Zerologon Explored: In-Depth Analysis and Mitigation Strategies for Microsoft's Critical Vulnerability

Hongxiang He*, Josh Self*, Kelton French*, Suman Bhunia*, Mohammad Salman†, Paulo A Regis‡
*Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio, USA
†University of Anbar, Anbar, Iraq
‡ Department of Computer Science, Southeastern Louisiana University–Hammond, Louisiana, USA
Email: {heh13, selfjm, frenchk9, bhunias}@miamioh.edu, mohammed_salman@uoanbar.edu.iq, pregis@southeastern.edu

***Abstract*—In this paper, we discuss Zerologon, a critical vulnerability rated at 10 in severity by authorities, and identified as one of the most exploited vulnerabilities in recent years, as per research. It enables a malicious actor to impersonate any computer or root domain controller, thereby infiltrating the network. In other words, an attacker can gain authentication without needing credentials. This paper not only provides background information on the vulnerable system, including a description of the domain controller and remote procedure, but also offers an in-depth analysis of the potential attack methods employed by malicious actors and their resulting impacts. To facilitate better comprehension, we include relevant mathematical formulas and cryptography knowledge in this section. The novelty of this paper primarily lies in the detailed explanation of the three phases of the solution. The first phase is the initial deployment phase; the second is the finding phase; the third is the 'Enforcement Phase.' This study aims to investigate and analyze the Zerologon vulnerability, focusing on how such attacks infect networks, impact companies, and can be deterred or mitigated.**

***Index Terms*—Index Terms-Microsoft Zerologon, domain controller, active directory, privilege escalation, Remote Procedure Call (RPC), Advanced Encryption Standard (AES)**

I. Introduction

Early in 2020, penetration testers discovered a vulnerability in Microsoft's domain controllers, enabling malicious actors to escalate their privileges and gain access to an entire network.

Privilege escalation is an attack designed to grant unauthorized privileges to a user within a system [1]. Hackers achieve this using five primary methods, which involve exploiting credentials, vulnerabilities, misconfigured systems, malicious code, and social engineering.

For the Zerologon vulnerability, hackers exploit weaknesses in the encryption scheme to achieve privilege escalation. Although Microsoft has issued a patch, some vulnerable systems remain unsecured.

According to Beyond Trust, "In 2020, elevation of privilege vulnerabilities accounted for 44% of all Microsoft vulnerabilities, as reported in the Microsoft Vulnerabilities Report 2021" [2]. This statistic underscores the significance of the Zerologon vulnerability. Additionally, Zerologon received a CVSSv3 score of 10.0/9.0 and a Vulnerability Priority Rating (VPR) score of 10 [3] [4], emphasizing its severity. Microsoft acted swiftly to patch Zerologon and plans to release updates in different phases to protect its customers.

Figure 1 illustrates how an attacker can access numerous computers within a network once they compromise a domain controller. With network access, hackers can potentially obtain sensitive information and launch attacks on the network.

In summary, the primary contributions of this paper encompass:

- **Comprehensive Analysis of Zerologon Vulnerability:** The paper offers an in-depth analysis of the Zerologon vulnerability, covering its background, attack methodologies, and consequences. It provides a detailed understanding of how this critical vulnerability works, its impact on networks, and the potential risks it poses to organizations.
- **Multi-Phase Defense Strategy:** The paper outlines a structured defense strategy against the Zerologon vulnerability, presenting a three-phase approach proposed by Microsoft. It explains how organizations can update and secure their systems to mitigate the risk of exploitation effectively. This practical guidance can serve as a valuable resource for organizations aiming to protect their networks.
- **Importance of Cryptographic Best Practices:** The paper underscores the importance of proper cryptographic implementation and advises against developing custom encryption schemes without extensive research. It emphasizes the significance of using tested and secure encryption methods, contributing to enhanced security awareness among developers and organizations.

To facilitate a comprehensive understanding of the Microsoft Zerologon vulnerability, this paper will be divided into six sections, each addressing various aspects of the vulnerability. These sections will encompass background information necessary for grasping the vulnerability, potential attack vectors, the resulting impact of such attacks, and defense solutions against the Zerologon vulnerability. These components

collectively contribute to a nuanced comprehension of the significance of Zerologon.

II. Background

To gain a better understanding of the attack methodologies, it is essential to first establish a foundation by exploring the vulnerable systems.

This section delves into the core components of domain controllers and remote procedure calls (RPC). Specifically, it highlights the role of a particular RPC known as Netlogon and how it serves as a gateway for malicious actors to escalate their privileges within a domain controller.

The Zerologon vulnerability, also identified as CVE-2020-1472, was uncovered in 2020 [3] [4]. This vulnerability was assigned a CVSSv3 score of 10.0/9.0 and a Vulnerability Priority Rating (VPR) score of 10. These scores underscore the severity of the vulnerability, underscoring the importance for organizations to ensure they have patched their domain controllers.

