black hat®

USA 2020

AUGUST 5-6, 2020

ARSENAL

#BHUSA @BLACKHATEVENTS

Information Classification: General

Starkiller: Threat Emulation Platform for Red Teams and Penetration Testers

Anthony Cx01N Rose

@BCSECURITY1

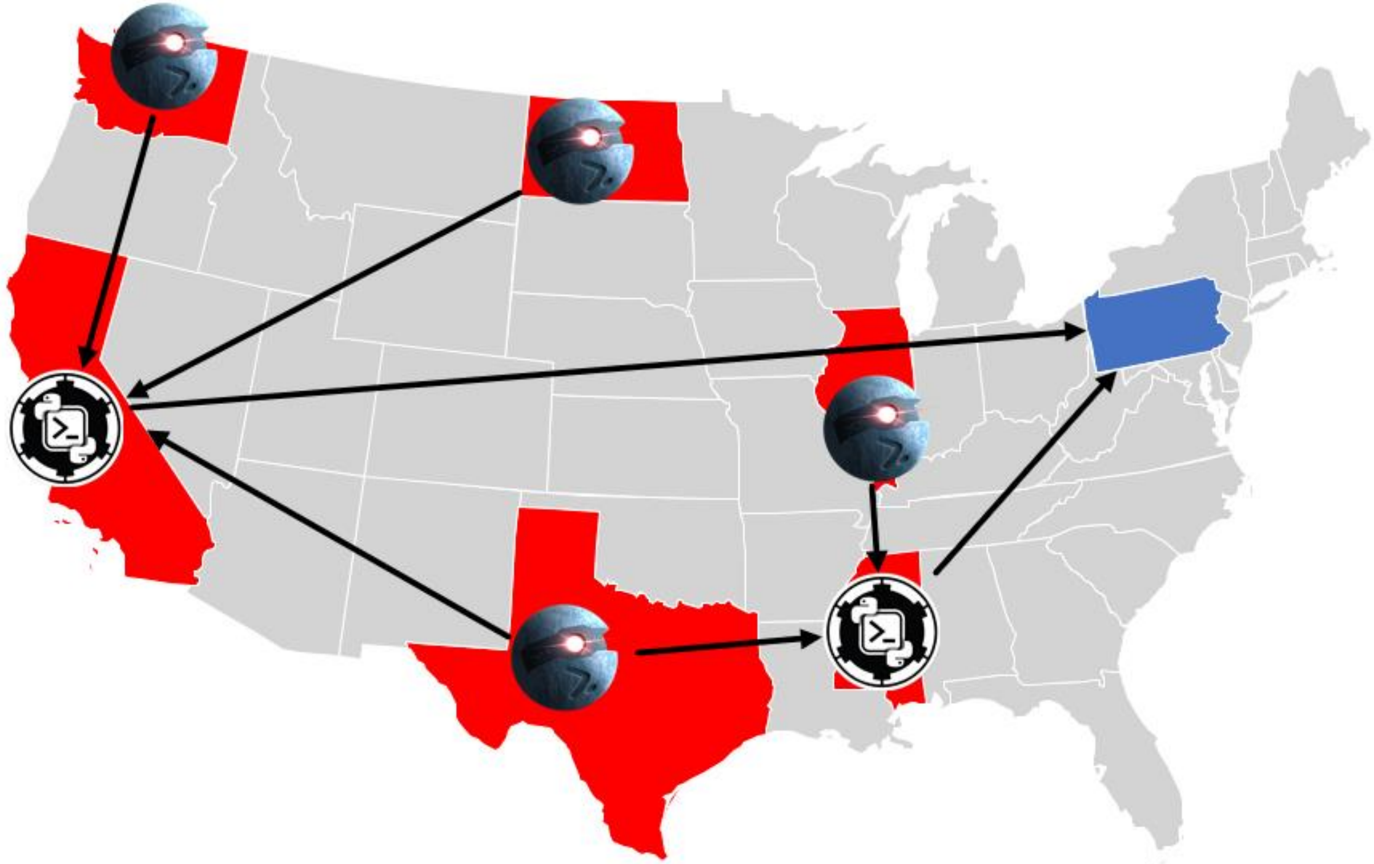
Information Classification: General

Adversary Emulation

A Red Team exercise that emulates how adversaries operate and follows similar tactics, techniques, and procedures (TTPs) to obtain a specific objective.

