

←

Post

Br3akp0int
@tccontre18

...

For past few mons. I've encountered several .dll malware using regsvr32 /install or /silent for its execution. And while @M_haggis and I burning some detection dev, we found out that you can run regsv32 parameter in several ways. 🤔 ??? 1/3

s\Public>regsvr32.exe /i ../AllTheThingsx64.dll

s\Public>

th trigger install

svr32 parameter

RegSvr32

OK

s\Users\Public>

All of this parameter trigger silent parameter of regsvr32

C:\Users\Public>regsvr32.exe /i AllTheThingsx64.dll

C:\Users\Public>

RegSvr32

OK

s\Public>regsvr32.exe /impossible ../AllTheThings

s\Public>

RegSvr32

OK

Usage: regsvr32 [/u] [/s] [/n] [/i] [cmdline]] dllname

default- Register server calling DllRegisterServer.

/u - Unregister server calling DllUnregisterServer.

/s - Silent; display no message boxes.

/i - Used without /u, calls DllInstall(TRUE, [cmdline]) to install the dll, after a successful call to DllRegisterServer. Used with /u, calls DllInstall(FALSE, [cmdline]) to uninstall the dll and DllUnregisterServer if DllInstall was successful.

/n - Do not call DllRegisterServer or DllUnregisterServer; this option must be used with /i.

dllname - The path (absolute or relative) to the DLL to call the entry points on. This DLL is required to export the entry points

6:13 PM · Jan 11, 2022

119 Reposts

6 Quotes

355 Likes

55 Bookmarks

💬

↺↻

❤️

🔖 55

📤

New to X?

Sign up now to get your own personalized timeline!

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#).

Something went wrong. Try reloading.

Retry

[Terms of Service](#) [Privacy Policy](#) [Cookie Policy](#)
[Accessibility](#) [Ads info](#) [More ...](#) © 2024 X Corp.

Don't miss what's happening
People on X are the first to know.

Log inSign up

Welcome to x.com!

We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.
For more details, see our Privacy Policy: <https://x.com/en/privacy>.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies

Page 1 of 1