Hacking AppLocker Cache

Grzegorz Tworek

Agenda

- AppLocker
- All animals are equal, but some animals are more equal than others.
- If everything seems under control, you're not going fast enough.

https://newsglobal24.com/funny-and-confusing-road-signs/

AppLocker

- Components
  - Management
    - GUI
    - PowerShell
  - AppIdSvc
  - Kernel driver (appid.sys)
  - Logging
- Enforcement
  - Path
  - Hash
  - Signature

https://www.goldcoastbulletin.com.au/funny-road-signs-from-around-the-world/news-story/5cf7e7bf0e8a8db6230bc47704d560c

Demo #1

All animals are equal, but some animals are more equal than others.

https://mobile.twitter.com/LionMountain_TV/status/1468143443868278785

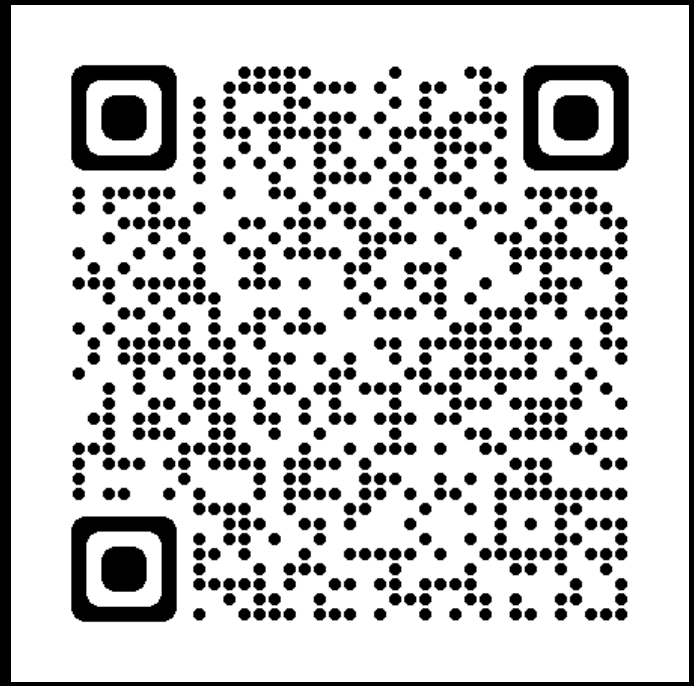
Demo #2

If everything seems under control, you're not going fast enough.

http://yesheydorji.blogspot.com/2012/04/funny-signboards-i-just-returned-from.html

Resources

- https://github.com/gtworek/PSBits/tree/master/AppLockerBypass
- https://github.com/gtworek/PSBits/tree/master/CopyEAs
- https://gtworek.github.io/PSBits/applockercachebypass.html
- https://youtu.be/587PDVQACGg



https://stderr.pl/a77a28298ba84c239d7c78b4f49d9d51.htm