SAND2020-7696C

Cyber Attack Chain: Nation State Initial Compromise

Jimmothy Winters, Brigham Young University

Tyler Morris, 09315

CECOR

TracerFIRE

Problem Statement

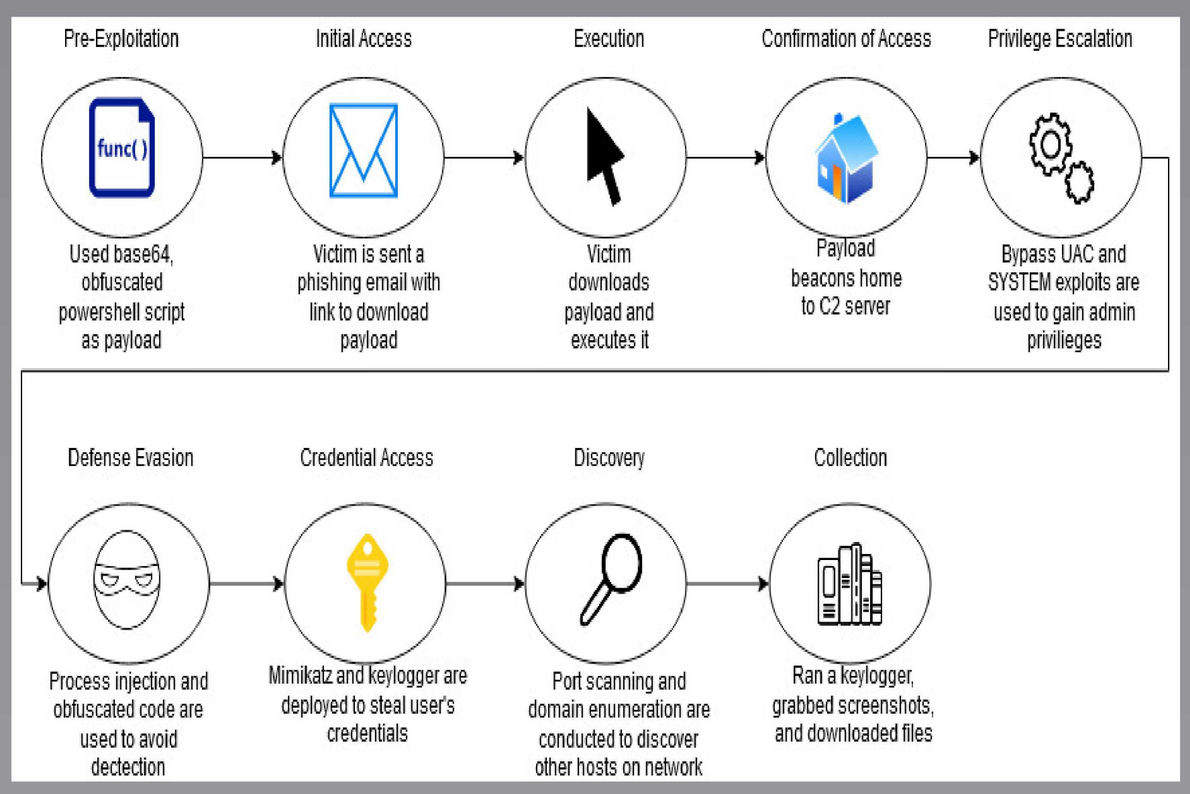
TracerFire is a Forensic and Incident Response Exercise simulation program that simulates an unauthorized, malicious breach of a corporate network. It allows hands on training in incident response and forensic analysis for both security professionals and students at the high school or university level.

In order to make TracerFIRE X as realistic as possible, we aim to use tactics deployed by advanced persistent threats (APTs) and to use the latest technologies and malware to attack the simulated corporate network.

Objectives

- Design an attack chain based off a known APT
- Use known and commonly used malware to compromise a corporate workstation
- Prepare to pivot and compromise other machines on the network

Attack Diagram



Approach

- Designed an attack chain based on the techniques found in the Mitre Att&ck Framework, specifically Initial Access, Execution, Privilege Escalation, Defense Evasion, Credential Access, Discovery, and Collection
- Used Cobalt Strike to replicate, as closely as possible, known attack strategies and techniques of APT29
- Researched ways to conduct lateral movement to remote workstations and domain controllers

```
$Base64= "U2V0LVN0cmljdE1vZGUgLVZlcnNpb2....”

$Content = [System.Convert]::FromBase64String($Base64)

Set-Content -Path "$env:USERPROFILE\AppData\Local\Temp\malware.ps1" -Value $Content –Encoding Byte

Invoke-Expression -Command "powershell.exe -windowstyle hidden -file '$env:USERPROFILE\AppData\Local\Temp\malware.ps1'"
```

Results

- The PowerShell payload linked in a phishing email successfully compromises workstation
- The victim runs the script as an administrator, and the attacker now has elevated access to workstation
- The attacker evades detection, collects credentials, and files
- The attacker discovers other hosts in the network and prepares to compromise the domain controller

Future Plans

- Incorporate persistence in attack design
- Incorporate lateral movement in attack design

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

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. SAND2019-???????

Sandia National Laboratories