CyberProof®

October 2021

Advanced Threat Hunting

CyberProof Guidelines for Threat Hunting

Microsoft HiveNightmare Vulnerability & BazarLoader to Conti Ransomware

Table of Contents

Session Stakeholders

This report was created for threat hunters and security analysts with highly technical skills – skills that can be used to identify threats by developing hypotheses, locating infection evidence across environments, and providing indicators for attack detection. The guidelines should provide the logic for hunting malware samples or malicious techniques - and can be converted into detection rules or mitigation strategies as well.

Hunting Via the SIEM Platform

Security information and event management (SIEM) is a software solution that aggregates and analyzes activity from various log sources across an entire IT infrastructure. SIEM platforms collect security data from network devices, servers, domain controllers, and more. CyberProof's guidelines assume that environmental data is collected into the SIEM platform, but if there is no SIEM platform (or the relevant data is not gathered), you should develop guidelines in order to limit the hunt to relevant data sources.

Hunting Via the EDR Platform

Endpoint Detection and Response (EDR) refers to a category of tools used to detect and investigate threats on endpoints. EDR tools typically provide detection, investigation, threat hunting, and response capabilities.

For additional malware review, please refer to CyberProof's Cyber Hub, or to the Appendix at the end of this document.

For more details or assistance regarding hunting workflows, please contact the CyberProof Threat Hunting team at hunters@cyberproof.com.

Microsoft HiveNightmare Vulnerability

Threat Explained

Recently, researchers discovered a new vulnerability in the Windows SAM database called HiveNightmare (aka SeriousSAM). Exploitation of this vulnerability could allow non-admin users to access the SAM database, which is a storage of local passwords and users. Essentially, an attacker could run arbitrary code with SYSTEM privileges, and then install programs; view, change, or delete data - or create new accounts with full admin rights.

The vulnerability affects Windows 10 version 1809 and newer operating systems. Additionally, an exploit is publicly available. After this discovery, Microsoft addressed the vulnerability and assigned it the following CVE ID: CVE-2021-36934. Microsoft has not yet published an official patch for the vulnerability; however, several mitigations and workarounds are suggested.

Since Windows 10 build 1809, the Access Control Lists (ACLs) for %windir%\System32\config have been granting read access to non-admin users. This is the primary directory that contains the files for the Windows Registry, including the Security Account Manager (SAM), which stores users' passwords. An attacker with the ability to execute code on a target host could exploit this vulnerability to elevate their privileges to SYSTEM. Due to the ACLs granting read access, Volume Shadow Copy Service (VSS) shadow copies of these files may exist. These could be, for example, as part of system restore points.

Correlated MITRE Techniques

Tactic	Technique	Description
Privilege Escalation	(T1078.003) Valid Accounts: Local Accounts	Adversaries could obtain and abuse credentials of a local account as a means of gaining initial access, persistence, privilege escalation, or defense evasion.
Credential Access	(T1003.002) Credential Dumping: Security Account Manager	Adversaries could attempt to extract credential material from the SAM database - either through in-memory techniques or through the Windows Registry where the SAM database is stored.
Credential Access	(T1552.001) Unsecured Credentials: Credentials in Files	Adversaries could search local file systems and remote file shares for files containing insecurely stored credentials.
Credential Access	(T1003.003) Credential Dumping: NTDS	Adversaries could attempt to access or create a copy of the Active Directory domain database in order to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights.
Defense Evasion	(T1218) Signed Binary Proxy Execution	Adversaries could bypass process and/or signature-based defenses by proxying execution of malicious content with signed binaries.
Defense Evasion	(T1202) Indirect Command Execution	Adversaries could abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters
Discovery	(T1012) Query Registry	Adversaries could interact with the Windows Registry to gather information about the system, configuration, and installed software.

Operational Hunting Workflows

The CyberProof Threat Hunting team worked collaboratively with the Cyber Threat Intelligence (CTI) team to import the external sources of information that the hunt was based on, as described below. We categorized the hunt according to the type of platform in which the indicators need to be verified: either the SIEM platform or the EDR platform.