Red Team Infrastructure

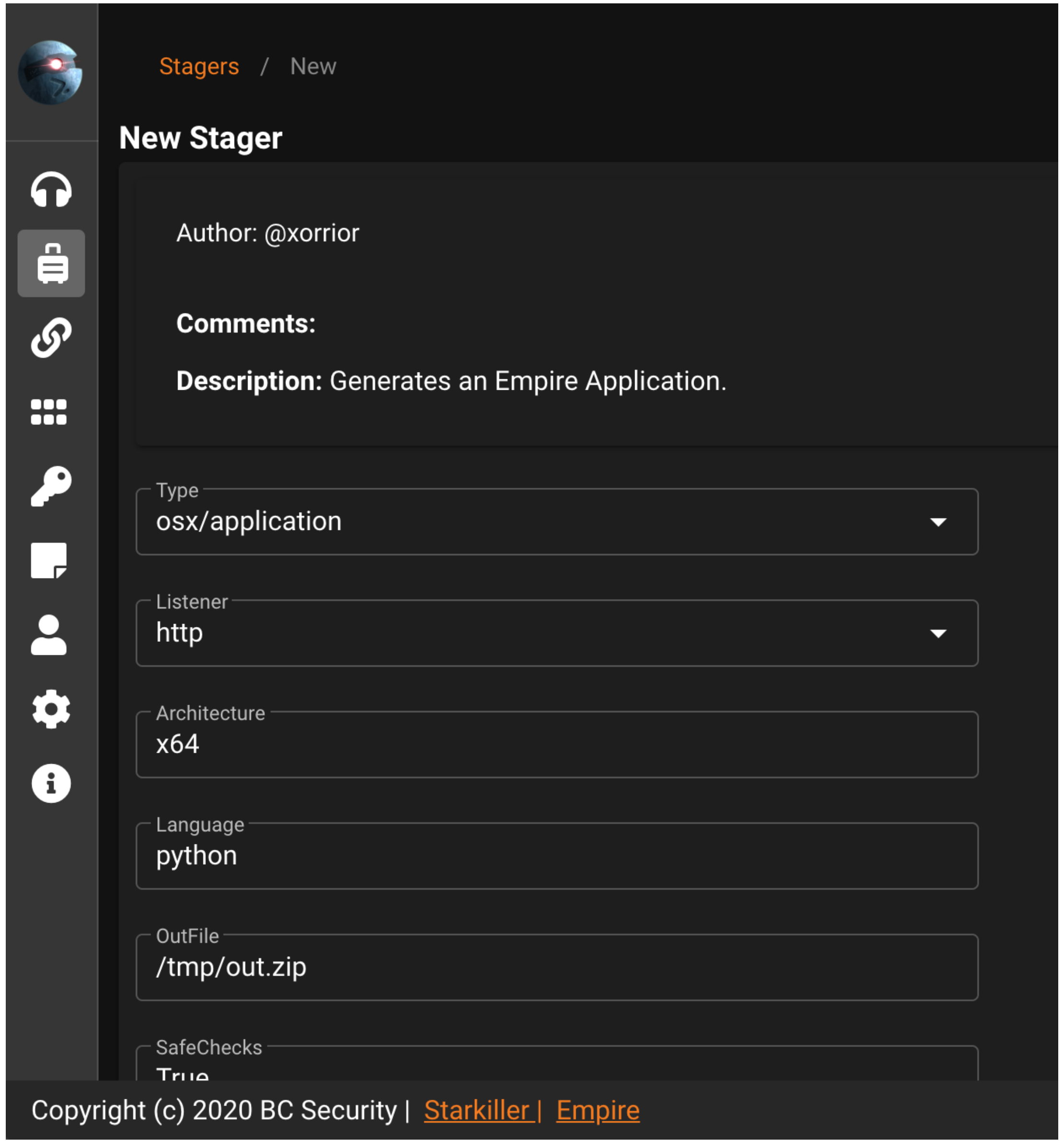
- Stage payloads, control implants, and store target data just like Advanced Persistent Threats (APTs)
- We don't want the discovery of a single domain or endpoint to compromise the whole operation
- It's how real adversaries run their operations



Information Classification: General

What is Starkiller?

- Intuitive Command and Control (C2) Interface
- Multi-User Support
- On-the-fly Reporting
- Simplified Workflows



New Stager

Author: @xorrior

Comments:

Description: Generates an Empire Application.

