SILENTTRINITY

BLACK HILLS
Information Security
• 2008 •

Agenda

- Quick recap of the BYOI concept which underpins SILENTTRINITY
- All things SILENTTRINITY!
  - Setup, Navigating the CLI, Sessions, Modules etc…
  - All the Updates
  - Demo
  - Writing your own modules
    - Undocumented features that make your life easier
  - Easily port existing C# tradecraft with this one easy trick!
- Q/A

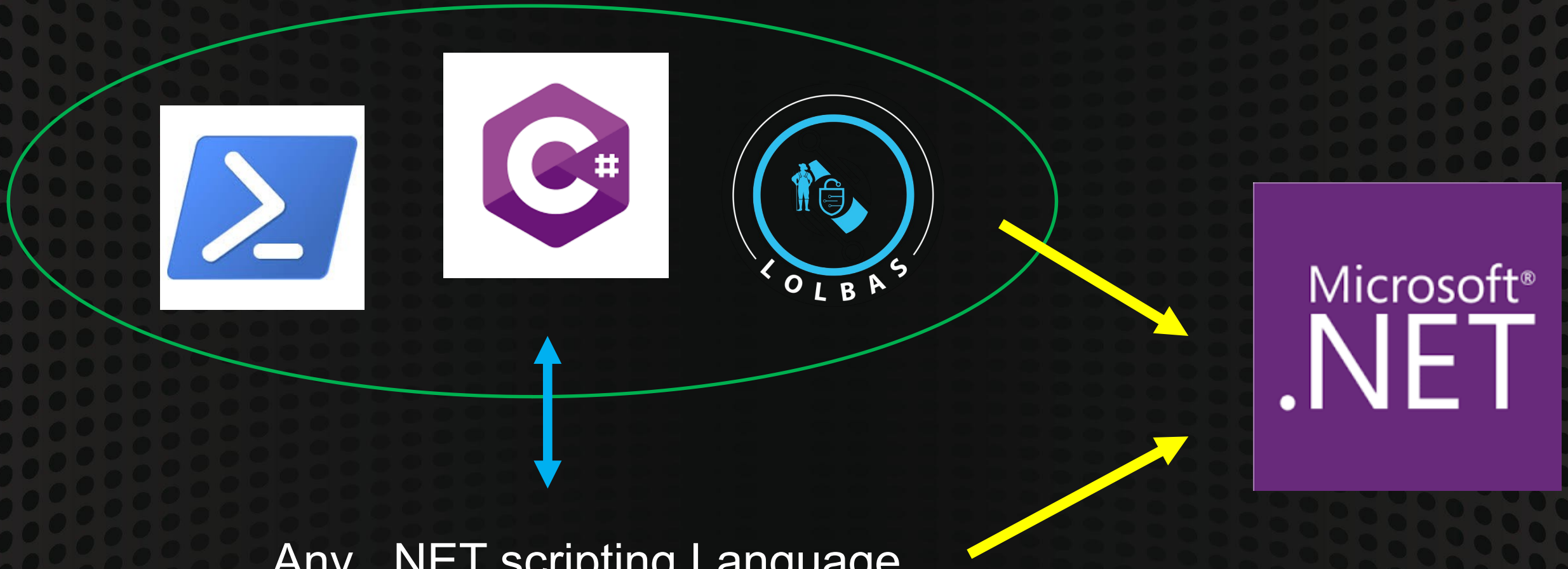
Links

- SILENTTRINITY
  - https://github.com/byt3bl33d3r/SILENTTRINITY
- OffensiveDLR
  - https://github.com/byt3bl33d3r/OffensiveDLR

