. These attacks are believed to have been done by multiple agents, both nation-state and small scale hackers and hacking groups. The ransomware that was identified was *DoejoCrypt/DearCry* which was being deployed into systems that were still vulnerable. This allowed for hackers to enter into vulnerable systems, and start to encrypt the data that was being stored within the systems. This would lead to black mailing, and ransom messages being sent to server owners. As this was seen as one of the most common forms of ransomware used in these attacks it could be inferred that many groups were put into situations where their data was encrypted until an amount of money was paid to the malicious agents. Another common impact for the Exchange servers was the installation of crypto currency mining botnets. Hackers were using the servers as a way to generate crypto currency for themselves, and using the hardware of the companies that had these local Exchange servers.

C. Affects on Organizations

These attacks have been detrimental for many businesses. Microsoft had identified originally that the attack had com-

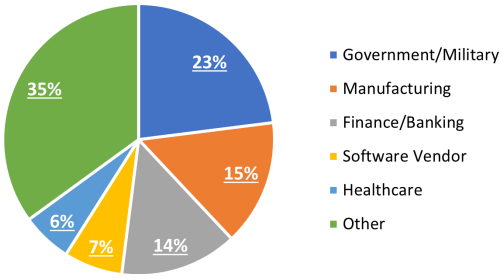

Fig. 5: Organization With Most Attacks

promised over 400,000 Exchange Servers. As shown in the Fig. 4 The United States was hit the worst, but there were also countries like Germany, and the United Kingdoms who suffered from these attacks. In Fig. 5 The largest portion of servers to be attacked was Government, and Military which is what led to the United States government taking action in this large scale compromise of Exchange Servers [30]. After Microsoft had released the first patch the amount of vulnerable servers has decreased tremendously. According to Microsoft in patch notes from March 12, 2021 the vulnerable servers have decreased by 95 percent with this current patch. Even with this patch there are still servers that are vulnerable due to multiple factors such as back door access, and many people who have not updated their Microsoft Exchange server. This large scale attack will have consequences for many years, and still is in the process of being re mediated as server hosts must check console logs, and ensure back doors are not in their server.

The impact of these attacks are large scale, and shows that once the news spreads of a vulnerability the situation can become even more dire. After Microsoft had released the news of the exploit the amount of systems being attacked increased, and more servers became compromised. The main issue was unlike a Cloud network where Microsoft could push an update directly, the local servers had to be updated locally. This in combination with having to release the news of the exploit to the server owners made it possible for attackers to act on this information.

V. Defense Solution

There are a few ways that one can prevent the attack that occurred. The vulnerabilities that were exploited within this are CVE-2021-26855, CVE-2021-26858, CVE-2021-26857, and CVE-2021-27065. CVE-2021-26855 "allows unauthenticated remote code execution" which is a major issue as anyone in the world could access the server [15]. In this section we talk about the various solutions to the issues described in previous sections.

A. First Solution: Install Security Update

The main remedy that Microsoft highly recommended to its users is that they update their systems to at least the March 2021 version as all the previous versions had the vulnerabilities that HAFNIUM used to break into the servers [1]. The issue with this however, is that it is difficult to switch to the current version right away and apply all of the security updates. On

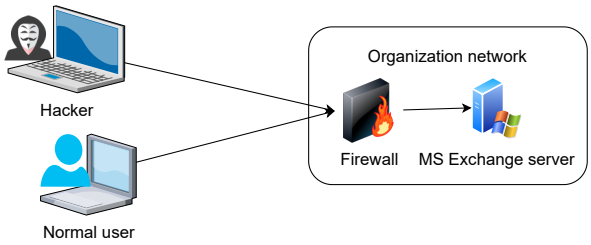

Fig. 6: Secondary Defense Solution blocking port 443 Traffic

their blog, Microsoft also gave some suggestions on how to immediately fix some of the more vulnerable issues such as running a mitigation tool that they wrote. The tools are helpful in closing off the access to the vulnerable servers but do not necessarily run scans to see if the server had already been exploited.