Type: osx/application

Listener: http

Architecture: x64

Language: python

OutFile: /tmp/out.zip

SafeChecks: True

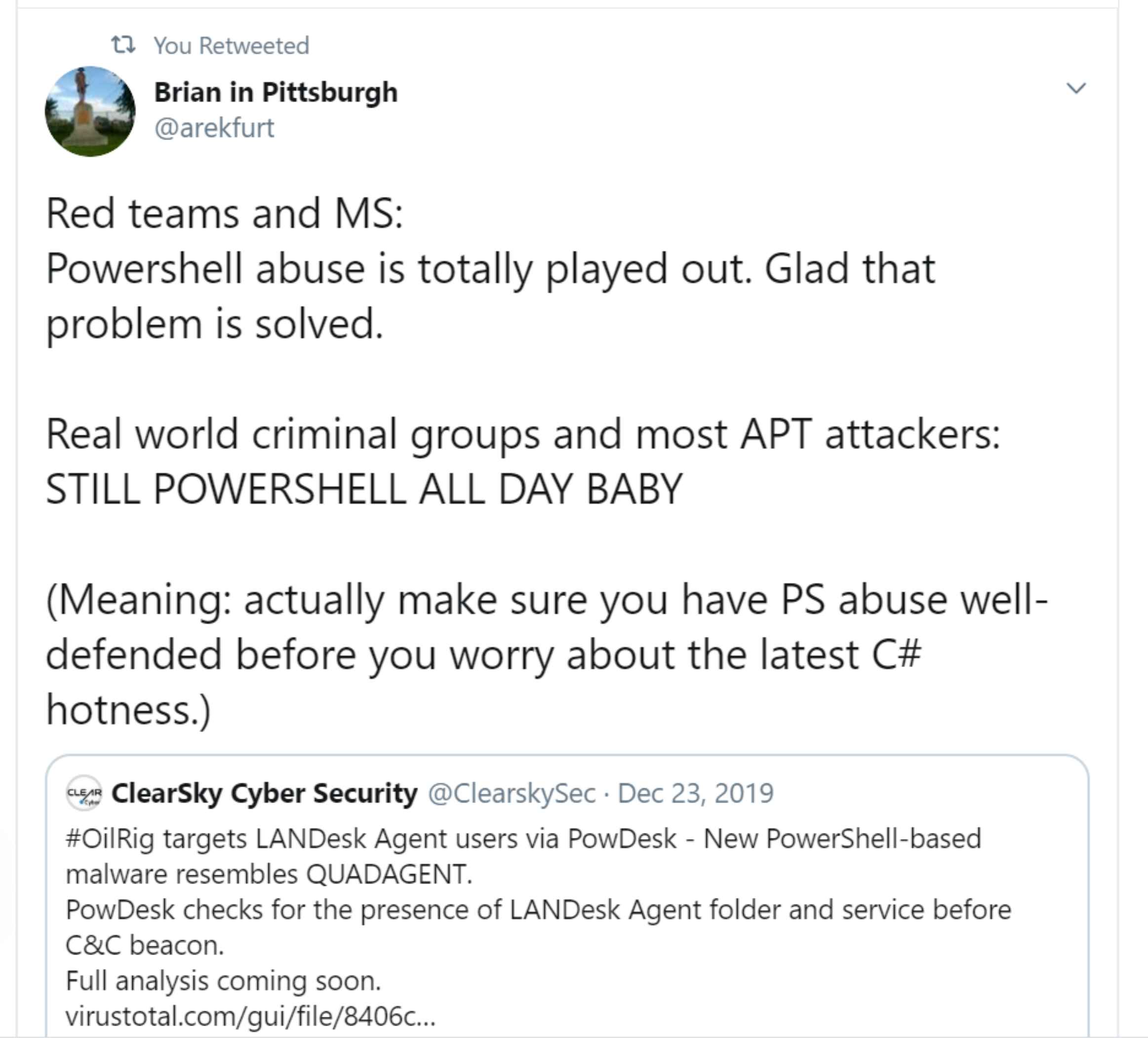
Copyright (c) 2020 BC Security | Starkiller | Empire

Empire

- Post-Exploitation Framework built around PowerShell and Python
- Can be ran as a Team Server or All-in-one C2
- Adaptive Modules
- Original project ended support in August 2019
  - Still being maintained as a Fork by us
  - https://github.com/BC-SECURITY/Empire

Why PowerShell?

