Create DeviceCredentialDeployment.yml #147

New issue

Merged **xenoscr** merged 3 commits into `LOLBAS-Project:master` from `ElliotKillick:DeviceCredentialDeployment` on Sep 17, 2022

Conversation 4 Commits 3 Checks 0 Files changed 1 +20 −0

ElliotKillick commented on Aug 17, 2021 • edited Contributor

New lolbin for hiding a console window (e.g. cmd.exe). First one that doesn't require PowerShell or VBS/JScript to my knowledge: DeviceCredentialDeployment.exe

`Create DeviceCredentialDeployment.yml` Verified `d521284`

ElliotKillick commented on Aug 28, 2021 Contributor Author

This is my favourite of all the lolbins I found because it perfectly solves a problem I (as well as I've seen many others) have with LNK scripts whereby the CMD prompt has to stay open and minimized to the taskbar while the payload is downloading. Now with this lolbin the window goes straight from minimized to hidden so fast that you don't even see the CMD logo popup in the taskbar!

And all without PowerShell, which may be disabled in "high security" environments among many other benefits of not requiring it.

api0cradle commented on Oct 22, 2021 Contributor

Sweet find Elliot!
Do you have some more input on how to use it?

Note2Self: Needs to be adjusted in terms of category

ElliotKillick commented on Nov 25, 2021 Contributor Author

Yes, generally there are a lot of possible use cases where hiding the CMD console window would be beneficial. One other I can think of is any situation where an upload lolbin is involved. Generally, if you're using an upload lolbin to exfiltrate data it's going to take a while to upload all of it (especially if you have to wait to zip it all up first) and having the process run in the background can make or break the attack.

xenoscr added 2 commits 2 years ago

`Removing extra document start "---" and updating category to Conceal.` Verified `1e6d6d2`

`Removing invalid MiterLink key.` Verified `7dd6ca2`

xenoscr merged commit `f5c797a` into `LOLBAS-Project:master` on Sep 17, 2022

xenoscr commented on Sep 17, 2022 Contributor

Reviewers
No reviews

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
Successfully merging this pull request may close these issues.
None yet

3 participants

Thank you **@ElliotKillick** for your addition to the LOLBas!