B. Second Solution: Block Traffic to Port 443

Another remedy that Microsoft suggested was to block off port 443, as shown in Fig 6. This port is used for HTTPS traffic [25]. In blocking this port, which would effectively isolate the server from the internet which is how the servers have all been infiltrated. As shown in 6 this was not the best response for the organization that is affected. It would block the hacker from gaining access to the system, but it would also disable access for a normal user of their service as well. Many companies could not use this solution as it would create a block in the way that their businesses operate.

C. Other Possible Solutions

Microsoft has multiple additional steps to take to prevent an attack on the server as well as help stop an attack in progress. Collecting evidence of the attack as well as vulnerabilities is something that is mentioned on Microsoft's blog for responders and investigators multiple times [31]. Collecting evidence of the attack is a key element as it helps the company develop more advanced tools for future attacks that are similar. As with all technology, restarting the system also helps remedy some issues, which is something that is highly suggested in the event of an attack [31]. The final suggestion that Microsoft mentions is that the responder remove any ASPX and ASP.NET files from the system that appear to be malicious.

D. Main Problems

The biggest issue responders encountered when remediating this attack was that the Exchange servers were locally hosted. Due to this Microsoft could not push this patch through directly to all exposed machines [4]. Unlike a cloud where Microsoft has access to these machines the local machines had to be updated by whoever was managing them, such as a companies IT department, or in some cases people had to be brought in to install the patch to companies systems [32]. This led to a slow response time from server owners, and the only way to tell the owners how to fix this was to raise awareness. As the awareness was being raised it helped for users to patch

their servers, but it also led to more hackers starting to increase their implementation of back doors, as it became more public. Even the federal government had become concerned about the large amount of compromised servers, and started to become part of the awareness movement [1].

In conclusion, the best solution is to isolate the server, as many of the vulnerabilities deal with enabling unauthorized remote access through web shells. Then to run the mitigation scripts from Microsoft to temporarily fix the server and protect it from further attacks while you wait for the main server security update to upload.

VI. Conclusion

The Microsoft Exchange Data Breach is a great example of how when a nation state hacker targets a system it is not always possible to mitigate an attack. HAFNIUM had been previously monitoring Microsoft systems, and the speed in infiltrating systems was evident as the day one vulnerability was found, and used very quickly. The Exchange Servers also being accessed were local which helped to escalate the situation, as Cloud Monitoring is done directly by Microsoft, and local servers did not have the same amount of surveillance and security. As well as the patch had to be announced publicly allowing the news of a large exploit on servers reaching many attackers who started scanning for vulnerable systems. Microsoft had taken the correct steps in the fixing the vulnerabilities, but due to the publicity and that the server owners being responsible for updating their servers it made this attack difficult to resolve.

References

[1] NPR, "China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying." https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.

[2] L. Sterle and S. Bhunia, "On SolarWinds Orion Platform Security Breach," in *2021 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, 2021.

[3] E. Caroscio, J. Paul, J. Murray, and S. Bhunia, "Analyzing the ransomware attack on dc metropolitan police department by babuk," in *IEEE International Systems Conference (SysCon)*, 2022.

[4] C. Osborne, "Everything you need to know about the Microsoft Exchange Server hack." https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/.

[5] B. Tran, J. Li, and A. Madry, "Spectral signatures in backdoor attacks," *arXiv preprint arXiv:1811.00636*, 2018.

[6] M. T. I. Center, "HAFNIUM targeting Exchange Servers with 0-day exploits." https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-server.

[7] J. Huddleston, P. Ji, S. Bhunia, and C. Joel, "How VMware Exploits Contributed to SolarWinds Supply-chain Attack," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.

[8] T. Burt, "New nation-state cyberattacks." https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/.

[9] A. Culafi, "The wide web of nation-state hackers attacking the US." https://searchsecurity.techtarget.com/news/252499613/The-wide-web-of-nation-state-hackers-attacking-the-US.

