

The background of the slide features a large, dark blue planet with a textured surface, resembling Starkiller from Star Wars. A large, dark, angular Death Star is positioned in the center, with a bright red laser beam emanating from its main cannon. The planet and the Death Star are set against a dark, starry space background.

Starkiller

VINCENT ROSE

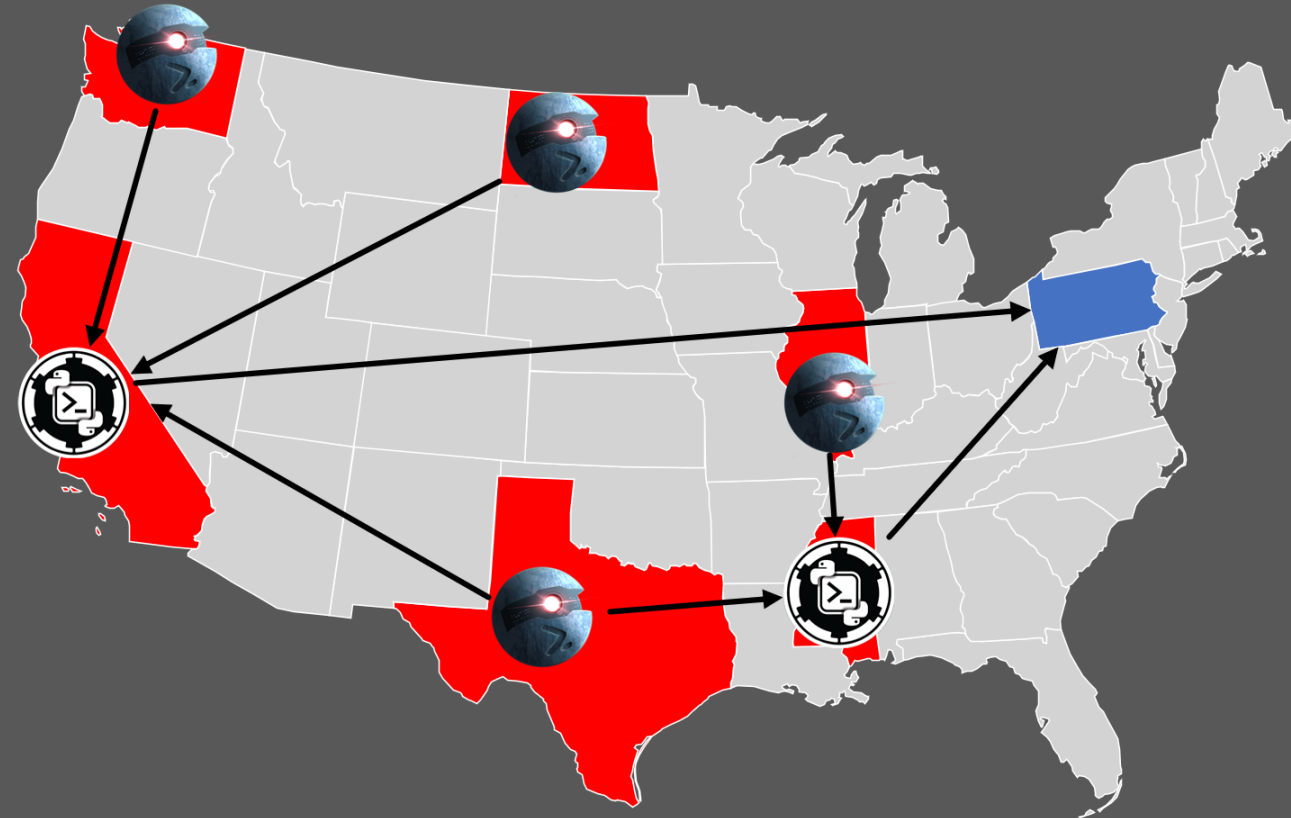
 @bcsecurity1

Adversary Emulation

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

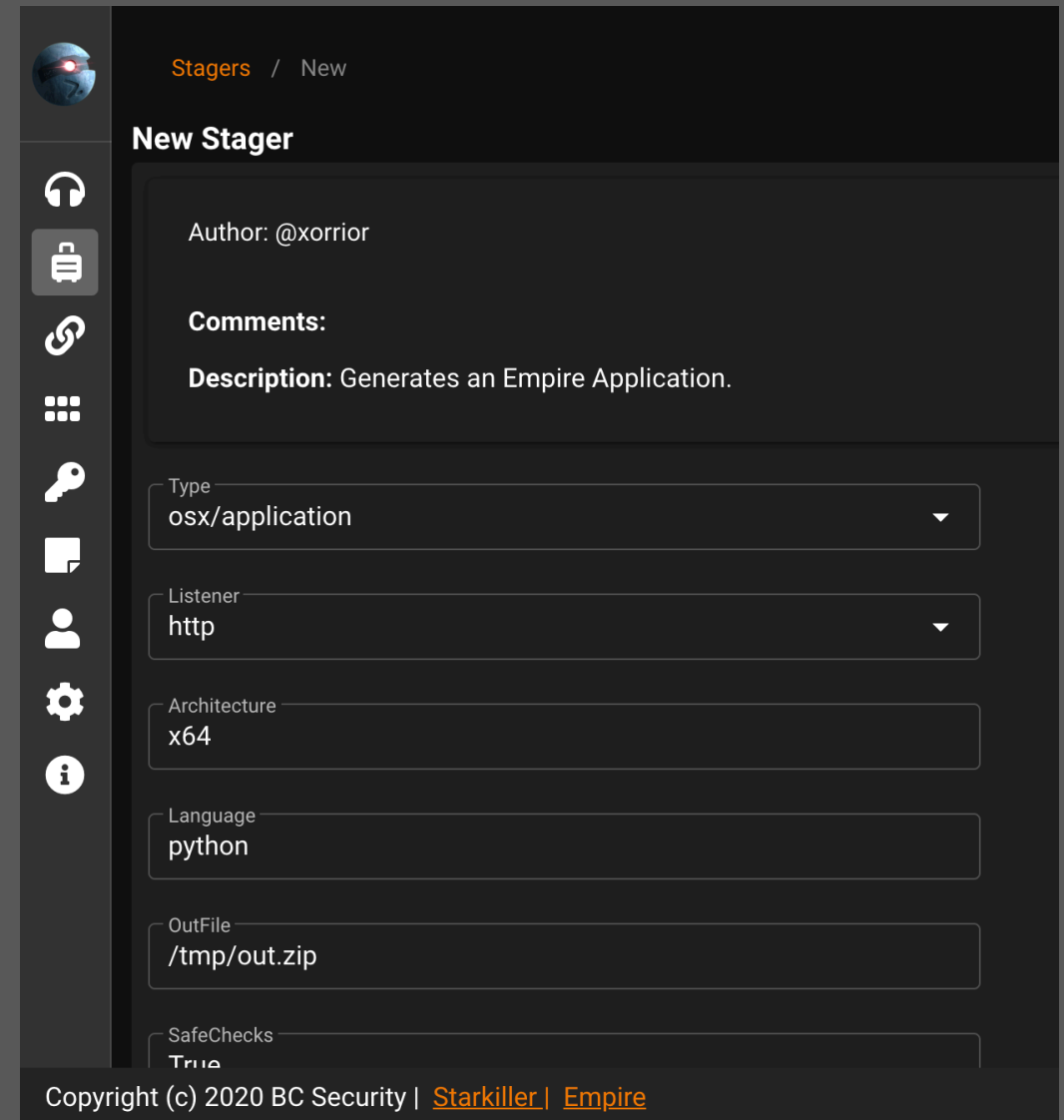
Red Team Infrastructure

- 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



What is Starkiller?

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



The screenshot displays the Starkiller web interface. On the left is a vertical sidebar with icons for a user profile, headphones, a briefcase, a link, a grid, a key, a document, a person, a gear, and an information icon. The main content area is titled 'Stagers / New' and 'New Stager'. It contains a form with the following fields: 'Author' (pre-filled with '@xorrior'), 'Comments' (empty), 'Description' (pre-filled with 'Generates an Empire Application.'), 'Type' (dropdown menu with 'osx/application' selected), 'Listener' (dropdown menu with 'http' selected), 'Architecture' (text input with 'x64'), 'Language' (text input with 'python'), 'OutFile' (text input with '/tmp/out.zip'), and 'SafeChecks' (checkbox labeled 'True'). At the bottom of the interface, a copyright notice reads '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.

