Kernel Based Security Solution

Morgan Stanley

Kelvin Chan

Windows Client And Kernel Security Engineer

Tencent

WHO AM I?

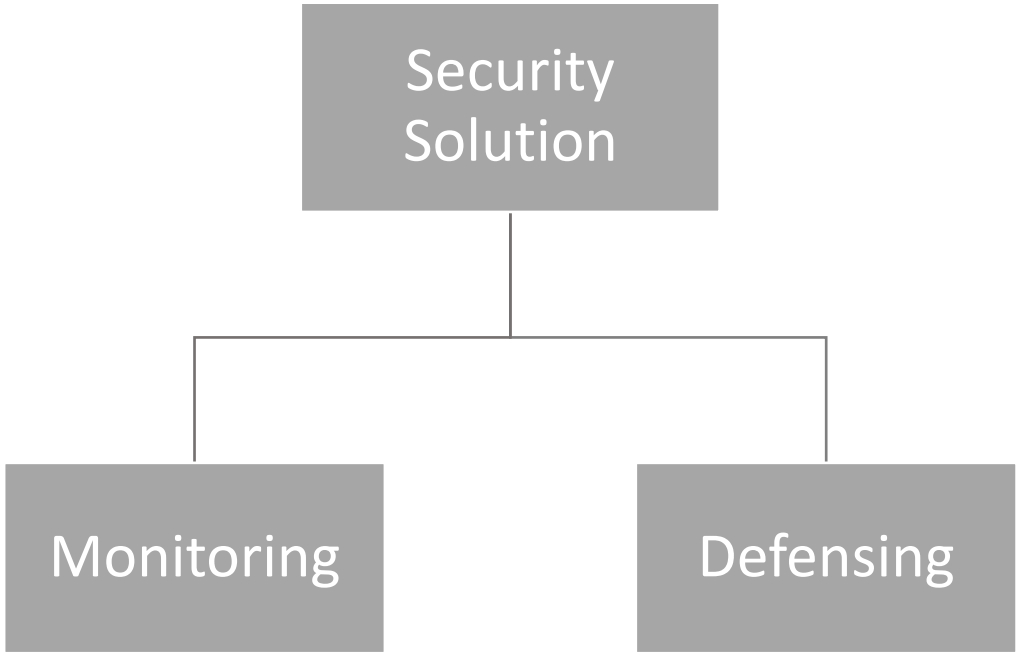
- Kelvin
- Windows Kernel Based Solution Researcher
- For Protecting Tencent Games in different layer.
- …..

Overview

- Ideal Security Solution Architecture
- What is kernel Based Solution?
- Why kernel Based is necessary?
- Who can be protected ?
- What data / behavior can be obtained ?
- Black Case – Keylogging
- Black Case – APT Attack
- Black Case – Game Cheat
- White Case – 360 Anti-Virus
- White Case – NProtect GameGuard
- White Case – Tencent QQ
- Difficulties for development
- Further Research – Virtualization Technology

Ideal Solution Architecture

- Suitable for enterprise internal
- Suitable for product protection
- Attacker hard to know who is trapped
- Who is attacker?
- Which part is being attacked?
- Good for security data analysis

