R2CON 2020

Workshop: Semi-automatic Code Deobfuscation

Tim Blazytko
`@mr_phrazer`
`tim@blazytko.to`
`https://synthesis.to`

Personal Details

reverse engineer, trainer, security researcher and former PhD student

- **trainings:** reverse engineering and software deobfuscation
- **research:** code deobfuscation, fuzzing and root cause analysis
- **full-time:** design and evaluation of obfuscation techniques at *emproof GmbH*

Live Coding: Automatic Detection and Removal of Opaque Predicates

- opaque predicates in `X-Tunnel` (APT128 malware)
- symbolic execution
- SMT solver
- identification of opaque predicates
- removing/patching opaque predicates

Slides and Code after the Stream

`https://github.com/mrphrazer/r2con2020_deobfuscation`