Hunting Via the SIEM Platform

(Relevant Data Sources: Windows Security Logs)

- Hunt for attempts to read 'config' directory content:
  - `Event ID: 4663`
  - Group SID: S-1-5-32-545 (BUILTIN\Users group)
  - Relevant files:
    - %windir%\system32\config\sam
    - %windir%\system32\config\security
    - %windir%\system32\config\system
    - %windir%\system32\config\software

Hunting Via the EDR Platform

- Hunt for attempts to read 'config' directory content:
  - Access level: Read
  - Group SID: S-1-5-32-545 (BUILTIN\Users group)
  - Relevant files:
    - %windir%\system32\config\sam
    - %windir%\system32\config\security
    - %windir%\system32\config\system
    - %windir%\system32\config\software

Prevention

The following recommendations have been provided by Microsoft. This is a temporary workaround until a patch is available. You must do both actions below in order to mitigate the vulnerability, and it is not known if it will affect different backup utilities that rely on the shadow copies. Please note that the steps include deleting ALL VSS shadow copies, after which you will not be able to restore them.

1. Reset the ACLs on the live registry hive files using the ICACLS command:

   - Command Prompt (run as administrator):

```
icacls $env:windir\system32\config\*.* /inheritance:e
```

   - Windows PowerShell (run as administrator):

```
icacls $env:windir\system32\config\*.* /inheritance:e
```

2. Verify the relevant permissions using the following script:

```
icacls %windir%\system32\config\sam && icacls
%windir%\system32\config\security && icacls
%windir%\system32\config\system && icacls
%windir%\system32\config\software
```

   The BUILTIN\Users group should not be given RX permissions to files in the %windir%\system32\config directory.

3. Remove all existing restore points or shadow copies:

   - Identify whether Shadow volumes exist with either Command Prompt or PowerShell (run as administrator):

```
vssadmin list shadows
```

   - Delete any System Restore points and Shadow volumes that existed prior to restricting access to the contents of %windir%\system32\config.

4. Recreate a new restore point, if needed.

PowerShell Script to Detect Vulnerable Hosts

Run this script on remote hosts (using SCCM or PsExec) to detect which hosts are vulnerable:

```
$LocalBuiltInUsersGroupName = (Get-Localgroup -SID S-1-5-32-545).Name
$checkPermissions = icacls c:\Windows\System32\config\sam
if ($checkPermissions -like "*$($LocalBuiltInUsersGroupName):(I)(RX*)*")
{
    Write-Host "Computer is vulnerable"
    Exit 1
}
else {
    Write-Host "Computer is not vulnerable"
    Exit 0
}
```

BazarLoader to Conti Ransomware

Threat Explained

BazarLoader is known to spread via phishing emails that purport to stem from legitimate sources. For instance, a malicious email could be disguised as payroll reports or lists of terminated employees. Clicking on the malicious link to documents can redirect the targeted victim to malicious landing pages resembling Excel sheets, PDFs, or Word documents.

BazarLoader has continued to be one of the preeminent initial access brokers for ransomware threat actor access. In July, we witnessed a BazarLoader campaign that deployed Cobalt Strike and ended with domain-wide encryption using Conti ransomware.

In this case, the initial activity began with a BazarLoader DLL. Upon initial execution on the beachhead, the malware made an initial connection to command and control, and then a few minutes later performed discovery tasks on the host using Microsoft utilities. After this activity, the host went quiet for about one hour before downloading and executing a Cobalt Strike beacon DLL.

Correlated MITRE Techniques

Tactic	Technique	Description
Defense Evasion	(T1550.002) Use Alternate Authentication Material: Pass the Hash	Adversaries could "pass the hash" using stolen password hashes and move laterally within an environment.
Privilege Escalation	(T1055) Process Injection	Process injection is a method of executing arbitrary code in the address space of a separate live process.
Execution	(T1059.001) Command and Scripting Interpreter: PowerShell	Adversaries could abuse PowerShell commands and scripts for execution.
Discovery	(T1018) Remote System Discovery	Adversaries could attempt to get a listing of other systems by IP address, hostname, or other logical identifiers on a network that could