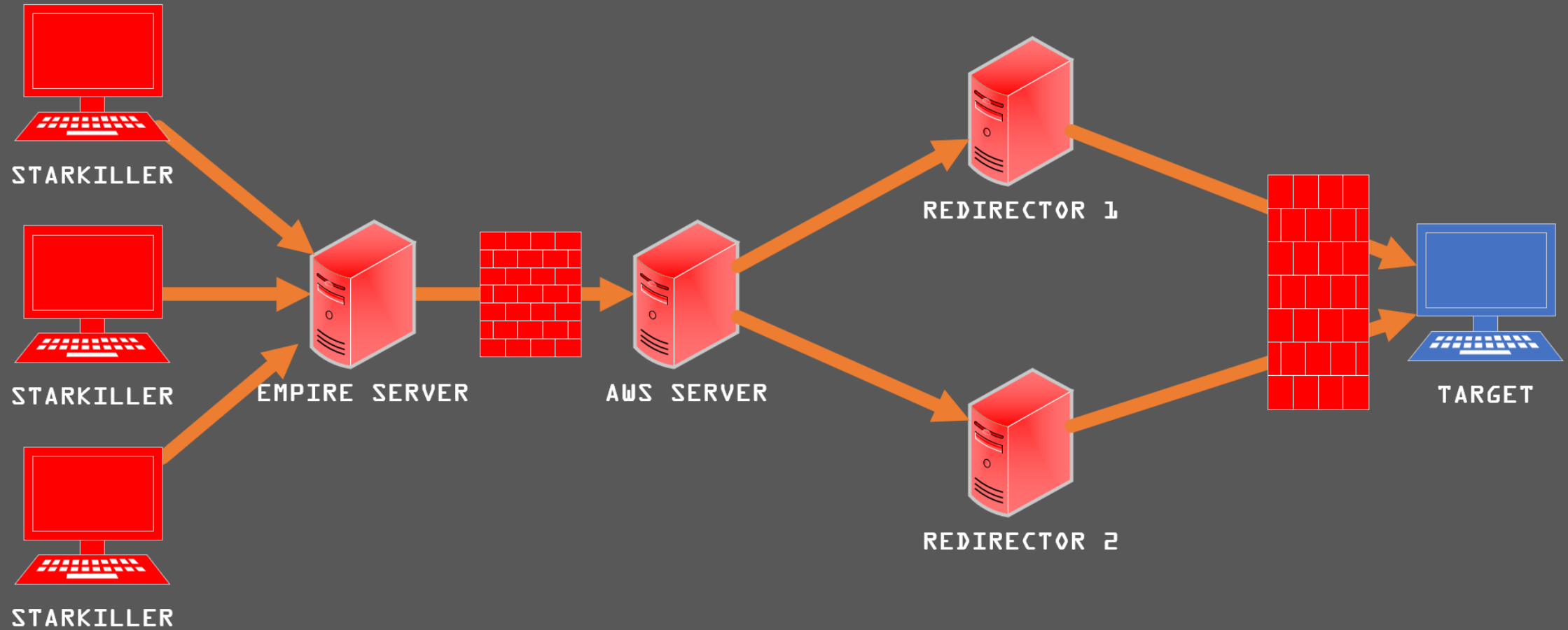
Real world criminal groups and most APT attackers:
STILL POWERSHELL ALL DAY BABY

(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

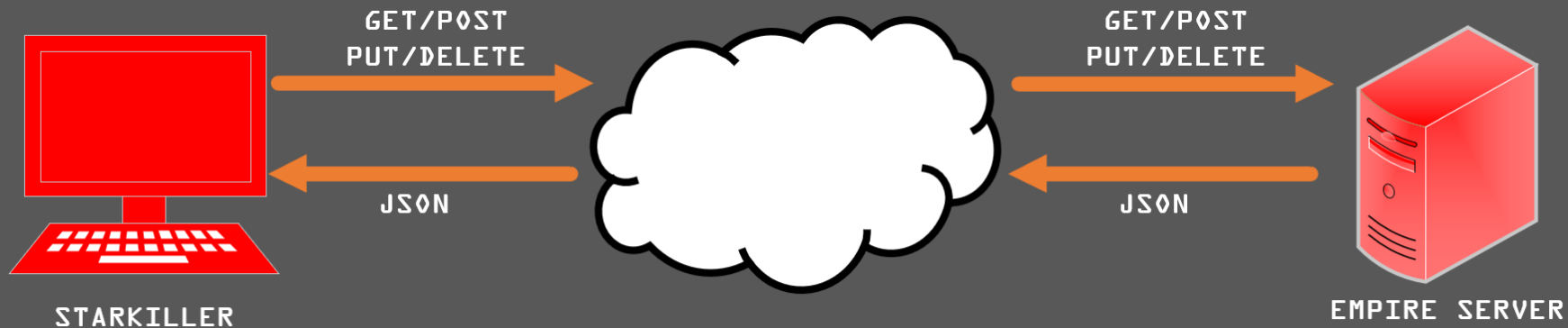
#OilRig targets LANDesk Agent users via PowDesk - New PowerShell-based malware resembles QUADAGENT.
PowDesk checks for the presence of LANDesk Agent folder and service before C&C beacon.
Full analysis coming soon.
[virustotal.com/gui/file/8406c...](https://www.virustotal.com/gui/file/8406c...)

