H2HC
HACKERS TO HACKERS CONFERENCE

Havoc C2 in Action:

Evasion and Adversary Simulation Techniques for Red Teamers

H2HC

whoami

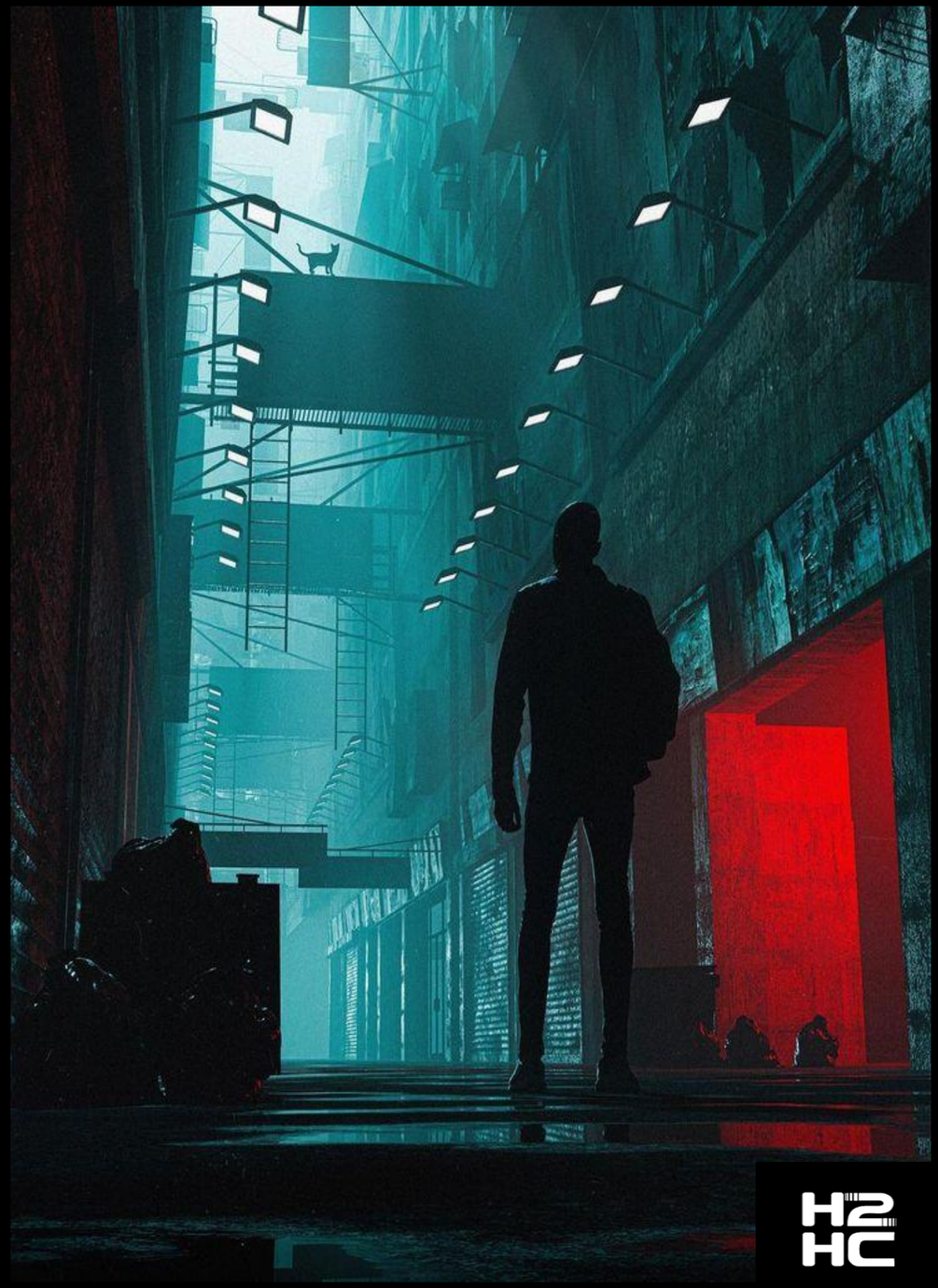
Oryon Farias “@0sfx01”

- Offensive Security Engineer at Unico IDtech
- Instructor at Gohacking EHMOB (Android/iOS)
- Graduate at cybersecurity

Agenda

- Introduction C2 Frameworks
- Why use C2 Frameworks
- Bypass Security policies
- References