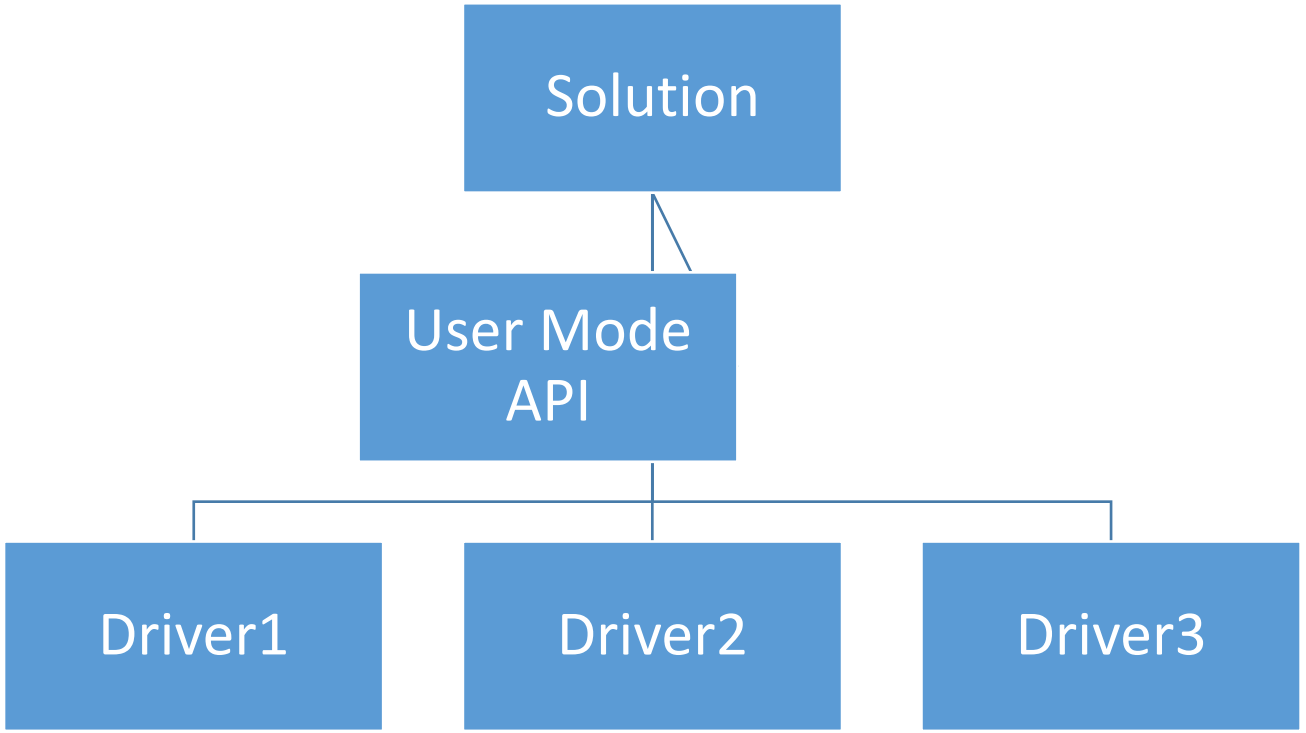


Question:

- How to ensure monitoring and confrontation is good enough?

What is kernel Based Solution?

- Kernel Based Solution always included different component
- Usual including :
  - A Dynamic Link Library (DLL) for interact with protected target
  - Different Function Driver which is running in kernel space



Why kernel is a good start point ?

- Moving a confrontation to the lower level
- A critical API is finally executed by kernel
  - Such as , OpenProcess, CreateFile, ReadFile, etc.
- Kernel behavior is transparent to API
- Good for hiding itself from the attacker , prevent attacker hack the solution
- Ensuring the correctness of data , prevent faked data by attacker

Why kernel based solution is necessary?

- Malware is moving to kernel (Rootkit)
- Kernel may also be infected , solution may easily be faked
- Most widely attack coverage
- Protection is not limited to specific attack
- Protection is not limited to specific process
- Providing Good Prevention
  - such as, file locking, kernel attacker can totally unlock it very easily
- Provide most accurate behavior and data
- Independent to the system, ensure the target execute environment is acceptable.
- Best User Experience for client , nothing need statically blocked, more flexible

Who can be protected ?

Online Game

– protecting the client , prevent illegal attack to the game

Bank

– protecting the account key-logging

Enterprise Internal security / staff behavior audit

– Whole Operating System itself can be strongly monitored

What data / behavior can be obtained ?

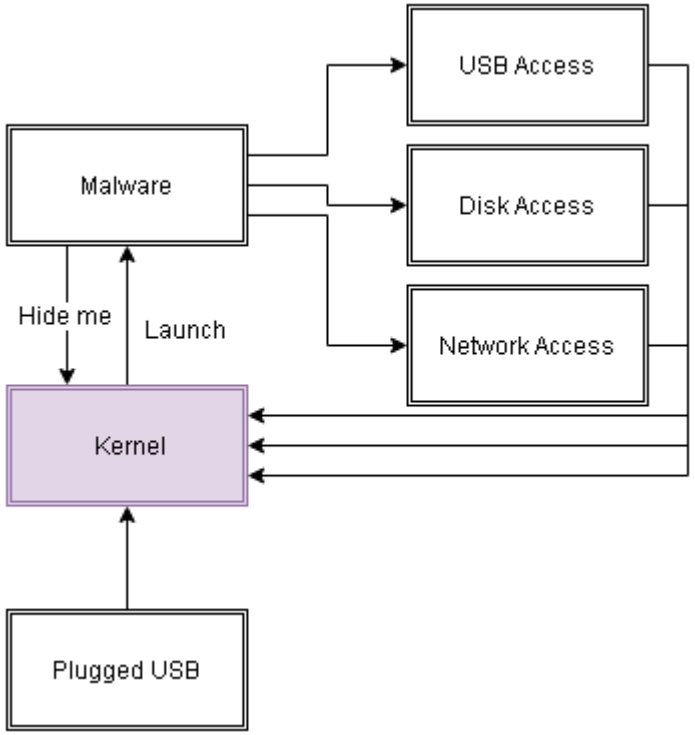
All data is first hand, before dispatch to application:

