Demon of Sandbox's Paradise





./whoami

- 20
- @kaganisildak
- kaganisildak.com
- malware.ninja







Ne anlatacak bu?

• CVE-2019-14270



Sandbox Basics



GO GO GO





Saldırı Aşamaları

- 1. Kullan
- 2. incele
- 3. Anla
- 4. Keşfet
- 5. Sömür





Modify Sandbox
Configuration

Hollow Process

Inject Code

ESCAPE





SORULAR







