Detecting and Hunting for the PetitPotam NTLM Relay Attack

research.nccgroup.com/2021/09/23/detecting-and-hunting-for-the-petitpotam-ntlm-relay-attack/

September 23, 2021

Overview

During the week of July 19th, 2021, information security researchers published a proof of concept tool named “PetitPotam” that exploits a flaw in Microsoft Windows Active Directory Certificate Servers with an NTLM relay attack. The flaw allows an attacker to gain administrative privileges of an Active Directory Certificate Server once on the network with another exploit or malware infecting a system.

The following details are provided to assist organizations in detecting and threat hunting for this and other similar types of threats.

Preparation

The default settings of Windows logging do not often catch advanced threats. Therefore, Windows Advanced Audit Logging must be optimally configured to detect and to be able to threat hunt PetitPotam and similar attacks.

Organizations should have a standard procedure to configure the Windows Advanced Audit Policies as a part of a complete security program and have each Windows system collect locally significant events. NCC Group recommends using the following resource to configure Windows Advanced Audit Policies:

> Malware Archaeology – Windows Logging Cheat Sheets

Log rotation can be another major issue with Windows default log settings. Both the default log size should be increased to support detection engineering and threat hunting.

Ideally, organizations should forward event logs to a log management or SIEM solution to operationalize detection alerts and provide a central console where threat hunting can be performed. Alternatively, with optimally configured log sizes, teams can run tools such as PowerShell or LOG-MD to hunt for malicious activity against the local log data.

Detecting and Threat Hunting NTLM Relay Attacks

The PetitPotam attack targets Active Directory servers running certificate services, so this will be the focus of the detection and hunting. Event log data is needed to detect or hunt for PetitPotam. The following settings and events can be used to detect this malicious activity:

Malicious Logins

PetitPotam will generate an odd login that can be used to detect and hunt for indications of execution. To collect Event ID 4624, the Windows Advanced Audit Policy will need to have the following policy enabled:

> Logon/Logoff – Audit Logon = Success and Failure

The following query logic can be used:

- Event Log = Security
- Event ID = 4624
- User = ANONYMOUS LOGON
- Authentication Package Name = NTLM*
- Elevated Token – *1842

Sample Query

The following query is based on Elastic's WinLogBeat version 7 agent.

```
"event.code"="4624" and winlog.event_data.AuthenticationPackageName="NTLM*"
and winlog.event_data.ElevatedToken="*1842" |
PackageName:=winlog.event_data.AuthenticationPackageName |
Token:=winlog.event_data.ElevatedToken |
WS_Name:=winlog.event_data.WorkstationName |
LogonProcess:=winlog.event_data.LogonProcessName |
LogonType:=winlog.event_data.LogonType |
ProcessName:=winlog.event_data.ProcessName |
UserName:=winlog.event_data.SubjectUserName |
Domain:=winlog.event_data.SubjectDomainName |
TargetDomain:=winlog.event_data.TargetDomainName |
TargetUser:=winlog.event_data.TargetUserName |
Task:=winlog.event_data.TargetUserName| table([event.code, @timestamp,
host.name, event.outcome, WS_Name, UserName, Domain, Token, PackageName,
LogonProcess, LogonType, ProcessName, TargetDomain, TargetUser, Task])
```

Malicious Share Access

PetitPotam will generate odd network share connections that can be used to detect and hunt for indications of execution. To collect Event ID 5145, the Windows Advanced Audit Policy will need to have the following policy enabled:

- Object Access – Audit Detailed File Share = Success
- Object Access – File Share = Success

The following query logic can be used:

- Event Log = Security
- Event ID = 5145
- Object Name = *IPC*
- Target Name = ("lsarpc" or "efsrpc" or "lsass" or "samr" or "netlogon"

Sample Query

The following query is based on Elastic's WinLogBeat version 7 agent.

```
"event.code"="5145" and winlog.event_data.ShareName=*IPC* and ("lsarpc" or
"efsrpc" or "lsass" or "samr" or "netlogon" or "srvsvc")
| Status:= keywords[0] | Src_IP:= winlog.event_data.IpAddress | PID:=
winlog.process.pid | UserName:=winlog.event_data.SubjectUserName | Domain:=
winlog.event_data.SubjectDomainName | Target_File:=
winlog.event_data.RelativeTargetName | Path:= winlog.event_data.ShareLocalPath |
Share:= winlog.event_data.ShareName | ObjectType:=winlog.event_data.ObjectType
| table([event.code, @timestamp, host.name, Status, Src_IP, PID, UserName, Domain,
task, Path, Share, Target_File, ObjectType])
```

If you find any false positives, validating them and excluding or refining the query may be needed. We hope this information can assist your detection and threat hunting efforts to detect this and similar types of attacks.

Additional Reading and Resources

- Windows Logging Cheat Sheets – https://www.malwarearchaeology.com/cheat-sheets
- Blumira Blog on PetitPotam – https://www.blumira.com/ntlm-relay-attack-petitpotam
- PetiPotam POC for testing and assessments – https://github.com/topotam/PetitPotam
- Mitigating NTLM Relay Attacks on Active Directory Certificate Services – https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429
- Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS) – https://msrc.microsoft.com/update-guide/vulnerability/ADV210003
- Extended Protection for Authentication – https://msrc-blog.microsoft.com/2009/12/08/extended-protection-for-authentication
- Audit Script PSPKIAudit – https://github.com/GhostPack/PSPKIAudit
- Abusing Active Directory Certificate Services – https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf
- AD CS relay attack – practical guide – https://www.exandroid.dev/2021/06/23/ad-cs-relay-attack-practical-guide/