- File Access , which files is going to be R/W , who is the accessor
- Network Access , packet filtering before the packet dispatch / send out of computer
- CPU execution , which function is going to be executed
- Memory Access , who is trying to access the memory, modify the memory.
- USB / Any PlugPlay Device Access, including the data transfer.
- Graphic Access – who is trying to make a screen capture ?

Black Case - APT Attack

Background:

- A Bank has attacked by internal staff (Real Case)
- No record
- Abuse to whitelist process (notepad.exe)
- Hidden itself from user mode(but kernel mode)
- It always on, and transferring a file.
- It is late when it discover



Problem:

- The bank is hard to make a auditing for the lost during the attacking period

- The bank has no idea how the malware come

- The bank security system has no any response since it just a user-mode protection solution

- The System record of USB Plug-Play is deleted by attacker

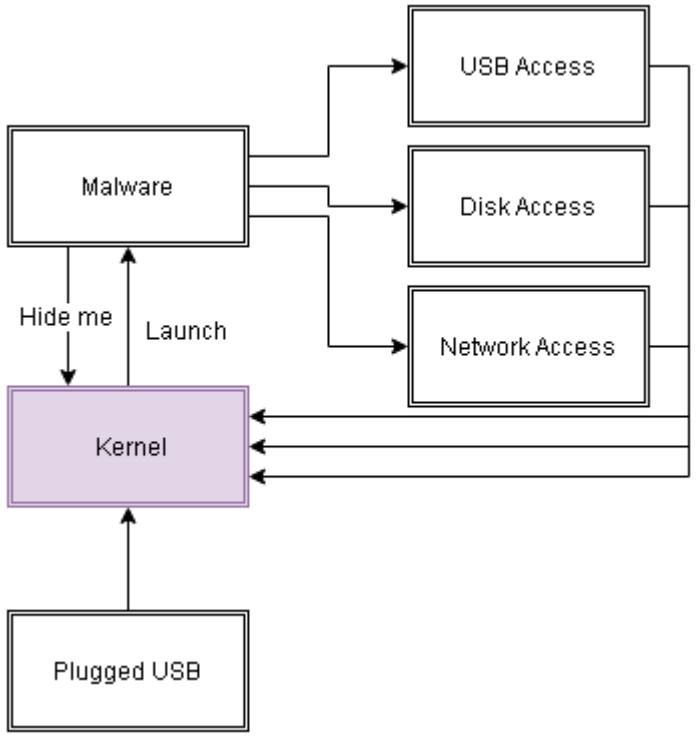
Black Case - APT Attack

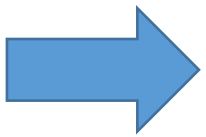
Kernel Solution:

