harleyQu1nn Merge pull request #16 from 0xAsh/master 570a7d7 · last year 189 Commits

DriverSearcher	Updated for CrowdStrike	5 years ago
Logging	Added Newer Symantec processes	7 years ago
Persistence	escape backslashes	4 years ago
AVQuery.cna	Fixed line 21 errors and added a pause ...	6 years ago
All_In_One.cna	Remaking this completely, keep an eye ...	6 years ago
ArtifactPayloadGenerator.cna	Updated and Fixed for CS 4.0	4 years ago
CertUtilWebDelivery.cna	Updated script to use PowerPick thank...	7 years ago
EDR.cna	Fixed a bunch of syntax + logic errors	last year
ProcessColor.cna	Added Cybereason processes	5 years ago
ProcessMonitor.cna	Add files via upload	7 years ago
ProcessMonitor.ps1	Add files via upload	7 years ago
README.md	Update README.md	last year
RedTeamRepo.cna	Update RedTeamRepo.cna	7 years ago
SMBPayloadGenerator.cna	SMB Artifact Payload Generator	6 years ago
logvis.cna	Added in real time updating	6 years ago

README

Aggressor Scripts

Collection of Aggressor scripts for Cobalt Strike 3.0+ pulled from multiple sources

- All_In_One.cna v1 - Removed and outdated
  - All purpose script to enhance the user's experience with cobaltstrike. Custom menu creation, Logging, Persistence, Enumeration, and 3rd party script integration.
  - Version 2 is currently in development!
- ArtifactPayloadGenerator.cna
  - Generates every type of Stageless/Staged Payload based off a HTTP/HTTPS Listener
  - Creates /opt/cobaltstrike/Staged_Payloads, /opt/cobaltstrike/Stageless_Payloads
- AVQuery.cna

About

Collection of Aggressor scripts for Cobalt Strike 3.0+ pulled from multiple sources