Red Team Infrastructure w/Starkiller



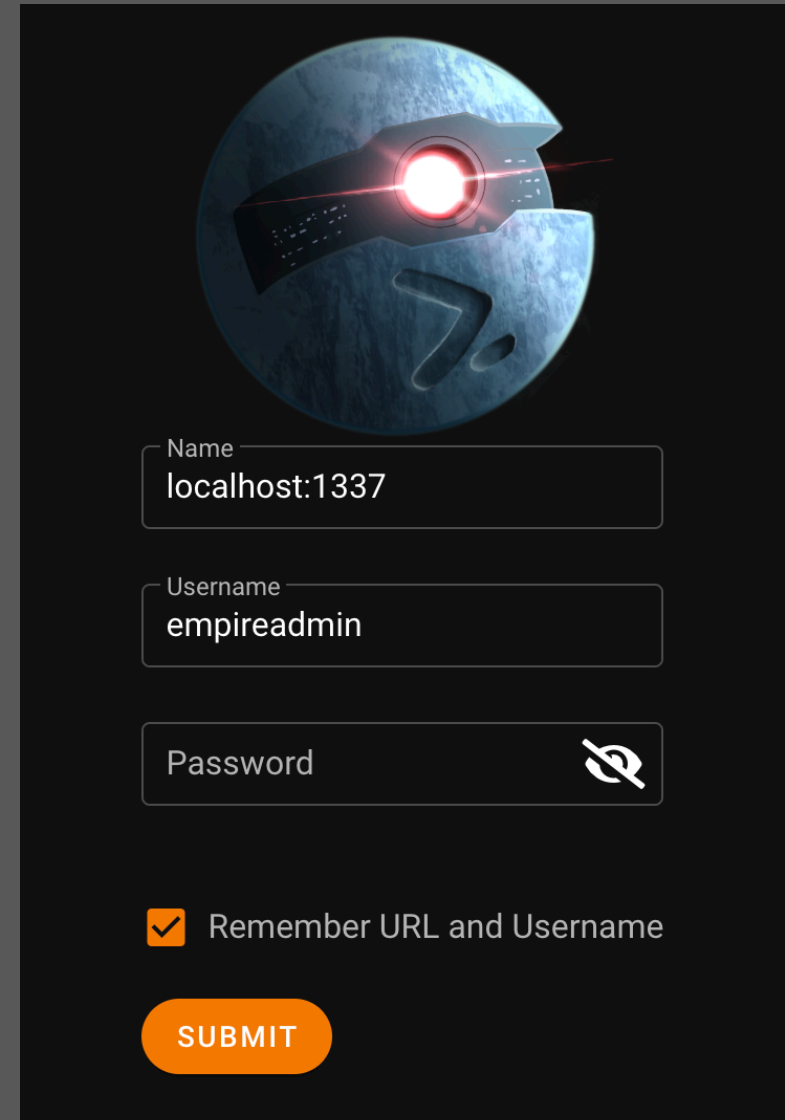
Starkiller

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



Starkiller Setup

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



The image shows the Starkiller login interface. At the top is a circular logo featuring a blue planet with a black orbital ring and a red laser beam. Below the logo are three input fields: 'Name' with the value 'localhost:1337', 'Username' with the value 'empireadmin', and 'Password' which is currently empty. To the right of the password field is an eye icon for toggling visibility. Below these fields is a checked checkbox labeled 'Remember URL and Username'. At the bottom is an orange 'SUBMIT' button.

Name
localhost:1337

Username
empireadmin

Password

☒ Remember URL and Username

SUBMIT

DEMO TIME





Questions?

INFO@BC-SECURITY.ORG

 @BCSECURITY1

[HTTPS://GITHUB.COM/BC-SECURITY/STARKILLER](https://github.com/BC-Security/STARKILLER)