Microsoft Threat Experts have observed the Zerologon exploit across multiple organizations [5]. In most cases, the observed activity was attributed to security teams conducting scans to identify vulnerable servers [5]. However, a few instances were identified where attackers exploited the vulnerability to target domain controllers that still ran unpatched software. At the time of Daniel Naim's article, 'Zerologon is now detected by Microsoft Defender for Identity,' the patch had already been available for a month, allowing ample time for these servers to be secured [5].

Before delving further into the Netlogon Protocol, it is essential to establish a clear understanding of what a domain controller is, its purpose, and the benefits it offers. A domain controller is a server tasked with handling authentication requests and verifying users on computer networks [6]. These controllers serve as a means of organizing users and computers within the same network in a hierarchical structure. Moreover, domain controllers play a vital role in maintaining organized and secure data. Regardless of an organization's size, having a domain controller is highly recommended, as it significantly enhances network security [6].

Domain controllers play a pivotal role in a network by storing data essential for validating access [6]. If this data were accessible to an attacker, it would grant them access to all devices on the network, making domain controllers a primary target during cyberattacks [6]. However, it's important to note that for an attacker to access a domain controller, they typically require an initial entry vector [5].

It's crucial to differentiate between domain controllers and Active Directory, as they are distinct technologies. A domain controller can serve as a component within an Active Directory server setup [6]. The primary function of a domain controller is to authenticate users by verifying their credentials and granting or denying access accordingly. This authentication role makes domain controllers attractive targets for attackers [6]. Nevertheless, domain controllers are instrumental in enhancing network security and providing centralized user management solutions for businesses.

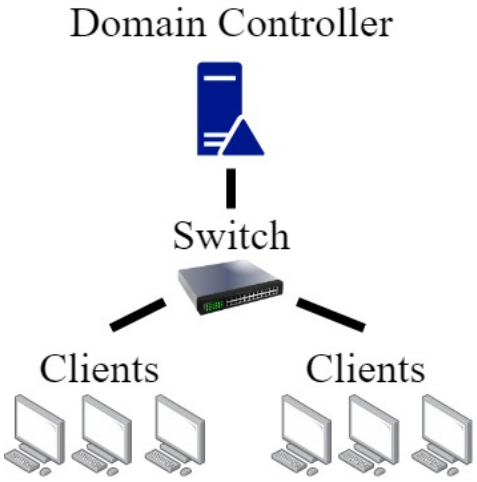

Figure 1: An example of the relationship between a domain controller and users/machines on a network.

Now that we have established what a domain controller is, let's delve into the role of Remote Procedure Calls (RPC) and their interaction with domain controllers. RPC is a communication protocol used by programs to request services from another program located on a different computer within the same network, without needing to understand the network's underlying details [7]. RPC operates based on the client-server model, where the requesting program acts as the client, and the program providing the service functions as the server. Domain controllers utilize RPC for verifying users and machines, and this vulnerability specifically targets a specific RPC known as Netlogon.

The Netlogon Remote Protocol is instrumental for domain controllers in maintaining relationships among domain members, domain controllers within the same domain, and between domain controllers across different domains [8]. These relationships encompass various functions, such as user and machine authentication within domain-based networks and database replication for backup domain controllers. The protocol holds immense significance in the domain controller's functionality as it plays a pivotal role in maintaining critical relationships within a domain.

As mentioned earlier, this vulnerability is exceptionally severe, and Microsoft has already issued a patch for it [9]. The gravity of this exploit stems from the fact that MS-NRPC is used to transmit account changes that a malicious actor can exploit to escalate their privileges once they have infiltrated the network. In the following section, we will explore how a malicious actor might employ this exploit and pinpoint the flaw within the Netlogon Remote Protocol.

The Zerologon vulnerability is rooted in an unreliable cryptographic algorithm used for Netlogon authentication. There are numerous security vulnerabilities associated with broken

or risky cryptographic algorithms (CWE-327), including CVE-2022-26854, CVE-2022-34757, and CVE-2022-34632 [10].

In 2022, CVE-2022-26854, this vulnerability, originated from an insecure key exchange algorithm in Dell EMC PowerScale OneFS, which received a CVSS score of 10.0 [11]. The algorithm in question included the default option, Diffie-Hellman-group14-sha1 [11]. SHA-1, a hash function used in this algorithm, was fully broken in 2020 due to its chosen-prefix collision, allowing attackers to gain full control over the target system [11].

One noteworthy parallel to the Zerologon vulnerability is the encryption scheme Zoom employed for its video conferencing service. Instead of using a robust encryption scheme, Zoom utilized ECB (Electronic Code Book), which failed to provide true encryption for users' videos, allowing objects within the video to remain discernible.

III. Attack Methodology

Now that we have covered the background of this vulnerability, let's explore the attack methodology behind the Zerologon exploit.

In cybercrimes, attackers typically follow a series of phases to infiltrate a system. CVE-2020-1472, also known as Zerologon, enables malicious actors to elevate their privileges without requiring credentials. The most direct approach involves changing the password of the computer account for the domain controller. This vulnerability primarily results from the inadequate implementation of the ComputeNetlogonCredential call within the Netlogon Remote Protocol [12]. There are two key issues contributing to this vulnerability:

Firstly, the initialization vector (IV) should always be a random number, rather than consistently set to all zeros [9].