Tactic	Technique	Description
		be used for lateral movement from the current system.
Execution	(T1569.002) System Services: Service Execution	Adversaries could abuse the Windows service control manager to execute malicious commands or payloads.
Execution	(T1059.003) Command and Scripting Interpreter: Windows Command Shell	Adversaries could abuse the Windows command shell for execution.
Discovery	(T1087) Account Discovery	Adversaries could attempt to get a listing of accounts on a system or within an environment.
Discovery	(T1482) Domain Trust Discovery	Adversaries could attempt to gather information on domain trust relationships that could be used to identify lateral movement opportunities in Windows multi-domain/forest environments.
Discovery	(T1082) System Information Discovery	Adversaries could attempt to get detailed information about the operating system and hardware.
Lateral Movement	(T1021) Remote Services	Adversaries could use valid accounts to log in to a service specifically designed to accept remote connections - such as telnet, SSH, and VNC.
Execution	(T1047) Windows Management Instrumentation	Adversaries could abuse Windows Management Instrumentation (WMI) to achieve execution.
Exfiltration	(T1048) Exfiltration Over Alternative Protocol	Adversaries could steal data by exfiltrating it over a different protocol than that of the existing command and control channel.
Lateral Movement	(T1021.001) Remote Services: Remote Desktop Protocol	Adversaries could use valid accounts to log into a computer using the Remote Desktop Protocol (RDP).
Lateral Movement	(T1021.002) Remote Services: SMB/Windows Admin Shares	Adversaries could use valid accounts to interact with a remote network share using Server Message Block (SMB).
Impact	(T1486) Data Encrypted for Impact	Adversaries could encrypt data on target systems or on large numbers

Tactic	Technique	Description
		of systems in a network to interrupt availability to system and network resources.
Discovery	(T1518.001) Software Discovery: Security Software Discovery	Adversaries could attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment.
Discovery	(T1012) Query Registry	Adversaries could interact with the Windows Registry to gather information about the system, configuration, and installed software.

Operational Hunting Workflows

The CyberProof Threat Hunting team worked collaboratively with the CTI team to import the external sources of information that the hunt was based on, as described below. We categorized the hunt according to the type of platform in which the indicators need to be verified - either the SIEM platform or the EDR platform.

Hunting Via the SIEM Platform

(Relevant Data Sources: Windows Security Logs)

- Hunt for event ID 4624 (lateral movement between workstations)
    - Where process name = ”NtLmSsp”
    - Where process name = ”seclogo”
- Hunt for process injection using the CreateRemoteThread API call with `Event ID 8` for the following processes:
    - svchost.exe
    - taskhostw.exe
    - winlogon.exe
    - explorer.exe
    - dllhost.exe
    - cmd.exe

  - SecurityHealthSystray.exe
  - rundll32.exe
- Hunt for dumping credentials out of LSASS memory across the domain:
  - In security event logs `Event ID 4663` and `Event ID 4656.`
  - If the Sysmon is configured `Event ID 10.`
- Hunt for installing new service of WinSCP in the system with `Event ID 7045.`
- Hunt for initiated RDP connections with `Event ID 4624.`
- Malicious network communications:
  - Hunt in firewall logs and in the proxy logs for communication to the following malicious IP addresses:
    - 34.219.130[.]241:443
    - 13.56.161[.]214:443
    - 162.244.83[.]216
    - 31.14.40[.]160 over port 22
  - Hunt in proxy logs for outbound network activity to the malicious domain Sammitng[.]com.

Hunting Via the EDR Platform

- Hunt for the execution of:
  - svchost.exe executes rundll32.exe.
- Hunt for svchost.exe, which performs SMB scanning across the environment over port 445 and 135.
- Hunt for usage of the following discovery command lines:
  - nltest /domain_trusts /all_trusts
  - net localgroup "administrator"
  - net group "domain admins" /dom
  - net1 group "domain admins" /dom
  - cmd.exe /C systeminfo
  - /C ping DOMAINCONTROLLER
  - /C ping ENDPOINT
  - cmd.exe /C net localgroup Administrators
  - C:\Windows\System32\Taskmgr.exe
  - cmd.exe /C time

