SAND2021-8358D

The Center for Cyber Defenders
Expanding computer security knowledge

TracerFIRE: Attack Chains

Mac Malware

Adrian Belmontes

Tyler Morris, Nick Kantor, Michael Reeves Org. 9373 Kevin Nauer Org 9312

Problem Statement:

- TracerFIRE is a Forensic and Incident Response program simulating a set of corporate level cyber attacks to produce forensic artifacts
- For TracerFIRE to be effective, realistic attack chains are created to simulate real world events. This involves real attack strategies from attackers and common negligence behavior from defenders.

Objectives:

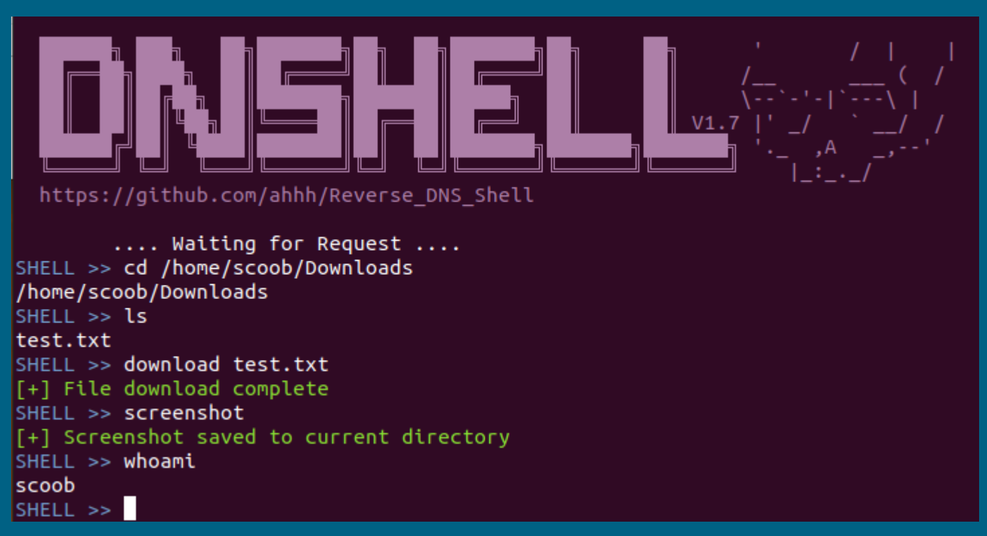
- Develop a realistic spyware malware targeting the mac operating system
- Extract personal information from the targeted mac machine

Approach:

- Draw inspiration from real world spyware and data exfiltration TTPs [1] [2]
- Analyze malware effectiveness on a Linux machine.
- Verify and reconfigure functions to work on the mac operating system
- Compile code into a binary for easier distribution and execution.

Results:

- The malware simulates real world spyware: exfiltrating data, taking screenshots, recording user keystrokes, etc…
- Data is exfiltrated via a reverse shell over an encrypted DNS Command and Control channel
- Real Cyber Forensic Artifacts generated from the Network traffic and Mac OS events



Impact and Benefits:

- Allows the execution of live malware to simulate a realistic spyware on a mac.
- Enables analysis of realistic malware TTPs
- Participants are able to investigate an authentic corporate attack

References:

- [1] Borges, D (2020) Reverse_DNS_Shell (Version 1.7) [Source Code]. https://github.com/ahhh/Reverse_DNS_Shell.
- [2] Owens, C (2021) MacC2 [Source Code]. https://github.com/cedowens/MacC2.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.