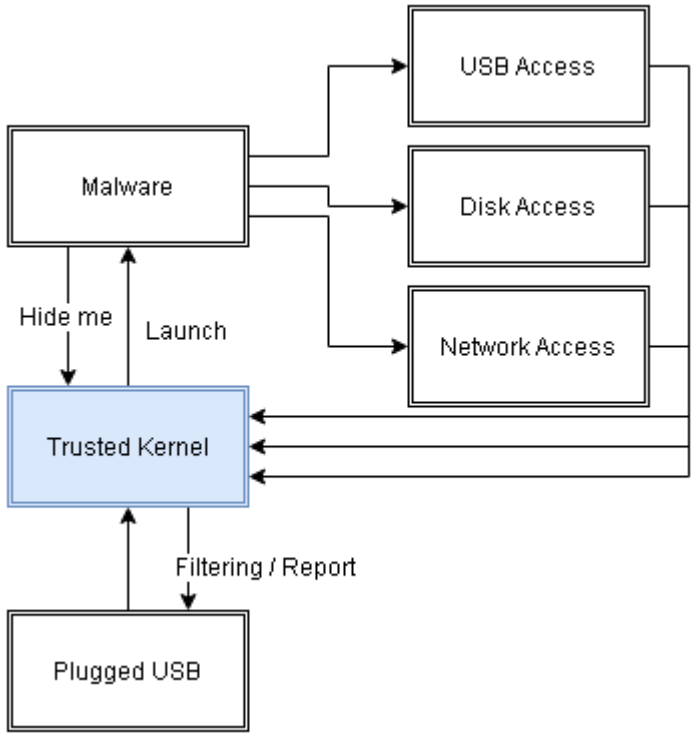
- Enumerating the process which is running in a computer entirely everyday and report it , for reducing the lost

- Monitoring and Report Every USB Plugged event to server, instantly

- Monitoring from kernel when the malware process is created, and stop it instantly







Black Case - Keylogging

Background :

- Key-logging for e-banking process
- A banking e-banking keylogging Trojan deployed in the client computer
- The banking is protected by the User Mode Security Solution, it is only able to detect the User Mode Key-log
- It intercept the user input from kernel

Result :

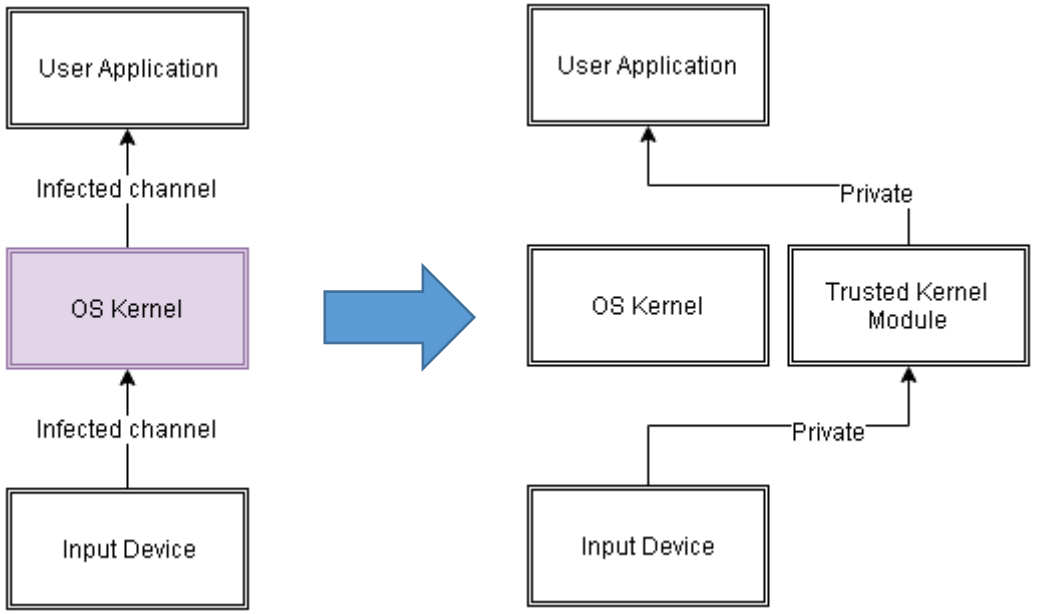
- Lost a lot of client (~100k) e-banking password
- Need to stop the system instantly , when it already boom.

Problem:

- Totally lack of protection for the client
- It shouldn't believe for the input path from OS , assume all OS is infected

Kernel Mode Solution:

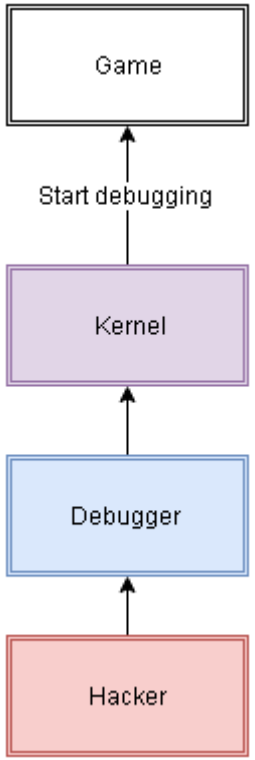
- Provide a private input channel from hardware (keyboard / mouse) directly to e-banking application



Black Case - Game Cheat (巨商)

Background :

- Good example for explaining the importance of kernel mode safety protection
- Over 1milion player game surround the world (Real Case)
- Many type of cheat was created at 2015
- These Cheat is totally damage a fair of the game.
- It operates about 10years with strong user base. The cheat is come, it closed.
- Many hacker try to analysis the game (debugging), do a input emulation , account stolen so on.