- Hunt for an encoded PowerShell command that executes from the domain controller:

```
powershell -nop -exec bypass -EncodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUA
bgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8A
MQAyADcALgAwAC4AMAAuADEAOgAyADQANgAxAC8AJwApADsAIABHAGUAdAAtAFcAbQBpAE8A
YgBqAGUAYwB0ACAALQBDAGwAYQBzAIAB3AGkAbgAzADIAXwBsAZwBpAGMAYQBsAaQBzAGsAI
AAtAEMAbwBtAHAAdQB0AGUAcgBOAGEAbQBlACAARQB4AHQAZQByAG4AYQBsAFMAZQByAHYAM
wAgAHwAIABTAGUAbABlAGMAdAAtAE8AYgBqAGUAYwB0ACAAcABzAGMAbwBtAHAAdQB0AGUAc
gBuAGEAbQBlACwAIABOAGEAbQBlACwAIABAAHsAbgA9ACIAUwBwAGEAYwBlACIAOwBlAD0Ae
wBbAG0AYQB0AGgAXQA6ADoAUgBvAHUAbgBkACgAJABfAC4AUwBpAHoAZQAvADEARwBCACwAM
gApAH0AfQAsACAAQAB7AG4APQAiAEYAcgBlAGUAUwBwAGEAYwBlACIAOwBlAD0AewBbAG0AY
QB0AGgAXQA6ADoAUgBvAHUAbgBkACgAJABfAC4ARgByAGUAZQBTAHAAYQBjAGUALwAxAEcAQ
gAsADIAKQB9AH0ALAAgAEAAewBuAD0AIgBCAFUAUwBZACIAOwBlAD0AewBbAG0AYQB0AGgAX
QA6ADoAUgBvAHUAbgBkACgAKAAkAF8ALgBTAGkAegBlAC0AJABfAC4ARgByAGUAZQBTAHAAY
QBjAGUAKQAvADEARwBCACwAMgApAH0AfQA=
```

- Hunt for the decoded Powershell command line:

```
IEX (New-Object
Net.Webclient).DownloadString('http://127.0.0.1:33242/'); Get-WmiObject
-Class win32_logicalDisk -ComputerName SYSTEMNAME | Select-Object
pscomputername, Name, @{n="Space";e={[math]::Round($_.Size/1GB,2)}},
@{n="FreeSpace";e={[math]::Round($_.FreeSpace/1GB,2)}},
@{n="BUSY";e={[math]::Round(($_.Size-$_.FreeSpace)/1GB,2)}}
```

- Hunt for the Powersploit module execution Get-NetComputer by the domain controller.

```
IEX (New-Object
Net.Webclient).DownloadString('http://127.0.0.1:36595/'); Get-
NetComputer -ping -operatingsystem *server*
```

- Hunt for the creation or execution of the following filenames:
  - start.bat.
  - Get-DataInfo.ps1
  - 7A86.dll
  - backup.exe
  - 3.exe
  - 162.244.83.216-cs.exe
- Hunt for the import of the Microsoft Active Directory PowerShell module:

```
Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name,
DNSHostName, OperatingSystem, LastLogonDate | Export-CSV
C:\Users\AllWindows.csv -NoTypeInformation -Encoding UTF8
```

- Hunt for network communication with the following malicious IP addresses:

  - 34.219.130[.]241:443
  - 13.56.161[.]214:443
  - 162.244.83[.]216
- Hunt for communication to the following malicious domain:
  - Sammitng[.]com
- Hunt for the execution of WMI:

```
C:\Windows\system32\cmd.exe /C wmic /node:"DOMAINCONTROLLER" process call create "C:\3.exe"
```

```
C:\Windows\system32\cmd.exe /C wmic /node:"ENDPOINT" process call create "C:\test.exe"
```

- Hunt for the WinSCP download:
  - Execution of WinSCP-5.19.1-Setup.exe
- Hunt for malicious communication from WinSCP:
  - IP address 31.14.40[.]160 over port 22

Mitigation

- Consider monitoring a custom Cobalt Strike C2 profile from the web access log. Additional information can be found in this repository.
- Monitor for internal scanning on ports 445 and 135 (SMB and DCE/RPC).
- Implement the relevant IOCs in your security systems.

