Sign in

RhinoSecurityLabs / Aggressor-Scripts

Public

Notifications Fork 42 Star 144

Code Issues 1 Pull requests Actions Projects Security Insights

Aggressor-Scripts / UACBypass /

Name	Last commit message	Last commit date
..		
modules		
ExampleAudit.png		
README.md		
uacbypass.cna		
uacdemo.mp4		

README.md

This aggressor script adds three UAC bypass techniques to Cobalt Strike's interface + beacon console. These include:

```
1. SLUI Registry Hijack
2. FODHELPER Registry Hijack
3. Token Duplication Attack
```

This is done by writing a statically named ADS file, temp.dll, and executing rundll32 as the command. It then deletes the ADS temp.dll as cleanup.

Functions added include:

- fodhelper_exploit
  - Uses fodhelper registry hijack to gain a new admin beacon shell.
- tokenduplication_exploit
  - Uses token duplication magic to gain a new admin beacon shell.
- slui_exploit
  - Uses SLUI registry hijack to gain a new admin beacon shell.
- audit_uac
  - Returns which UAC bypasses from this script will execute successfully.

A demonstration can be found in uacdemo.mp4 (sorry for the poor quality, but should give a basic sense.). An example of the audit can be found in the ExampleAudit.png image.

Credit to the original authors of the bypass UAC techniques implemented here, including:

- bytecode77
- winscripting
- enigma0x3
- tiraniddo
- fuzzySec
- hfiref0x for creating an aggregate repository of UAC bypasses.