Secondly, servers fail to reject unencrypted Netlogon sessions [12].

Cryptography is inherently compromised when predictability exists [9]. Therefore, having a random IV every time data is encrypted is crucial. MS-NRPC utilizes the Advanced Encryption Standard - Cipher Feed Back 8-bit (AES-CFB8), which poses challenges due to its limited recognition and testing [9]. This choice of encryption scheme inadvertently exposes the system to cryptographic attacks, enabling hackers to assume complete control over a domain controller [9].

Performing the exploit

A. Performing a brute-force attack

This marks the first step of the exploit. After successfully completing this stage of the attack, hackers can bypass authentication and gain access to the domain controller, as shown in Figure 2

In this phase, the attacker employs an 8-byte challenge and ciphertext composed entirely of zeros, disguising it as originating from the same domain controller [12]. Because the IV is set to all zeros, the attacker's computer can efficiently discover the encryption keys through brute force, a process that takes just a few seconds [9].

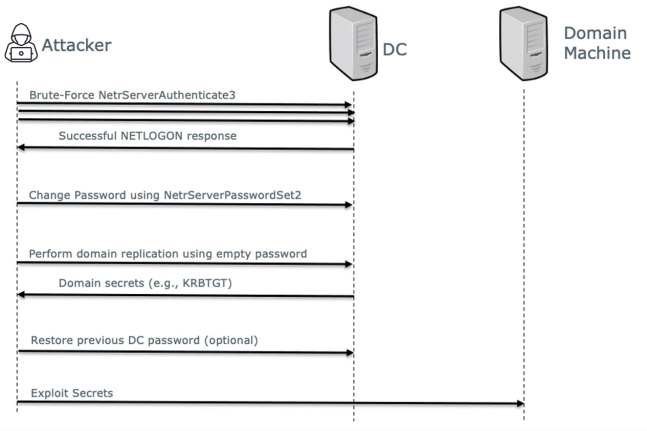

Figure 2: This figure shows how an attacker can gain access to the network and then cover their tracks.

To comprehend how this works, it's essential to understand the concept of Cipher Feedback (CFB) mode. CFB mode, similar to Output Feedback (OFB), is an AES block cipher mode. The encryption process is represented by the formula Vi = EK(Vi-1), where EK represents the block encryption algorithm, and V0 is the initialization vector. The following formula demonstrates encryption in OFB mode: Ci = Vi $\oplus$ Bi. Decryption follows a similar process: Bi = Vi $\oplus$ Ci. OFB mode employs a single encryption algorithm for both encryption and decryption.

We divide the plaintext into N pieces, such as V-1, V-2, and V-3. In each round of ciphertext calculation, we encrypt the ciphertext from the previous round (AES is used for encryption in AES-CFB mode) and then XOR it with the plaintext to obtain a new set of plaintext. Since each AES key results in 00 for every round of encryption, the entire process remains the same when the plaintext consists of 8 zero-bytes, assuming an AES key that produces this outcome.

While there is no guarantee that the AES key will yield the desired result, increasing the number of attempts can help achieve the desired outcome, as shown in Figure 3.

By employing brute force, the attacker would need only 256 attempts to successfully spoof the credentials or password of a client on the network [9]. You might wonder if the system would lock the attacker out after a certain number of attempts. However, the attacker need not worry about being locked out due to too many wrong password attempts, as there is no limit on the number of incorrect password attempts a computer will allow [9].

B. Set the domain controller's password empty

With the domain controller's authentication successfully bypassed, the attacker can proceed to escalate their privileges.

At this stage, the attacker gains the ability to change the password for the account [9]. Among all devices, an Active Directory (AD) server, particularly the root AD server, is the most vulnerable to this attack. Attackers utilize the