Yara Rule

```
Conti_1 {
  meta:
    description = "Files - file start.bat"
    author = "The DFIR Report"
    reference = "https://thedfirreport.com"
    date = "2021-08-30"
    hash1 = "63de40c7382bbfe7639f51262544a3a62d0270d259e3423e24415c370dd77a60"
  strings:
    $x1 = "powershell.exe Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process -Force" fullword
ascii
    $x2 = "powershell.exe -executionpolicy remotesigned -File .\\Get-DataInfo.ps1 %method" fullword
ascii
    $x3 = "powershell.exe -executionpolicy remotesigned -File .\\Get-DataInfo.ps1 %1)" fullword ascii
    $s4 = "set /p method=\"Press Enter for collect [all]:  \"" fullword ascii
    $s5 = "echo \"Please select a type of info collected:\"" fullword ascii
    $s6 = "echo \"all ping disk soft noping nocompress\"" fullword ascii
  condition:
    filesize < 1KB and all of them
}
```

```
Conti_2{
  meta:
    description = "Files - file
24f692b4ee982a145abf12c5c99079cfbc39e40bd64a3c07defaf36c7f75c7a9.exe"
    author = "The DFIR Report"
    reference = "https://thedfirreport.com"
    date = "2021-08-30"
    hash1 = "24f692b4ee982a145abf12c5c99079cfbc39e40bd64a3c07defaf36c7f75c7a9"
  strings:
    $s1 = "fbtwmjnrrovmd.dll" fullword ascii
    $s2 = "AppPolicyGetProcessTerminationMethod" fullword ascii
    $s3 = " Type Descriptor'" fullword ascii
    $s4 = "operator co_await" fullword ascii
  condition:
    uint16(0) == 0x5a4d and filesize < 900KB and all of them
}
```

```
Conti_3 {
  meta:
    description = "Files - file 3.exe"
    author = "The DFIR Report"
    reference = "https://thedfirreport.com"
    date = "2021-08-30"
    hash1 = "37b264e165e139c3071eb1d4f9594811f6b983d8f4b7ef1fe56ebf3d1f35ac89"
  strings:
    $s1 = "https://sectigo.com/CPS0" fullword ascii
    $s2 = "?http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl0v" fullword ascii
    $s3 = "2http://crl.comodoca.com/AAACertificateServices.crl04" fullword ascii
    $s4 = "3http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt0%" fullword ascii
    $s5 = "       <requestedExecutionLevel level=\"asInvoker\"/>" fullword ascii
    $s6 = "http://ocsp.sectigo.com0" fullword ascii
    $s7 = "2http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#" fullword ascii
    $s8 = "2http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s" fullword ascii
    $s9 = "ealagi@aol.com0" fullword ascii
    $s10 = "bhfatmxx" fullword ascii
    $s11 = "orzynoxl" fullword ascii
    $s12 = "  <trustInfo xmlns=\"urn:schemas-microsoft-com:asm.v3\">" fullword ascii
    $s13 = "     <!--The ID below indicates application support for Windows 8.1 -->" fullword ascii
    $s14 = "     <!--The ID below indicates application support for Windows 8 -->" fullword ascii
    $s15 = "O:\\-e%" fullword ascii
    $s16 = "     <!--The ID below indicates application support for Windows 10 -->" fullword ascii
    $s17 = "     <!--The ID below indicates application support for Windows 7 -->" fullword ascii
    $s18 = "     <!--The ID below indicates application support for Windows Vista -->" fullword ascii
    $s19 = "  <compatibility xmlns=\"urn:schemas-microsoft-com:compatibility.v1\">" fullword ascii
    $s20 = "  </compatibility>" fullword ascii
  condition:
    uint16(0) == 0x5a4d and filesize < 1000KB and 8 of them }
```

```
Conti_4 {
  meta:
    description = "Files - file 7A86.dll"
    author = "The DFIR Report"
    reference = "https://thedfirreport.com"
    date = "2021-08-30"
    hash1 = "9d63a34f83588e208cbd877ba4934d411d5273f64c98a43e56f8e7a45078275d"
  strings:
    $s1 = "ibrndbiclw.dll" fullword ascii
    $s2 = "AppPolicyGetProcessTerminationMethod" fullword ascii
    $s3 = "Type Descriptor'" fullword ascii
    $s4 = "operator co_await" fullword ascii
  condition:
    uint16(0) == 0x5a4d and filesize < 500KB and all of them }
```

Appendix: IOC Types

IOC Type	Event Source	Query Timeframes
IP Address	Firewall Traffic Firewall Threat Protection DNS Queries Proxy Queries Authentication Logs EDR Logs	30-60 Days
Domain	DNS Queries Proxy Queries EDR Logs	30-60 Days
URL	Firewall Threat Protection DNS Queries Proxy Queries EDR Logs	30-60 Days
HASH (MD5, SHA1, SHA265)	Firewall Threat Protection Email Threat Protection EDR Logs Anti-Virus Logs	30-60 Days
Email Address	Email Gateway Email Threat Protection Authentication Logs	30-90 Days

References

https://news.sophos.com/en-us/2021/07/22/hivenightmare-aka-serioussam-vulnerability-what-to-do/

https://nakedsecurity.sophos.com/2021/07/21/windows-hivenightmare-bug-could-leak-passwords-heres-what-to-do/

https://us-cert.cisa.gov/ncas/alerts/aa21-265a

https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/