Open in app ↗ Sign up Sign in

Medium Search Write

Hunting for Zerologon

BI.ZONE · Follow

13 min read · Nov 9, 2020

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

CVE-2020–1472, or Zerologon, has already been named one of the most dangerous vulnerabilities discovered in recent years. It allows an attacker to compromise a domain controller's machine account and access the contents of the entire Active Directory database. The only thing the attacker requires to exploit this vulnerability is a network connection to the company's domain controller.

We did our own research on Zerologon and developed various methods to detect its existence: by Windows audit log events, by network traffic and by YARA rules. This article will focus on each of them in detail. The methods

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Zerologon was caused by a flaw in the cryptographic authentication scheme used by Netlogon Remote Protocol (MS-NRPC). MS-NRPC handshake and authentication involves the use of AES-CFB8 mode (with 8-bit encrypted feedback). This is a version of the AES block cipher and is designed to work with input blocks of 8 bytes instead of the usual 16 bytes (128-bit).

As Tervoort discovered, applying AES-CFB8 cipher to plaintext consisting of only zeros will result in the same plaintext cipher. This is due to an implementation error for 1 of the 256 keys.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

1. Sending zero bytes. Instead of sending eight random bytes, the attacker sends eight null bytes. The attacker repeats sending these messages until the server successfully accepts one of them and thus bypasses the authentication process. In the case of Zerologon, an average of 256 attempts to send a single zero byte message are required to connect to the server successfully.

2. Disabling the RPC signing and sealing mechanism. MS-NRPC uses the RPC signing and sealing mechanism for transport layer encryption. Usually, encryption is a mandatory process for data transfer, but in MS-NRPC this

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

PoC and Exploits

The first PoC was published by Secura at GitHub. The script will try to exploit the Zerologon vulnerability: once the connection is established successfully, it will terminate the work immediately and will not perform any actions via Netlogon.

As for exploits, there have already been many at the time of publishing this article. However, they all behave the same way: they either reset the password or set it to a user-defined value.

Medium

Sign up to discover human stories that deepen your understanding of the world.

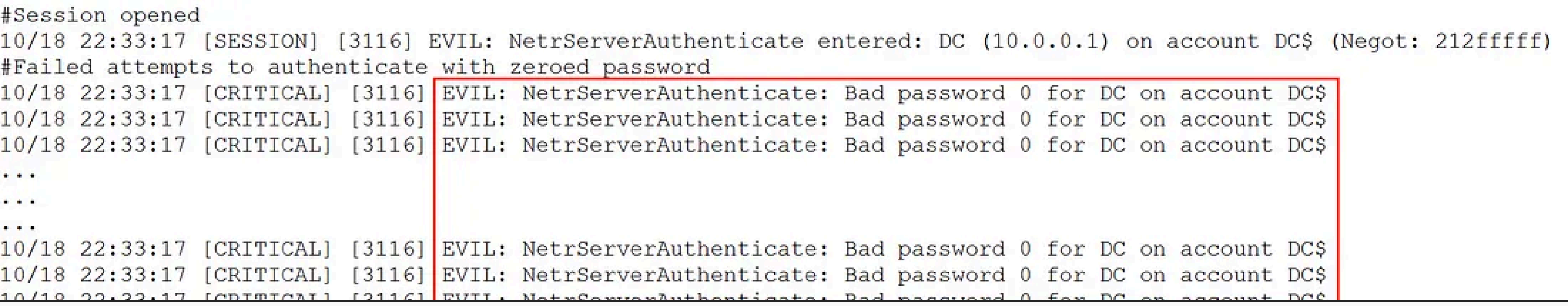
Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