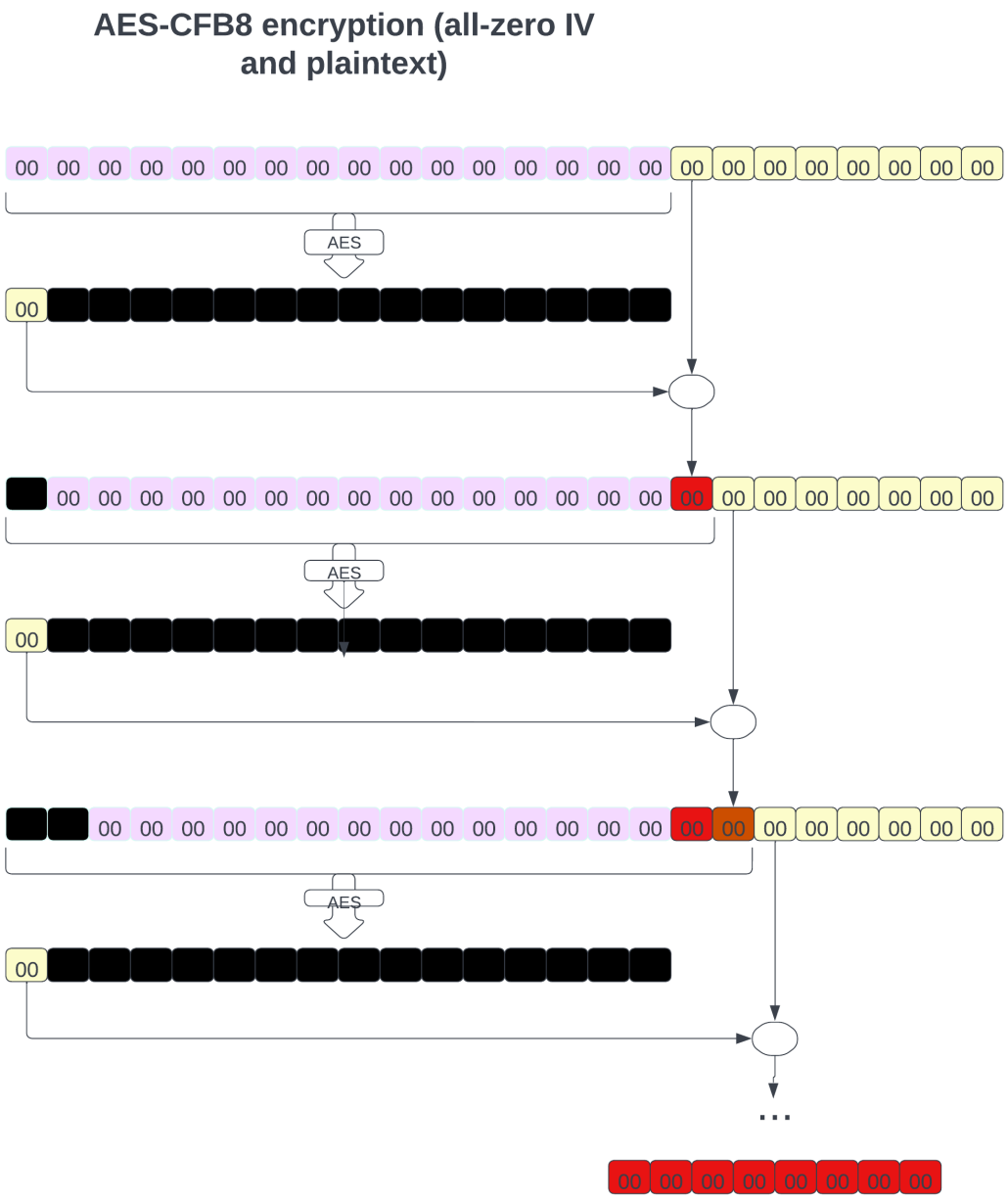

Figure 3: This figure shows process of AES encryption after setting all zeroes

Remote Procedure Call, specifically NetrServerPasswordSet2, to change the password.

However, it's important to note that such actions can disrupt certain domain controller functionalities, as the password recorded in the local registry will no longer match the domain controller's password. To avoid detection, the attacker should revert the password to its previous state as stored in the domain controller's registry [12].

C. Dump additional hashes

Now that the hacker has gained access to the domain controller, they have the capability to execute various actions using the compromised account.

To further exploit this access, the attacker can utilize an empty password to connect to the same domain controller and subsequently employ the Domain Replication Service (DRS) protocol to post additional hashes [12]. With these additional hashes in hand, the attacker is empowered to carry out any desired attacks based on the information obtained.

[13] [9]

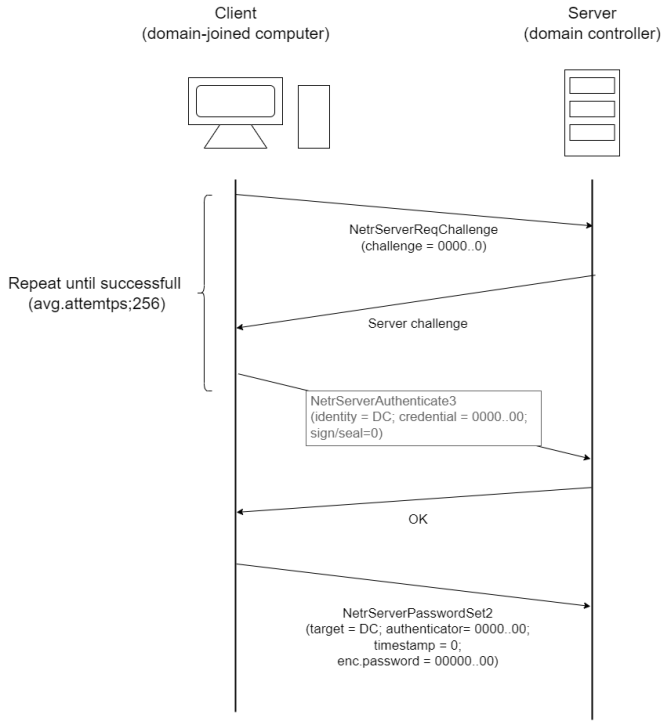

Figure 4: This figure shows the process of Zerologon and how it set an empty computer password on DC.

