Detection and Countermeasures of Cheat Engine

Lijiu Liang *Zhenlei Song*
928000822 *862009388*

Abstract

Cheat Engine (CE) is an open-source memory scanner for Windows operating system, which is mostly used for cheating in PC-games. Cheat Engine can view the disassembled memory of a specific process and allow the alteration of game data to break the normal game routine. To keep their productions away from illegal alterations or cheating, PC-game designers take some measures to detect Cheat Engine and prevent it create a thread in its own process. Meanwhile, the existing methods of detection and countermeasures are deficient. This project does an investigation of current popular detecting method and implements a new method to detect and counter Cheat Engine by using Windows API.

Introduction

•Cheat Engine is a free and open-source memory scanner created by Eric Heijnen ("Dark Byte"). It is developed on Lazarus IDE for 32 and 64-bit versions of Windows. Most parts of Cheat Engine are written in Object Pascal, while the kernel modules are written in C. The most famous feature of Cheat Engine is viewing the disassembled memory of a PC-game process based on scanning changes in specific value. After knowing the address information of certain data, Cheat Engine allow the alternation of game states to give the user advantages such as infinite health, changing the number of items, or even clearing stages without playing. Cheat Engine also has some Direct3D manipulation tools that support vision through walls or creating amibots. Another important feature of Cheat Engine is, it allow users to share their addresses locations or Lua scripts via Cheat Table, a file with extension .CT that can be opened by Cheat Engine.
•For the purpose of altering memory value, Cheat Engine scans the virtual memory section of the target process and finds the accurate address of certain value by detecting the value's change. However, game processes are executed on Ring 3 of the privilege ring for the operating system. Ring 3 has no privilege to access physical memory and change the value. Cheat Engine can access Ring 0 by using Windows API. The Windows API (WinAPI) is Microsoft's core set of application programming interfaces available in the Microsoft Windows operating systems. WinAPI is the most direct method for almost all Windows programs to interact with Windows operating system.
•Meanwhile, Windows API calls can be forbidden by using hooking. In that case, Cheat Engine also provides APIs by itself. These APIs are offered by dbk32.sys and are basically similar to Windows APIs. Hence, Cheat Engine can bypass hooks implemented by game designers and access the memory of game processes all the time.
•The motivation of this project is to find out a new method to detect and counter Cheat Engine while not so consumptive. We will introduce detailed mechanisms of Cheat Engine and demonstrate the way of detection and countermeasures.

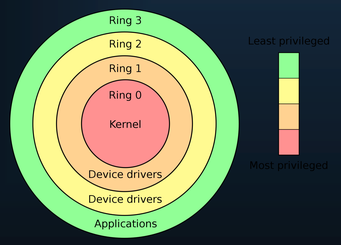

Figure 1. Privilege rings for x86 Windows

Existing Methods

•Steam maintains a blacklist that is updating rapidly. Their famous anti-cheat system VAC scans the environment of clients and matches the name appears in their blacklist. They also take snapshots for some specific flags in a game and upload to their database, then they analyse them manually.

•Another famous anti-cheat program is TenProtect (TP) by Tencent. TP implements many hooks on Windows OS and hence it has the most significant effect to count any form of cheat, including Cheat Engine. However, this anti-cheat tool seriously relies on the current environment of client's computer. Crushes can be caused by any change on client's OS. TP is notorious by its frequent update and corrupting the performance of OS.

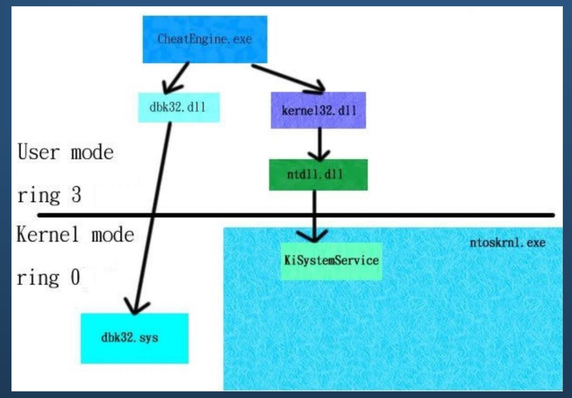

Figure 2. Methods for Cheat Engine to access Ring 0

Countermeasure

•There are mainly two classes of Cheat Engine countermeasures for games: external methods and internal methods. For external level, WinAPI offers a function \textit{TerminateProcess} to kill any process by passing the handle of that process. This is the most direct way to counter Cheat Engine: as long as we detect it, we kill it instantly. However, this function requires administrator privilege. In other word, the PC game implemented this approach has to running under administrator privilege. This will lead serious security issues. The safer way is implementing an internal method that manipulates the game itself, like quitting the game itself or applying other method to prevent cheaters befitting from Cheat Engine. For instance, the "save" option may be disabled after Cheat Engine is detected. In the famous online game \textit{Monster Hunter: World}, Capcom$^\circledR$ disable the Internet connection service to prevent cheaters from infecting other players.According to above reason, the countermeasures varies from different games. Game designers should propose an internal method based on the mechanisms of the game.

