

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

🔍

Sign in

Sign up

📄 harleyQu1nn / AggressorScripts Public

🔔 Notifications

Fork 300

Star 1.5k

<> Code

🕒 Issues 2

Pull requests

🔄 Actions

Projects

Security

Insights

master ▾

🔍

Go to file

<> Code ▾

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

📈 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%

📖 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- All_In_One.cna v1 - Removed and outdated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

- 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

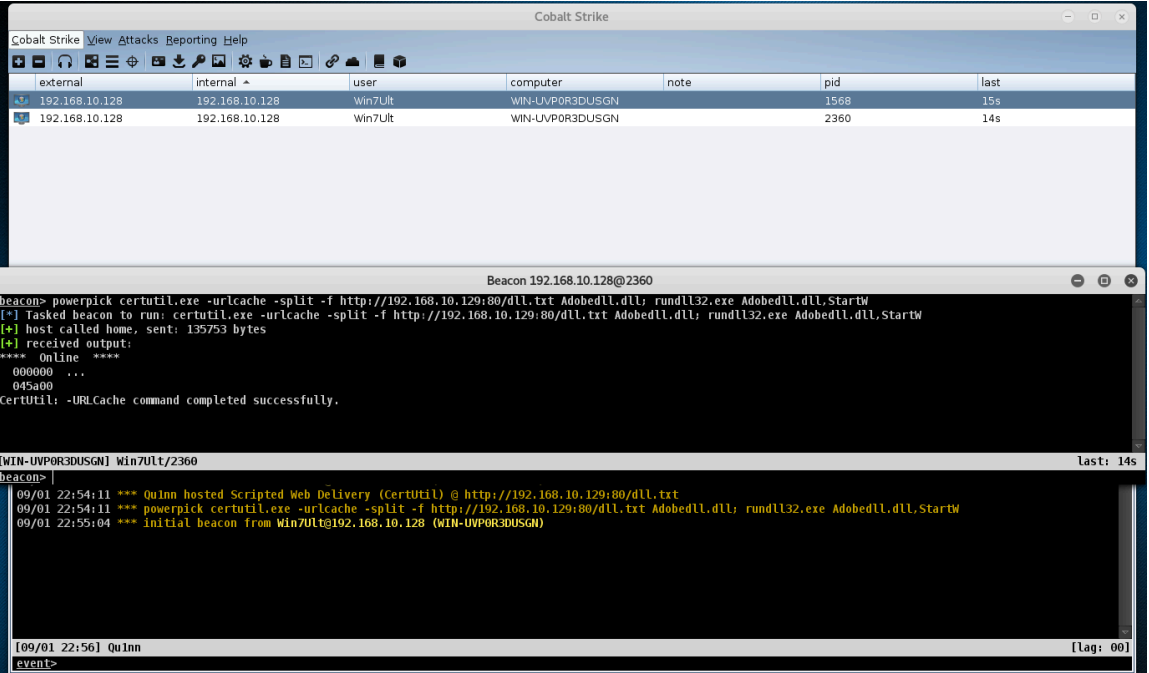
Windows Defender AV Signature Version:
1.247.735.0

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!

```

Beacon 192.168.10.128@2068

Syntax: RedRepo [Option]

List Options: RedRepo [List]

Displays well known commands for an OS, or diplays great tips or tricks for a Red Team Operator.

beacon> RedRepo List
[+] RedRepo Options
=====

Option          Description
-----
[*] Windows      Windows Enumeration Commands
[*] Linux         Linux Enumeration Commands
[*] Tips          Red Team Tips
[*] List          List of Options
[*] Smile         Happy Hacking!

beacon> RedRepo Windows
[+] ===== Common Windows Commands =====

[+] ===== WMIC Enumeration Commands =====

[*] wmic computersystem get Name,domain,NumberOfProcessors,Roles,totalphysicalmemory
[*] wmic desktop get Name,ScreenSaverActive,Wallpaper
[*] wmic netlogin get Caption,Privileges,UserID,UserType,NumberOfLogons>PasswordAge,LogonServer,Workstations
[*] wmic process get CSName,Description,ExecutablePath,ProcessId
[*] wmic service get Caption,Name,PathName,ServiceType,Started,StartMode,StartName
[*] wmic volume get Label,DeviceID,DriveLetter,FileSystem,Capacity,FreeSpace
[*] wmic netuse list full
[*] wmic startup get Caption,Command,Location,User
[*] wmic PRODUCT get Description,InstallDate,InstallLocation,PackageCache,Vendor,Version
[*] wmic qfe get HotFixID,InstalledOn
[*] wmic ntdomain list
[*] wmic bios [list full]

[+] ===== Info Harvesting =====

[*] systeminfo
[*] systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
[*] SER
[*] ipconfig /all
[*] route print
[*] arp -a
[*] netstat -ano | findstr /I listening
[*] netstat -ano | findstr /I established
[*] nbststat -A *target IP*
[*] nslookup
[+] net sweep flood

[WIN-UVP0R3DUSGN] Win7Ult/2068
beacon>
```

- 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>

```

Beacon : ██████████ @2872

beacon> ps
[*] Tasked beacon to list processes
[+] host called home, sent: 12 bytes
[*] Process List with process highlighting of AV/HIPS, Browsers, Explorer/Winlogon, current processes
[*] Current Running PID: Yellow
[*] AV/HIPS: RED
[*] Browsers: GREEN
[*] Explorer/Winlogon: BLUE

PID  PPID  Name                Arch  Session  User
---  ---
0     0     [System Process]
4     0     System
256   4     smss.exe
280   492   svchost.exe
332   324   csrss.exe
384   324   wininit.exe
396   376   csrss.exe
432   376   winlogon.exe
492   384   services.exe
500   384   lsass.exe
508   384   lsm.exe
572   852   dwm.exe             x64   1
576   2872  explorer.exe         x64   1
612   492   svchost.exe
672   492   vmacthlp.exe
708   492   svchost.exe
788   492   svchost.exe
852   492   svchost.exe
896   492   svchost.exe
932   492   svchost.exe
1036  492   csrss.exe
```