[10] J. Rudie, Z. Katz, S. Kuhbander, and S. Bhunia, "Technical analysis of the nso group's pegasus spyware," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.

[11] Microsoft, "Exchange architecture." https://docs.microsoft.com/en-us/exchange/architecture/architecture?view=exchserver-2019.

[12] M. H. Nguyen Ba, J. Bennett, M. Gallagher, and S. Bhunia, "A Case Study of Credential Stuffing Attack: Canva Data Breach," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.

[13] B. Gibson, D. Lewis, S. Townes, and S. Bhunia, "Vulnerability in Massive API Scraping: 2021 LinkedIn Data Breach," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.

[14] Unknown, "A Basic Timeline of the Exchange Mass-Hack." https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/.

[15] M. S. Team, "Protecting on-premises Exchange Servers against recent attacks." https://www.microsoft.com/security/blog/2021/03/12/protecting-on-premises-exchange-servers-against-recent-attacks/.

[16] Microsoft, "Unified Messaging: Exchange Server." https://docs.microsoft.com/en-us/exchange/unified-messaging-exchange-2013-help.

[17] A. S. Gillis, "What is insecure deserialization?." https://searchsecurity.techtarget.com/definition/insecure-deserialization.

[18] S. Narang, "CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065: Four Zero-Day Vulnerabilities in Microsoft Exchange Server Exploited in the Wild." https://www.tenable.com/blog/cve-2021-26855-cve-2021-26857-cve-2021-26858-cve-2021-27065-four-microsoft-exchange-server-zero-day-vulnerabilities.

[19] A. Prodromou, "An introduction to Web Shells." https://www.acunetix.com/blog/articles/introduction-web-shells-part-1/.

[20] Microsoft, "ProcDump v10.11." https://docs.microsoft.com/en-us/sysinternals/downloads/procdump.

[21] İsmail Baydan, "What is Windows lsass.exe?." https://www.poftut.com/what-is-windows-lsass-exe-local-security-authority-subsystem-service/.

[22] Microsoft, "Exchange Server Powershell." https://docs.microsoft.com/en-us/powershell/exchange/exchange-management-shell?view=exchange-ps.

[23] Kali, "Nishang, Kali Linux Tools." https://www.kali.org/tools/nishang/.

[24] lukebaggett, "Powercat." https://github.com/besimorhino/powercat.

[25] Unknown, "Victims of Microsoft hack scramble to plug security holes." https://www.cbsnews.com/news/microsoft-hack-victims-plug-security-holes/.

[26] Riya, "The data breach at Microsoft Power Apps compromised the personal data of 38 million users." https://thedigitalhacker.com/the-data-breach-at-microsoft-power-apps-compromises-the-personal-data-of-38-million-users/.

[27] "At least 30,000 u.s. organizations newly hacked via holes in microsoft's email software." https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/.

[28] S. Hollister, "Microsoft was warned months ago - now, the Hafnium hack has grown to gigantic proportions." https://www.theverge.com/2021/3/8/22319934/microsoft-hafnium-hack-exchange-server-email-flaw-white-house.

[29] S. Ikeda, "Microsoft Power Apps Data Leak Fallout: 38 Million Records Exposed, State and City Governments Among Those Breached." https://www.cpomagazine.com/cyber-security/microsoft-power-apps-data-leak-fallout-38-million-records-exposed-state-and-city-governments-among-those-breached/.

[30] C. P. Software, "Exploits on Organizations Worldwide Grow Tenfold after Microsoft's Revelation of Four Zero-days." https://blog.checkpoint.com/2021/03/11/exploits-on-organizations-worldwide/.

[31] MSRC, "Guidance for responders: Investigating and remediating on-premises Exchange Server vulnerabilities." https://msrc-blog.microsoft.com/2021/03/16/guidance-for-responders-investigating-and-remediating-on-premises-exchange-server-vulnerabilities/.

[32] W. Defeo, "Staying Dedicated to Vulnerability Management – On-Premise and Cloud." https://www.cylumena.com/insights/microsoft-exchange-breach/.