Detection

•We implement two naive methods to detect Cheat Engine and using WinAPI call to kill the Cheat Engine's process as a countermeasure first.

•Detection based on scanning all processes

•In order to access the basic information of a process, function CreateToolhelp32Snapshot takes a snapshot of the specified processes. We can get the process ID and the name of the executable file for this process. And function Process32First and Process32Next are used to traverse the current processes in the background. Combine these functions, we can scanning all of the current processes and search for the name of executable file by matching with a blacklist. As we mentioned before, this approach can be easily bypassed by modifying the source file of Cheat Engine in Lazarus. The name of executable file can be customized randomly and the blacklist will fail to match the name.

•Detection based on opening window

•Another approach to search whether the process of Cheat Engine is running is searching the current opening windows. Up to the latest released version of Cheat Engine, it has to work with a GUI window opened. So there must be a window for Cheat Engine when it is working.This approach can evidently reduce the workload of detection, for the reason that the amount of opening windows is significantly less than the amount of current processes. Function \textit{FindWindow} will find the window of Cheat Engine by exactly matching the name of the window. After searching, if there exists a target window, function \textit{GetWindowThreadProcessId} accesses the pid of this process.However, this approach has a considerable limitation. It has to match the window by exact name. Although the exact name of windows can be accessed by function \textit{GetForegroundWindow}, this approach again can be bypassed by modifying the source file of Cheat Engine in Lazarus. We are trying to extract another feature to identify the process of Cheat Engine.

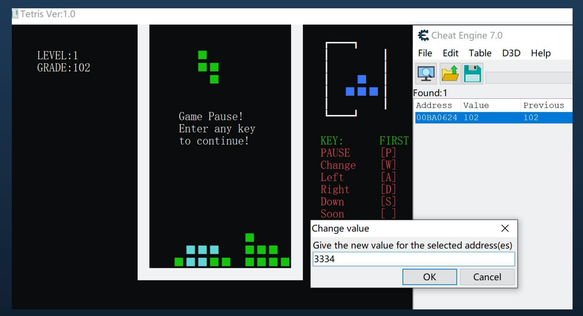

Figure 3. Tetris Data Modify

Detection (cont.)

•To overcome the above limitations, we implement a improving method using hash.

•Detection based on data integrity

•The main purpose of cheat engine is to modify essential data in games. The idea of checking the data integrity come up then. Normally essential is stored in memory itself. If we calculate its hash value each time when writing, and check if the 'data-hash' pair match when reading. We can find out if there exists illegal writing operation. Here we present an example in a classic game 'Tetris' shown in Figure 3. We pretend to be a cheater using cheat engine to modify the score from 102 to 3334. Then at the end of current round, this action is found.

•Besides data aspect, the other purpose using cheat engine is to manipulate the functions in games. Like in shooting games, cheaters can replace API of clicking mouse to auto-aiming shooting function. By modifying Windows system DLL, or modifying DLLs provided by games.In this aspect, we came up with that either to change Windows API or replace game API, the ultimate result is to modify DLL. Thus, our detection measure is to detect the integrity of all DLLs and EXE files repeatedly. Calculate Md5 value of all lib files, if any of them is changed, it must be illegal. Then a cheat action has been found. The MD5 format is shown in Figure 4.

```
MD5 的 C:\Users\songzhenlei\source\repos\netSec_pro\Debug\netSec_pro.exe 哈希:
833baccf896de588689a02c57c59dcd4
CertUtil: -hashfile 命令成功完成。
MD5 的 C:\Windows\SYSTEM32\ntdll.dll 哈希:
013f9a951a890a4e517d2a13fc4b80c0
CertUtil: -hashfile 命令成功完成。
MD5 的 C:\Windows\System32\KERNEL32.DLL 哈希:
226049bc657b3884e96c5b9edc908cd7
CertUtil: -hashfile 命令成功完成。
MD5 的 C:\Windows\System32\KERNELBASE.dll 哈希:
38054754e51d3846471281e6e8af5c56
CertUtil: -hashfile 命令成功完成。
MD5 的 C:\Windows\SYSTEM32\VCRUNTIME140D.dll 哈希:
28b900d857f8958d25f73350a7fa711b
CertUtil: -hashfile 命令成功完成。
MD5 的 C:\Windows\SYSTEM32\ucrtbased.dll 哈希:
ceeda0b23cdf173bf54f7841c8828b43
CertUtil: -hashfile 命令成功完成。
```

Figure 4. Example of Hash

Discussion

This project is encouraged by the facts that people cheats in PC-games using Cheat Engine recently and Cheat Engine is hard to be detected. Meanwhile, the existing protection methods applied by big companies like VAC and TP are defective. For this point, We implement a new method to detect Cheat Engine from the aspect of data integrity and .dll integrity. Cheat Engine's modification can be detected by monitoring the integrity of important data in real time. In the end, this methods is proved to be effective by our implementation.For the further studies, we will implement our method on some more sophisticate games and measure the performance of our detector.