IV. Impact

The following section covers the various repercussions that a company would have to deal with if a hacker successfully performed the Zerologon exploit.

The impact of a Zerologon attack can be devastating. Microsoft initially assigned it a severity rating of 10 even before any specific information about the vulnerability had been disclosed, highlighting the gravity of the threat as perceived by Microsoft [14]. This underscores the danger it poses.

The attack has a certain limitation—it can only operate from within a network. However, once an attacker gains access to the network, they can leverage the Zerologon vulnerability to seize control of the Active Directory, which contains the stored passwords for systems within the network.

With control over the Active Directory, it becomes relatively straightforward for the attacker to escalate their privileges to that of an administrator, granting them near-complete control over the network. After obtaining these permissions, the attacker can conveniently revert passwords to their original states, allowing them to remain covert [15]. They can enter and exit the system without detection, and even after departure, they can prevent the attack from being discovered for an extended period.

In essence, this attack has a profound impact—it essentially enables any attacker within the local network, including potential malicious insiders, to assume complete control of the Windows domain. Furthermore, the attack remains completely unauthenticated, as it does not require any user credentials, rendering the attacker untraceable [15]. Attackers can introduce various attack chains to further their objectives.

The primary weakness of this attack lies in its requirement for the attacker to establish a foothold within the system. However, cybercriminals have various methods at their disposal to compromise networked computers, including phishing emails, physical access through network cable jacks in office areas, or exploiting other CVEs to gain initial access. Once inside, they attain complete control. This clarifies why Microsoft was deeply concerned about this vulnerability and promptly patched it.

The vulnerability persists as long as legacy authentication protocols are allowed within older operating systems [16]. Microsoft terminated support for these older protocols on patched systems in February 2021. Consequently, non-patched operating systems cannot interact with patched systems. Consequently, organizations are compelled to retire all systems running end-of-life operating systems and transition to modern platforms, a potentially costly endeavor for many companies.

As of July 2021, data from the CISA Research report indicates that Zerologon has become one of the most frequently exploited security vulnerabilities since 2020 [17]. This vulnerability has garnered attention from both the Department of Homeland Security and CISA, prompting them to issue an alert regarding the vulnerability. Executive departments and agencies have been urged to apply the update to remediate the vulnerability [15]. Tools for detecting and mitigating this vulnerability have become commonplace in network security toolkits, given its prevalence in modern attacks.

Part of what made this attack so shocking when it was initially disclosed was its Common Vulnerability Scoring System (CVSS) rating of 8.8, which falls into the category considered “normal” at first [15]. However, on the very same day, the rating was swiftly elevated to the maximum score of 10 [15]. This sudden adjustment reflects that even Microsoft didn’t fully grasp the potentially catastrophic nature of this vulnerability when it was initially discovered.

Researcher Claire Tills has proposed a hypothesis suggesting that the initial rating of 8.8 might have been assigned because the patch was already available, leading Microsoft to assume that most organizations would promptly update their domain controllers [15]. However, they evidently underestimated the initial impact of Zerologon, eventually assigning it the highest possible rating.

One of the challenges in defending against attacks like this is that individuals are integral to the system. If they neglect to update their technology, they inadvertently leave “doors” open to potential attacks.

This attack operates in a stealthy manner since the attacker doesn’t need to log into anything, allowing the vulnerability to slip through undetected. Its ability to conceal itself, coupled with the relatively straightforward messages required for execution, contributed to its rapid adoption. In the first year after Microsoft initially released a patch, there were more than 100 fixes issued for this issue per month for most months [15].