scripts cobalt-strike aggressor-scripts red-team cna aggressor

Readme
Activity
1.5k stars
67 watching
300 forks
Report repository

Releases

No releases published

Packages

No packages published

Contributors 6

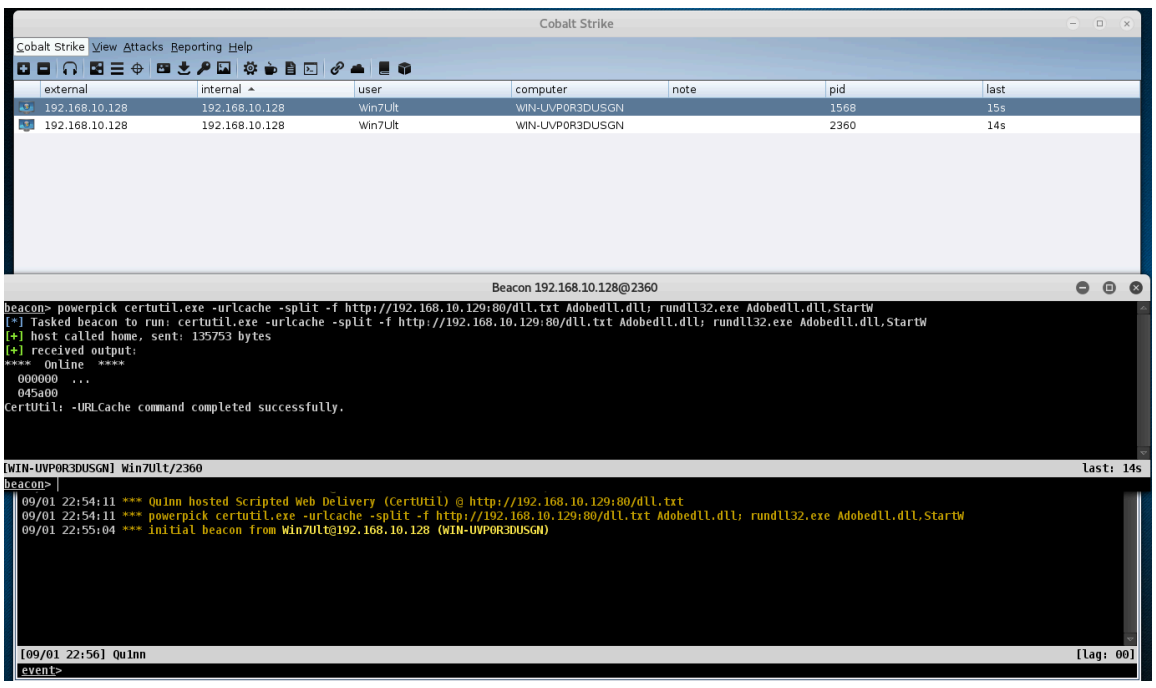
Languages

C# 71.1% Python 18.9% PowerShell 10.0%

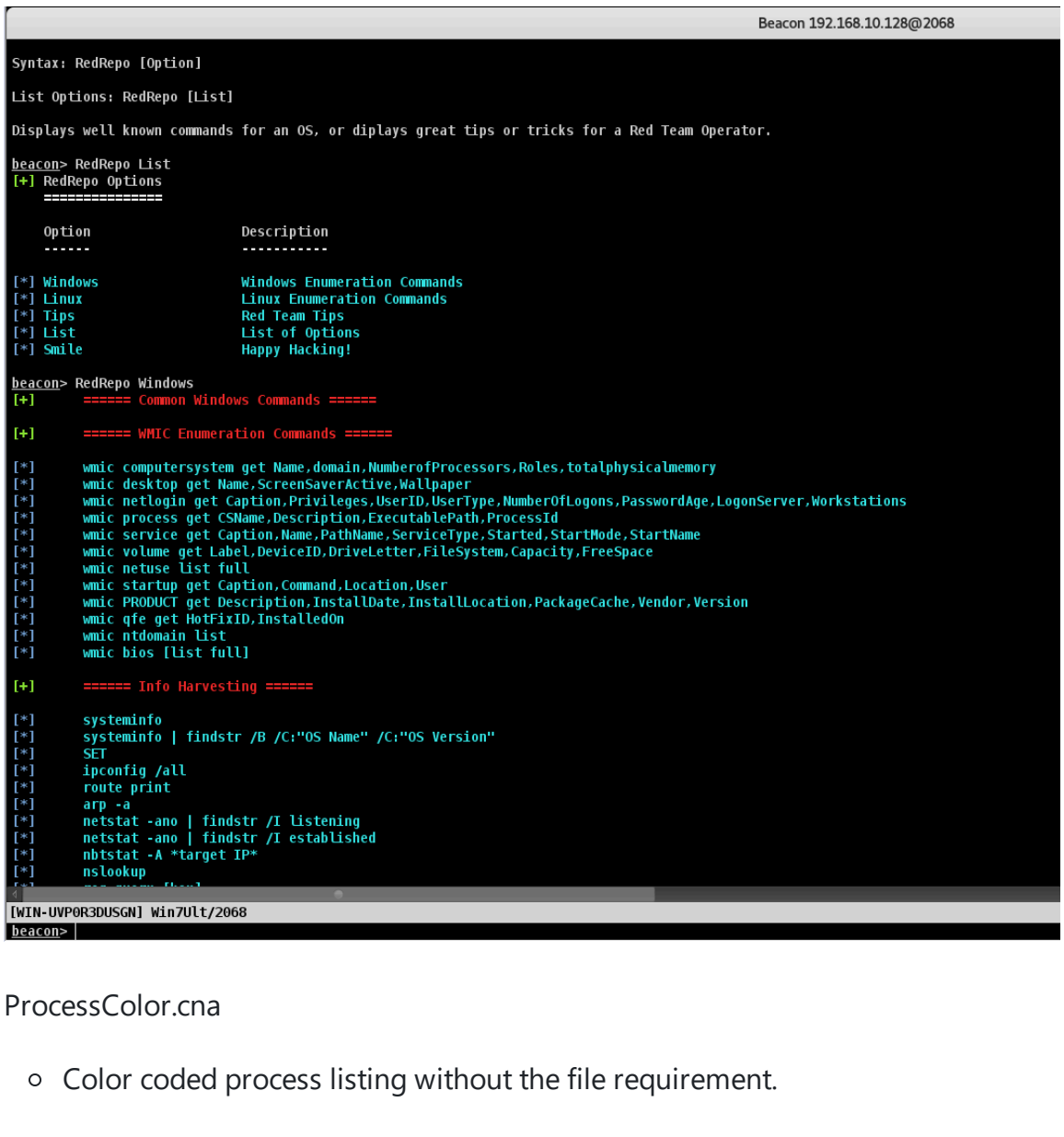
- Queries the Registry with powershell for all AV Installed on the target
- Quick and easy way to get the AV you are dealing with as an attacker

```
beacon> AV_Query
[+] Determining what AntiVirus is installed...
[+] host called home, sent: 1437 bytes
[+] received output:

PID|Name|Path

1820|McTray|C:\Program Files (x86)\McAfee\Common Framework\McTray.exe
2380|shstat|C:\Program Files (x86)\McAfee\VirusScan Enterprise\SHSTAT.EXE
4796|UdaterUI|C:\Program Files (x86)\McAfee\Common Framework\UdaterUI.exe

Windows Defender AV Signature Version:
1.247.735.0

AV Name|Version|Install Date

McAfee Agent|4.5.0.1810|20130408
McAfee VirusScan Enterprise|8.8.00000|20130408
Malwarebytes version 3.1.2.1733|3.1.2.1733|20170710

[+] received output:
displayName                 pathToSignedProductExe
McAfee VirusScan Enterprise  "C:\Program Files (x86)\McAfee\VirusScan Enterprise\SHSTAT.EXE" /!REMEDIATE
Malwarebytes                C:\Program Files\Malwarebytes\Anti-Malware\MBAMWsc.exe
```

- CertUtilWebDelivery.cna
  - Stageless Web Delivery using CertUtil.exe
  - Powerpick is used to spawn certutil.exe to download the stageless payload on target and execute with rundll32.exe



- EDR.cna
  - Detects EDR solutions running on local/remote hosts
- RedTeamRepo.cna
  - A common collection of OS commands, and Red Team Tips for when you have no Google or RTFM on hand.
  - Script will be updated on occasion, feedback and more inputs are welcomed!



- ProcessColor.cna
  - Color coded process listing without the file requirement.
  - Thanks to @oldb00t for the original version: https://github.com/oldb00t/AggressorScripts/tree/master/Ps-highlight