- Gives Full .NET Access
- Direct access to Win32 API
- Operates in Memory
- Installed by default in Windows



You Retweeted

Brian in Pittsburgh
@arekfurt

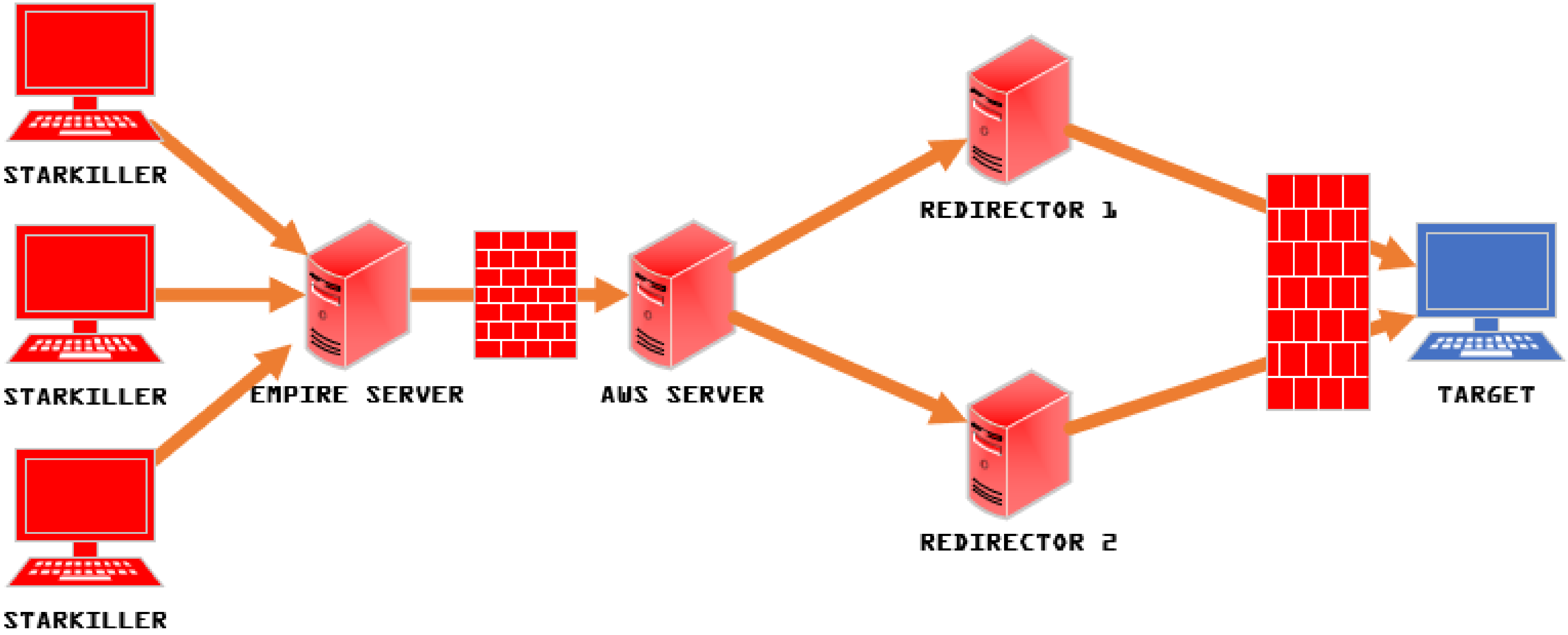
Red teams and MS:
Powershell abuse is totally played out. Glad that problem is solved.

Real world criminal groups and most APT attackers:
STILL POWERSHELL ALL DAY BABY

(Meaning: actually make sure you have PS abuse well-defended before you worry about the latest C# hotness.)

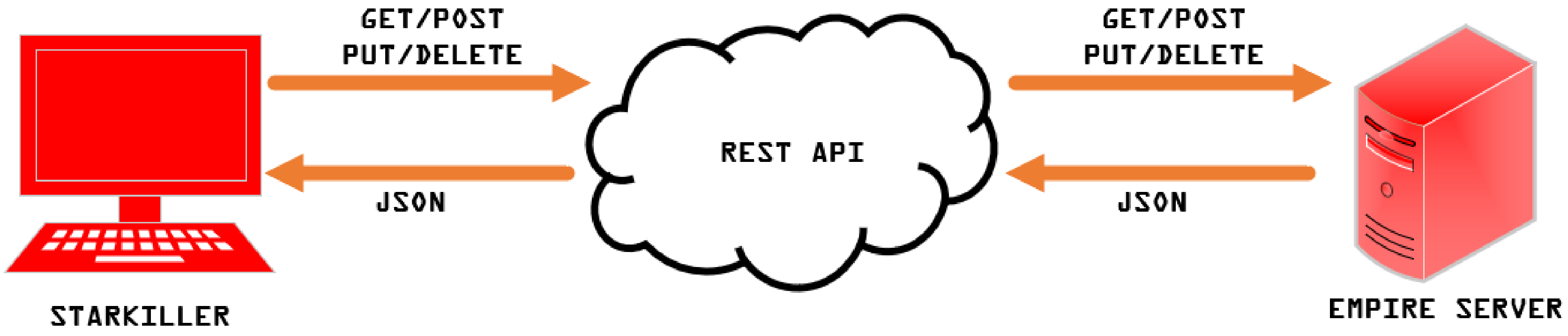
ClearSky Cyber Security @ClearskySec · Dec 23, 2019
#OilRig targets LANDesk Agent users via PowDesk - New PowerShell-based malware resembles QUADAGENT.
PowDesk checks for the presence of LANDesk Agent folder and service before C&C beacon.
Full analysis coming soon.
virustotal.com/gui/file/8406c...