Introduction



Introduction C2 frameworks

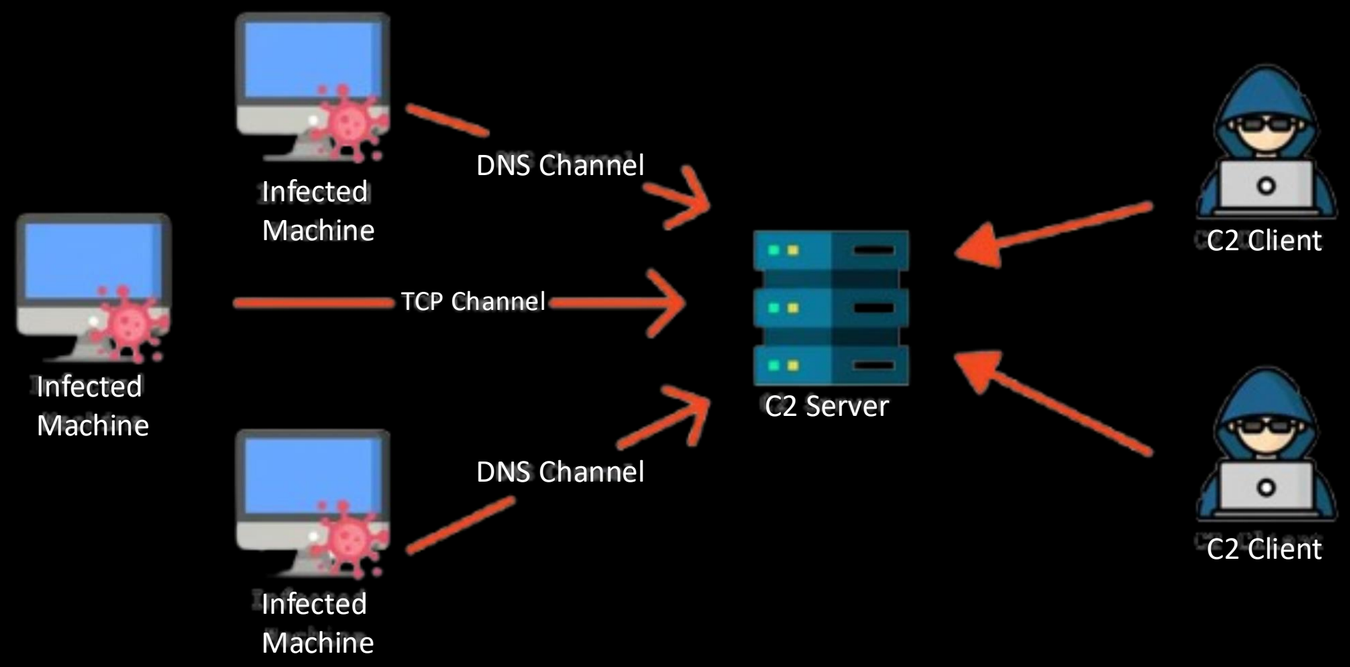
- Command and Control (C2) is a tool used to control compromised systems in simulations or real attacks.

- Allows the sending of commands, collection of information and execution of actions on targets.

- Examples:
  - Cobalt Strike;
  -Metasploit;
  - Havoc;