BYOI Payloads

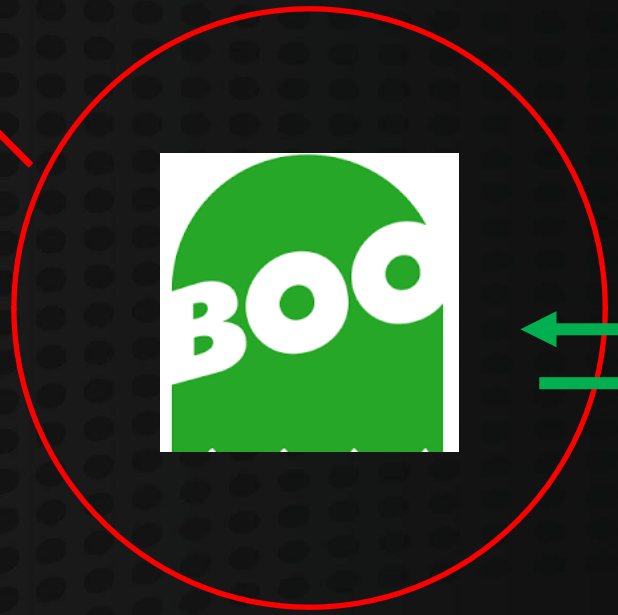
- Bring Your Own Interpreter
  - Embed scripting languages into your .NET payloads!
  - Another webcast I did a while covering the topic in more depth
    - https://www.youtube.com/watch?v=IGMj9paeEWM
  - DerbyCon Talk:
    - https://www.youtube.com/watch?v=o6m6_TncrcI

BYOI Payloads

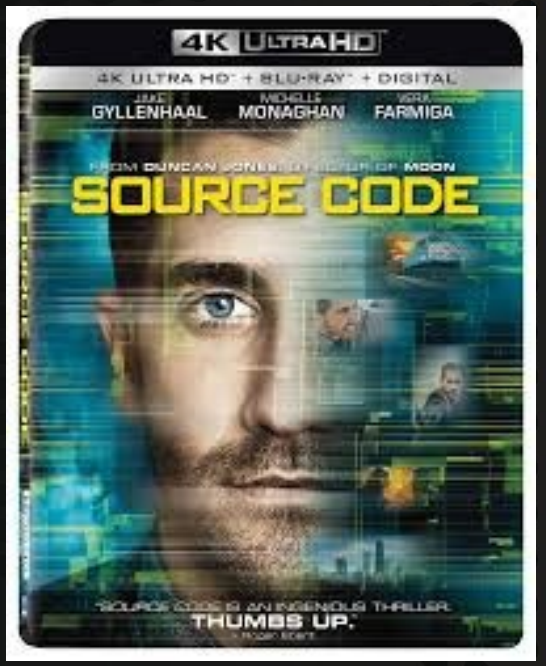


BYOI Payloads/SILENTTRINITY In a Nutshell

Any .NET Language or LOLbin/feature that ingests a .NET assembly!



C2 Channel



Pros & Cons

- Pros
  - PowerShell style-like attacks without PowerShell!
  - Not limited to a single language!
  - No compilation, everything is source code, everything is dynamic
  - By design, Anti-RE
    - If you decompile the assembly, nothing inherently malicious
  - Because of the way Dynamic Languages are built in .NET, you never have to worry about AMSI if you instrument payloads correctly
- Cons
  - Embedding languages is sometimes not straight forward
  - ~~Can't take Advantage of existing C# tradecraft~~
    - Somewhat solved ! :)

SILENTTRINITY v0.4.5 (Codename: “Zanzibar”)

- Fresh off the presses
- Around 50 (!!) new modules thanks to some amazing contributions!
  - Process migration/injection
  - Lateral movement
  - UAC bypasses
  - Recon
  - Lulz

- Vastly improved error handling everywhere
- Listener revamp
- Unit tests!

BLACK HILLS
Information Security
• 2008 •

Twitter: @byt3bl33d3r (Marcello)

- SILENTTRINITY
  - https://github.com/byt3bl33d3r/SILENTTRINITY
- OffensiveDLR
  - https://github.com/byt3bl33d3r/OffensiveDLR