Red Team Infrastructure w/Starkiller



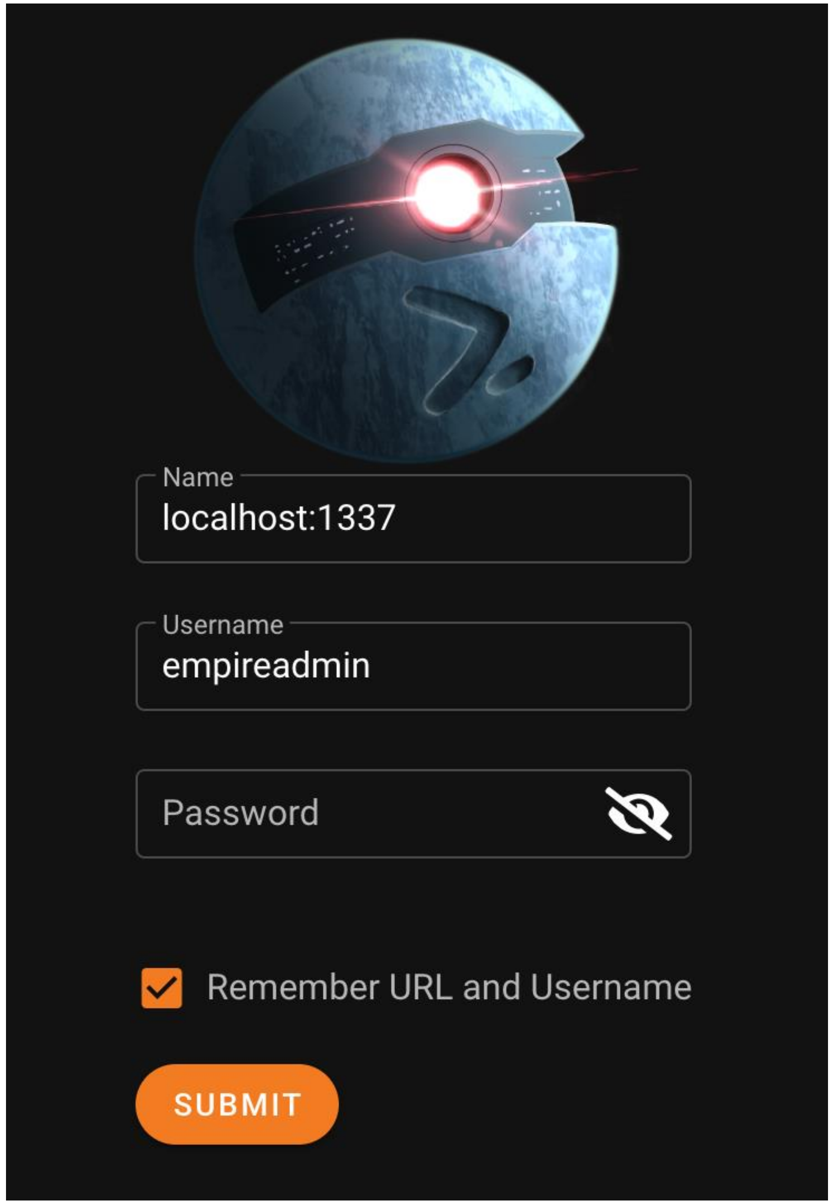
Starkiller

- Remote control of Empire (from a distance)
- Option to run solo or as a team
- Goal:
  - More efficient Red Team workflows
  - Team-oriented engagements



Starkiller Setup

- Run Empire with its API
  - ./empire --rest
- Default login
  - Username: empireadmin
  - Password: password123
- Multiplatform
  - Windows
  - MacOS
  - Linux



Name: localhost:1337

Username: empireadmin

Password

☑ Remember URL and Username

https://github.com/BC-SECURITY/Starkiller

DEMO TIME

https://github.com/BC-SECURITY/Empire

https://github.com/BC-SECURITY/Starkiller

@BCSECURITY1