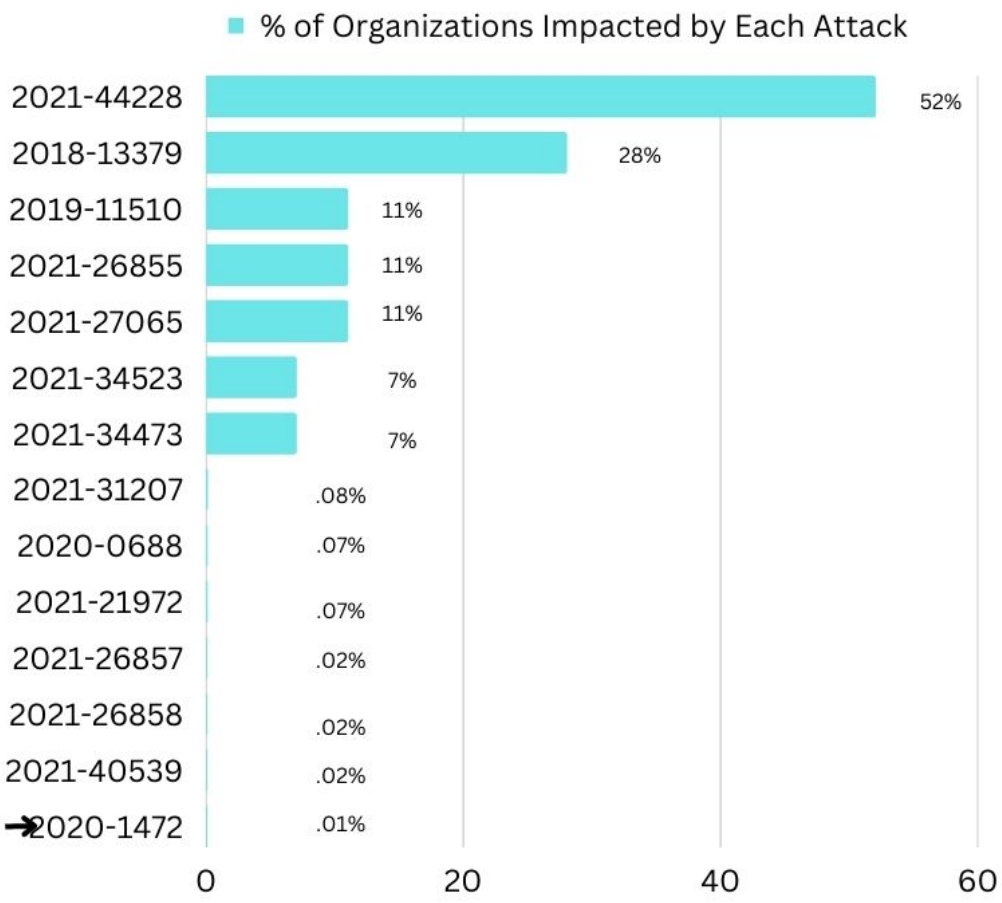

Figure 5: This figure shows the top 15 exploited vulnerabilities in 2021, with Zerologon being the 15th.

The Zerologon vulnerability poses an exceptionally devastating threat to a system due to its all-encompassing nature and untraceable characteristics. Once an attacker gains entry into the network, they can easily assume the role of an administrator by simply sending a series of zeros. Its simplicity has made it one of the top methods employed by hackers in their attacks.

For companies that have not updated their domain controllers to apply the patch, the entire system is left vulnerable. After successfully infiltrating the network, the attacker gains unrestricted access to carry out their objectives, and they can exit without leaving any trace. They can manipulate passwords to gain entry and then revert them to their original states, erasing any evidence of their presence. Collectively, these factors contribute to the profound impact of such attacks, compromising the integrity of the entire network.

V. Defense Solution

This section presents a three-phase defense strategy designed to mitigate the risks associated with the Zerologon vulnerability. The plan involves updating all vulnerable systems, identifying any systems that remain unpatched, and enforcing compliance across all devices.

Microsoft devised a multi-phased strategy to counter the Zerologon vulnerability [18]. These phases enable organizations to progressively enhance the security of their networks over time, providing a comprehensive solution. The first phase involves the release of updates aimed at initially resolving the vulnerability. The subsequent phase, known as the enforcement phase, focuses on ensuring that all devices comply with the updates introduced in the first phase.

Phase 1: Initial Deployment

The first phase, known as the initial deployment phase, was initiated on August 11, 2020, when Microsoft released updates that introduced changes to the Netlogon protocol. These updates aimed to enhance device protection by default, log events for non-compliant devices that were identified, and address the ability to enable protection for all domain-joined devices.

After this update domain controllers will [18]:

- Enforce secure RPC for all Windows-based accounts and domain controllers
- Log denied connections
- Log allowed connections
- Log whenever a vulnerable Netlogon secure channel connection is allowed

While extensive logging and the enforcement of secure RPC channels contribute to resolving the Zerologon vulnerability, it's just the beginning. The subsequent phase is of paramount importance [18]. Without this phase, hackers could potentially identify a vulnerable computer and execute the exploit without the company even being aware of it.

Phase 2: Find and Address

The second phase, known as the finding phase, comes into action after domain controllers have been updated with the patch released on August 11, 2020 [18]. Its primary objective is to identify devices that do not comply with the Phase 1 update. This can be achieved through the use of monitoring software or scripts designed to oversee domain controllers.

Once non-compliant devices are detected, the vulnerability can be promptly addressed. To tackle this vulnerability, companies can update devices as needed. Windows devices that have been fully updated will not rely on vulnerable Netlogon secure channel connections [18]. For non-Windows devices, seeking support from the manufacturer is crucial to ensure the use of a secure RPC channel.

Companies also have the option, if necessary, to permit third-party devices to connect using an unsecured RPC channel, although this approach is not recommended [18]. According to Microsoft's guide on managing changes in Netlogon secure channel connections, allowing vulnerable connections from devices that do not comply with secure RPC standards may carry unknown security risks and should be employed cautiously.

Microsoft 365 Defender offers the capability to employ advanced hunting queries to identify devices suspected of launching the Zerologon exploit [5]. Figure 6 illustrates a sample outcome of such queries, simplifying the process for companies to pinpoint malicious actors and devices in need of updates.