Introduction C2 frameworks

Command and Control (C2) - architecture

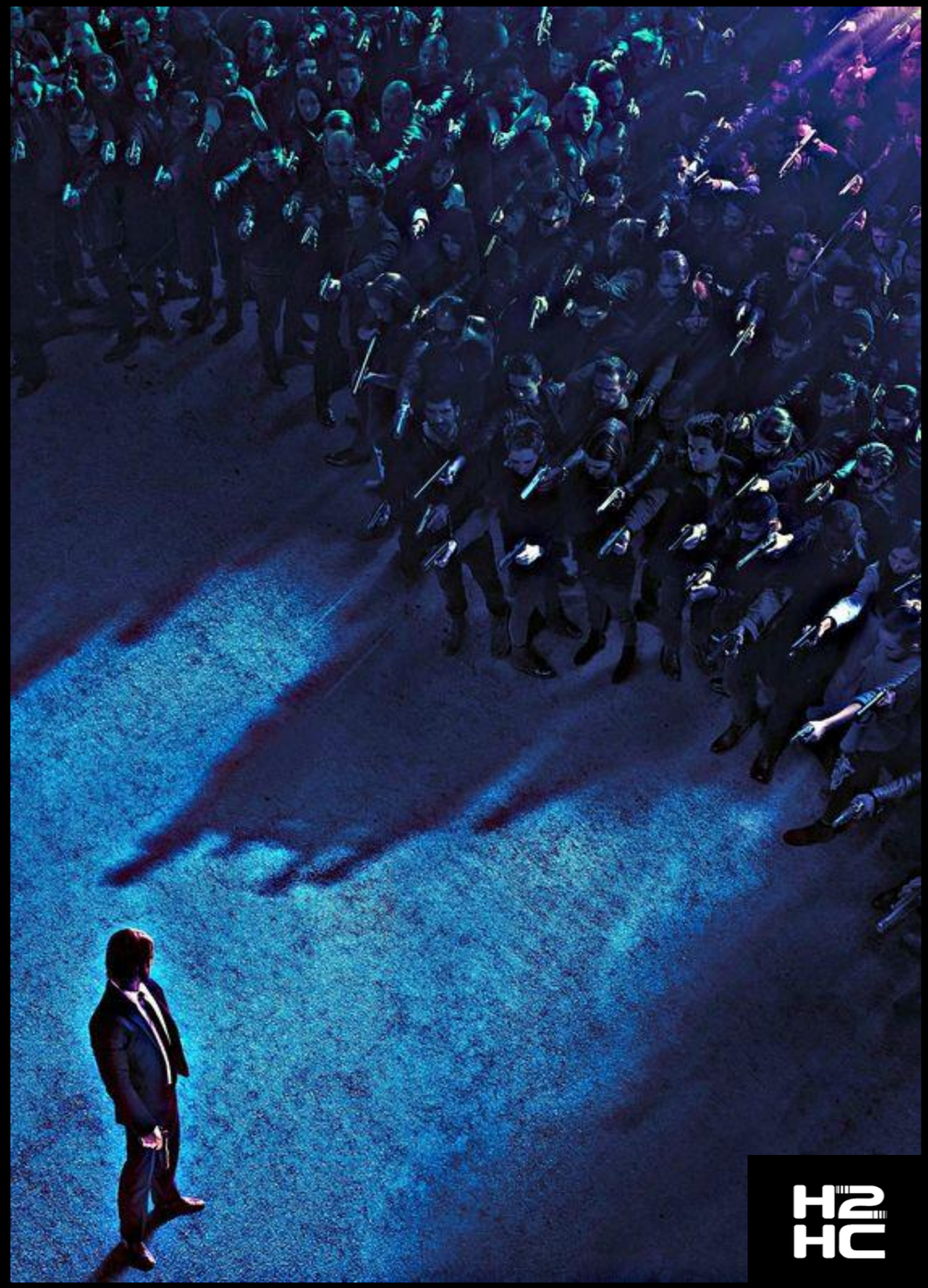


Why use C2 Frameworks

Why use C2 Frameworks

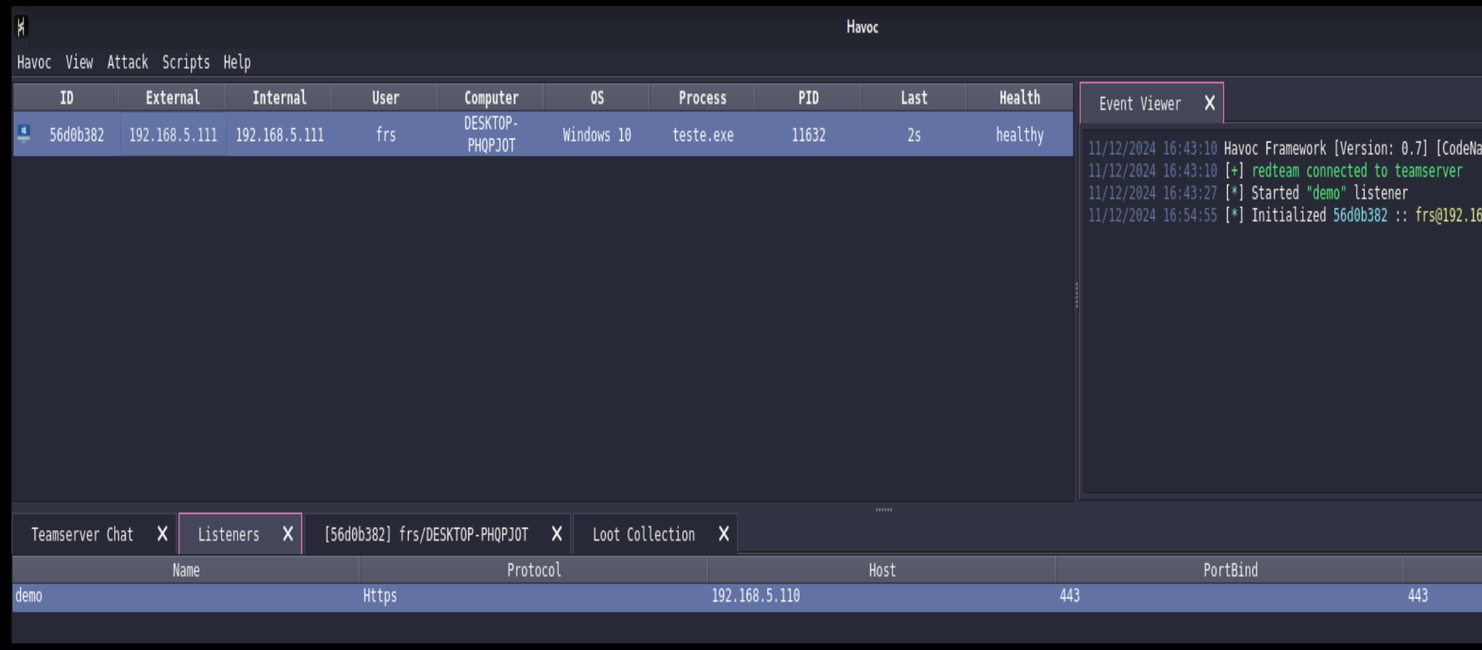
- Test organizacional security um realistic scenarios.
- Simulate modern adversary techniques.
- Reduce the impact of real attacks.

What makes Havoc special ?



Introduction C2 frameworks

- Open-source framework focused on adversary simulations.
- Modularity and customizable expansion.
- Intuitive interface for operations



DEMO

Questions? Thank You!

linkedin.com/in/oryon-farias/

Oryon Farias
0sfx01

instagram.com/0sfx01/