`C:\Windows\debug\netlogon.txt`. The Netlogon service must then be restarted. The screenshot below shows a few interesting lines that were logged by the Netlogon service during the exploitation of the Zerologon vulnerability.



```
#Session opened
10/18 22:33:17 [SESSION] [3116] EVIL: NetrServerAuthenticate entered: DC (10.0.0.1) on account DC$ (Negot: 212fffff)
#Failed attempts to authenticate with zeroed password
10/18 22:33:17 [CRITICAL] [3116] EVIL: NetrServerAuthenticate: Bad password 0 for DC on account DC$
10/18 22:33:17 [CRITICAL] [3116] EVIL: NetrServerAuthenticate: Bad password 0 for DC on account DC$
10/18 22:33:17 [CRITICAL] [3116] EVIL: NetrServerAuthenticate: Bad password 0 for DC on account DC$
...
...
...
10/18 22:33:17 [CRITICAL] [3116] EVIL: NetrServerAuthenticate: Bad password 0 for DC on account DC$
10/18 22:33:17 [CRITICAL] [3116] EVIL: NetrServerAuthenticate: Bad password 0 for DC on account DC$
10/18 22:33:17 [CRITICAL] [3116] EVIL: NetrServerAuthenticate: Bad password 0 for DC on account DC$
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Multiple unsuccessful authentication attempts result in the generation of event 5805 on the domain controller: ‘The session setup from the computer <hostname> failed to authenticate. The following error occurred: Access is denied’ (see example event in the screenshot below).

Additionally, if an incorrect domain controller account name was specified in the exploit, an attempt to authenticate with an incorrect account will generate event 5723 on the domain controller: ‘The session setup from computer <hostname> failed because the security database does not contain a trust account <account> referenced by the specified computer’ (see the

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

changed using Zerologon.

By default, the computer account password has a maximum validity period of 30 days. Upon expiry of this period, the password will be changed by the operating system using the Netlogon protocol. This value can be changed using local or group policy:

Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options → Domain member: Maximum machine account password age

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

by the system. It is logged on the computer that changed the password'. This event means that the computer account has been legitimately changed by the system.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

when both of (**EventID = '4742' AND TargetUserName IN "Domain_Controller_Accounts_List" AND PasswordLastSet != '-'**) and not **(EventID = '5823')** were detected on the same host within 1 minute.

The rule implemented according to the logic described above will enable the exploitation Zerologon to be detected with high precision. No additional configuration of the audit policy will be required for it to work. The only thing that will be required is to prepare a list of the organisation's domain controllers and place it in the Domain_Controller_Accounts_List.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

in the vast majority of cases at least 10 attempts are required to bypass the authentication mechanism. This anomaly can be easily detected in network traffic. The DCE/RPC protocol is used to send ServerChallenge requests using the NetrServerReqChallenge method and attempts to authenticate using the NetrServerAuthenticate method with a zero ClientChallenge value to the MS-NRPC RPC interface.

The traffic from Mimikatz version 2.2.0–20200916, without DCE/RPC load encryption when bypassing zero key authentication, contains an artifact in the Computer Name variable of the NetrServerReqChallenge method

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

NetrServerAuthenticate2 (Opnum 15) repetitive methods in the traffic from a single source within a few seconds' time frame.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

`(hNetrServerAuthenticate3)`, the Local Security Authority Subsystem Service (LSASS) is used in the authentication process. When calling the authentication server, an artifact — a structure containing the parameters transferred to the `hNetrServerAuthenticate2 (hNetrServerAuthenticate3)` function — is sent to the `lsass.exe` process address space (see figure below).

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

A byte is also visible in memory, meaning the type of secure channel Netlogon ServerSecureChannel (06).

However, sometimes for unspecified reasons this and other bytes may take different values that are not related to the above description. Artifacts in the address space of the `lsass.exe` process are stored in a segment that does not involve long-term data storage and can be deleted at any time after they appear. Our research has shown that in most cases, artifacts will remain in the `lsass.exe` process memory for no longer than half an hour after which they are overwritten with other data.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

form of bytes ff ff 2f 21, which contain flags that are used by all the exploits tested during the survey.

In addition to bypassing the detection logic of YARA rules, which will be described below, the use of some Netlogon Negotiable Options flags results in the lsass address space leaving no artifacts that can be used to identify the exploitation of Zerologon. One of these flags is 0x312fffff. Our research confirms the hypothesis that the flags which make it possible to disable the RPC signing and sealing mechanism are not actually designed for this purpose.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

and the appropriate tools, you can periodically scan the lsass.exe process memory on domain controllers.

Of course, all of the above approaches can be used in tandem, which will make it possible not only to detect cases of Zerologon past and present exploitation, but also to increase the speed of incident classification.

Reports of corporate information systems being encrypted during Zerologon attacks are becoming more and more common. Therefore, it should be remembered that the ability to detect Zerologon exploitation is not enough

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

BI.ZONE: an expert in digital risks management. We help organizations around the world to develop their businesses safely in the digital age

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app