Once all non-compliant devices within a network have been identified and addressed, the next phase, enforcement mode, can be initiated [18].

Phase 3: Microsoft Enforcement Mode

The third phase, known as the "Enforcement Phase," was introduced on February 9, 2021 [18]. Microsoft has taken a proactive stance in addressing the Zerologon vulnerability by enabling "enforcement mode" by default on domain controllers. This measure, which commenced on February 9, 2021, is designed to block connections from devices that could potentially exploit the Zerologon vulnerability.

Enforcement mode functions by mandating that all devices connecting to the domain controller use secure RPC with the Netlogon secure channel [19]. While customers have the option to allow non-compliant devices to connect, this practice is not ideal. This phase represents the final step in Microsoft's plan to counter the Zerologon threat, but it's important to note that security risks may persist beyond this phase.

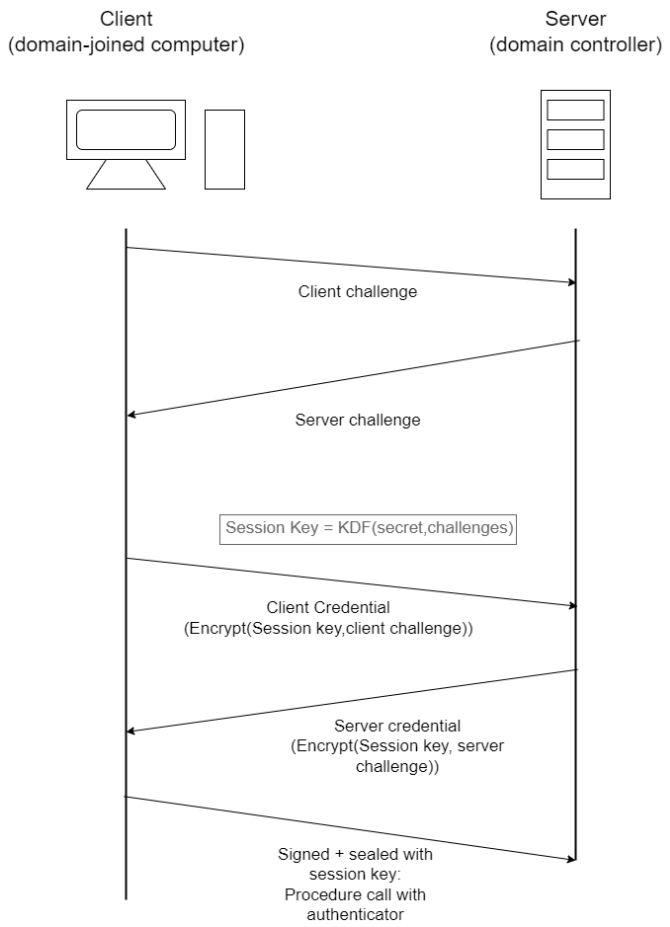

Figure 6: This figure shows simplified authentication handshake.

Stopping entry vectors

The Zerologon vulnerability requires a malicious actor to be inside a network to execute the exploit, as illustrated in Figure 4. While Microsoft's three-phase plan is an effective means of mitigating the Zerologon vulnerability, it's crucial to recognize that the patch primarily addresses the vulnerability itself and does not include mechanisms for detecting or removing hackers from the network. This underscores the importance of maintaining network security and adhering to sound security practices.

Microsoft is taking the Zerologon vulnerability seriously [19]. By patching vulnerable systems and rigorously enforcing these patches, Microsoft aims to encourage more companies to update their vulnerable domain controllers. Defending against this vulnerability ensures that malicious actors are prevented from gaining access to networks and potentially harming customers.

VI. Conclusion

The Microsoft Zerologon vulnerability (CVE-2020-1472) is a threat that can have a significant impact due to its simplicity in attack methods, but it can be effectively defended against.

One of the most concerning aspects of the Zerologon vulnerability is its wide range of potential targets. Any server running Windows 2019, 2016, 2012, 1909, 1903, or 1809 versions without the necessary patch is vulnerable [17]. Once an attacker gains access to a system, they can achieve privilege escalation, granting them administrator-level control and the ability to execute various commands. Subsequently, attackers often attempt to escalate their privileges further to conceal their actions effectively.

The Microsoft Zerologon vulnerability (CVE-2020-1472) has gained notoriety among hackers due to its versatility, ease of use, and effectiveness. In fact, it ranked among the top 20 used exploits in 2020 and climbed to the 15th spot on the list of most exploited vulnerabilities by hackers in 2021 [17], as shown in Figure 5. The Zerologon attack's simplicity, combined with its ability to infiltrate systems without requiring login credentials, has made it a staple for malicious actors.

What makes the Zerologon vulnerability particularly dangerous is its accessibility, even to less experienced attackers. This ease of use allows script-kiddie hackers to leverage the exploit to gain significant control over a system. While the initial hurdle is obtaining network access, once inside, the attacker can manipulate inputs to force certain values to be all zeroes, ultimately impersonating a network device. This provides them with the opportunity to escalate their privileges and launch successful attacks on the system [14].

