RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

SESSION ID: LAB3-T01

Attack, Detect, and Respond with the C2 Matrix and Multiple C2 Frameworks

#RSAC

Jorge Orchilles

Instructor, Author, Ambassador
SANS Institute
@JorgeOrchilles

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

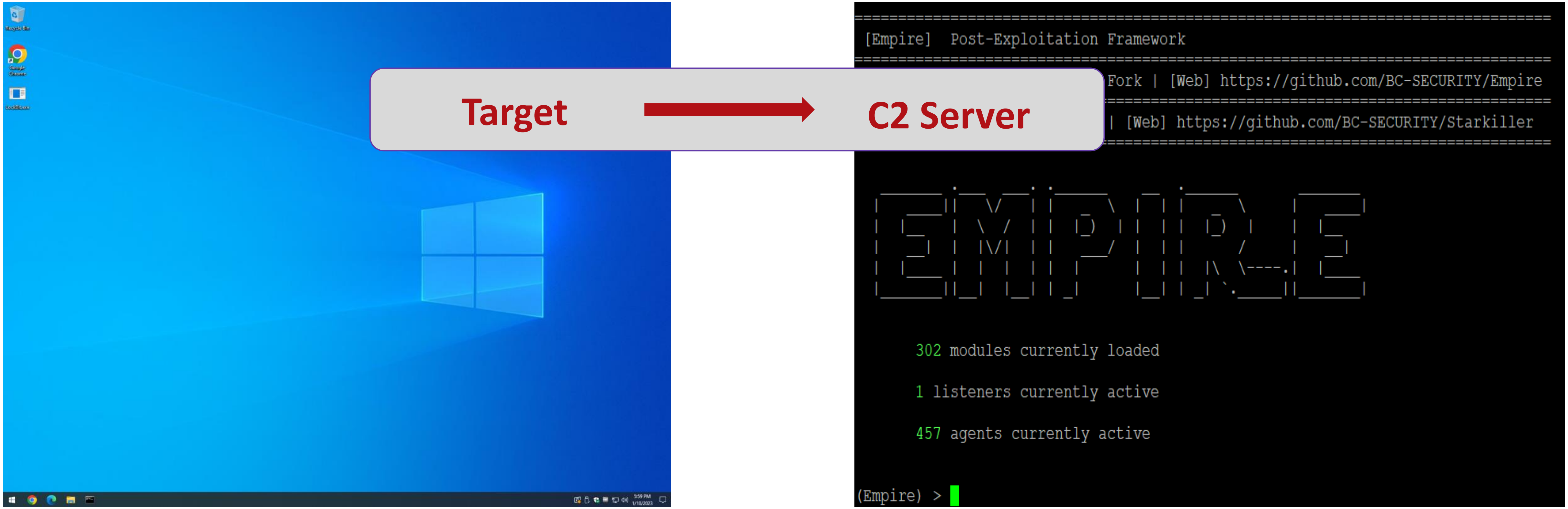
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

T1033 – User Discovery: Jorge Orchilles

- SANS Principal Instructor and Author of SEC565: Red Team Operations and Adversary Emulation
- Director – Vulnerability Management, Pen Test, Red Team, Breach and Attack Simulation, Purple Team, and Adversary Emulation
- Creator of Purple Team Exercise Framework and C2 Matrix
- Contributor to ATT&CK, Atomic Red Team, CVSSv3, and others
- ISSA Fellow, NSI Technologist Fellow
- Soccer/Football Fan: HALA MADRID

TA0011 – Command and Control (C2)

“techniques that adversaries may use to communicate with systems under their control within a victim network" - MITRE ATT&CK®



```
================================================================================
 [Empire]  Post-Exploitation Framework
================================================================================
                                   Fork | [Web] https://github.com/BC-SECURITY/Empire
================================================================================
                                  | [Web] https://github.com/BC-SECURITY/Starkiller
================================================================================

   _______   ___  ___   ______    __   ______        _______
  |   ____| |   \/   | |   _  \  |  | |   _  \      |   ____|
  |  |__    |  \  /  | |  |_)  | |  | |  |_)  |     |  |__
  |   __|   |  |\/|  | |   ___/  |  | |      /      |   __|
  |  |____  |  |  |  | |  |      |  | |  |\  \----. |  |____
  |_______| |__|  |__| | _|      |__| | _| `._____| |_______|


       302 modules currently loaded

       1 listeners currently active

       457 agents currently active


(Empire) >
```

Listeners

- A command and control (C2) server is an attacker-controlled system that is used to communicate with implants
- C2 servers "listen", serve tasks, and retrieve the results from the registered implants
- A variety of methods to establish network communications or "channels“
  - HTTP/S (network egress)
  - DNS (network egress)
  - TCP (peer-to-peer)
  - SMB (peer-to-peer)

C2 Client

- A listener needs a client to connect to it for command and control
- Depending on framework/tool they may be called stagers, payloads, implants, agents, and/or grunts
- This is the code that will run on the target system and communicate to the listener over the respective channel
- Many C2 frameworks will generate the client in a variety of different formats

C2 Frameworks

- There are so many C2 frameworks we created a C2 Matrix to compare them
- Google sheet of most C2 frameworks
- Documents capabilities and limitations of each framework
- www.thec2matrix.com

Demo of C2 Matrix

https://thec2matrix.com/

SANS Slingshot C2 Matrix Edition

- Free virtual machines from SANS with multiple pre-installed tools
- C2 Matrix Edition aims to aid learning of C2 frameworks and get straight to testing C2s in your organization
- Used in multiple SANS courses
- New release today for RSAC!
- https://www.sans.org/tools/slingshot/
- https://howto.thec2matrix.com/slingshot-c2-matrix-edition

RSAConference™2023

Stronger Together

Hands On Time

“Apply” Slide

- Next week you should:
  - Ask what C2 frameworks the cyber security teams are tracking
- In the first three months following this presentation you should:
  - Run a Purple Team Exercise leveraging a C2 that is likely to be used against your organization
- Within six months you should:
  - Establish a Purple Team Program to test other C2 frameworks, adversary behaviors, and tactics, techniques, and procedures (TTPs)