Starkiller

VINCENT ROSE

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

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

https://github.com/BC-SECURITY/Starkiller
Red Team Infrastructure w/Starkiller

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

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

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

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

LET'S PRAY
TO THE DEMO GODS
Questions?

INFO@BC-SECURITY.ORG
@BCSECURITY1
HTTPS://GITHUB.COM/BC-SECURITY/STARKILLER