Furthermore, the human factor plays a crucial role in the threat posed by this attack. Patching is a key mitigation measure, but it relies on individuals taking action to update their Windows devices. When the Zerologon attack gained popularity in 2020, the risk could have been mitigated through patching. However, the effectiveness of this solution depended on individuals being informed and proactive about applying updates, and a lack of information or action inadvertently provided attackers with an advantage [15]. This highlights the need for robust cybersecurity practices and awareness to counter evolving threats.

In conclusion, safeguarding against cybersecurity threats hinges on a fundamental practice: keeping software and hardware updated. In most cases, when vulnerabilities are known, steps are taken to mitigate or eliminate the potential for exploitation. However, it's crucial to recognize that no defense is infallible, as highlighted by the Zerologon vulnerability, which emerged with little prior knowledge and was addressed simultaneously with the release of a patch.

The Zerologon challenge remains an ongoing, evolving issue. Microsoft had to adapt its response from day one by adjusting the severity rating and crafting a multi-phase solution that evolved alongside attackers. This exemplifies the dynamic nature of cybersecurity, where hackers continually seek new vulnerabilities, defenses are erected in response, and the cycle persists. Staying aware of existing threats is paramount.

Looking ahead, developers should invest in studying effective cryptographic implementation. Additionally, companies should exercise caution and avoid attempting to devise their own encryption schemes without thorough research. Relying on established, proven encryption methods can significantly reduce the prevalence of vulnerabilities like Zerologon, safeguarding both companies and their customers against the menace of cyberattacks. Cybersecurity is a constantly evolving landscape, and proactive measures are essential to navigate its complexities effectively.

References

[1] "What Is Privilege Escalation?." https://www.crowdstrike.com/cybersecurity-101/privilege-escalation/.

[2] "Privilege Escalation Attack and Defense Explained." https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained.

[3] "Netlogon Elevation of Privilege Vulnerability." https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472.

[4] S. Narang, "CVE-2020-1472: Microsoft Finalizes Patch for Zerologon to Enable Enforcement Mode by Default." https://www.tenable.com/blog/cve-2020-1472-microsoft-finalizes-patch-for-zerologon-to-enable-enforcement-mode-by-default.

[5] D. Naim, "Zerologon is now detected by Microsoft Defender for Identity." https://www.microsoft.com/security/blog/2020/11/30/zerologon-is-now-detected-by-microsoft-defender-for-identity/.

[6] "What is a Domain Controller, When is it Needed + Set Up." https://www.varonis.com/blog/domain-controller.

[7] L. Rosencrance, "Remote Procedure Call (RPC)." https://www.techtarget.com/searchapparchitecture/definition/Remote-Procedure-Call-RPC.

[8] "[MS-NRPC]: Netlogon Remote Protocol." https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-nrpc/19896c1c-7e64-419b-a759-a9dc5662a780.

[9] M. Simakov and Y. Zinar, "what is Zerologon." https://www.trendmicro.com/en_us/what-is/zerologon.html/.

[10] "CVE details cweid-327." https://www.cvedetails.com/vulnerability-list/cweid-327/vulnerabilities.html.

[11] "Exploring CWE-327 Use of a Broken or Risky Cryptographic Algorithm." https://www.ubiqsecurity.com/exploring-cwe-327-use-of-a-broken-or-risky-cryptographic-algorithm.

[12] M. Simakov and Y. Zinar, "Zerologon (CVE-2020-1472): An Unauthenticated Privilege Escalation to Full Domain Privileges." https://www.crowdstrike.com/blog/cve-2020-1472-zerologon-security-advisory/.

[13] A. Z. Mustafeez, "What is OFB?." https://www.educative.io/answers/what-is-ofb.

[14] C. Cimpanu, "Zerologon attack lets hackers take over enterprise networks: Patch now." https://www.zdnet.com/article/zerologon-attack-lets-hackers-take-over-enterprise-networks/.

[15] S. Kelly, "One Year Later, a Look Back at Zerologon." https://www.darkreading.com/vulnerabilities-threats/one-year-later-a-look-back-at-zerologon.

[16] M. Chabot, "The Zerologon Vulnerability and its Long-term Impact." https://thrivenextgen.com/the-zerologon-vulnerability-and-its-long-term-impact/.

[17] "Alert (AA21-209A) Top Routinely Exploited Vulnerabilities." https://www.cisa.gov/uscert/ncas/alerts/aa21-209a.

[18] "How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472." https://support.microsoft.com/en-us/topic/how-to-manage-the-changes-in-netlogon-secure-channel-connections-associated-with-cve-2020-1472-f7e8cc17-0309-1d6a-304e-5ba73cd1a11e.

[19] L. O'Donnell, "Microsoft Implements Windows Zerologon Flaw 'Enforcement Mode'." https://threatpost.com/microsoft-implements-windows-zerologon-flaw-enforcement-mode/163104/.