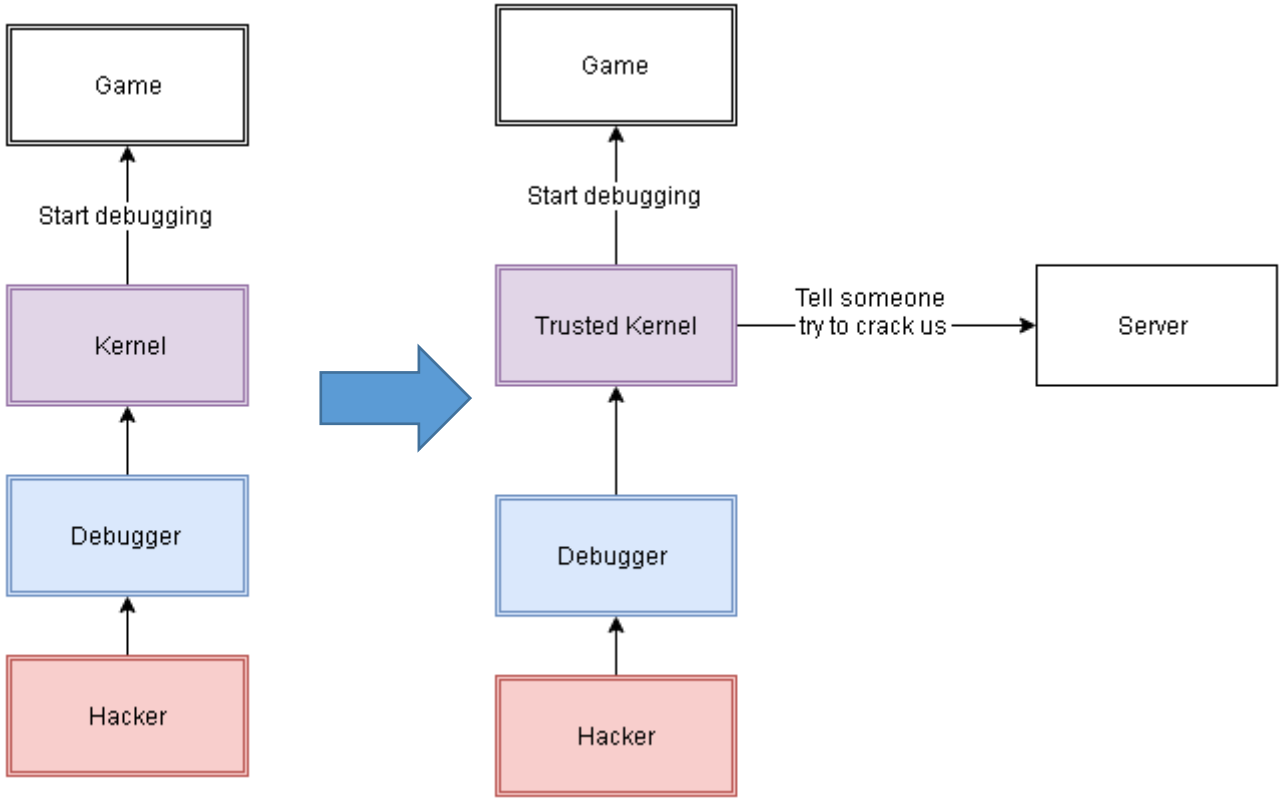
Problem:

- Game Cheat is totally damaging a fair of the game.
- Lack of Anti-Game Cheat from kernel, it has very weak protection
- Easily to debugging (disassembly analysis) it

Black Case - Game Cheat (巨商)

Solution:

- Anti-debugging from kernel
- Speedy check
- Anti-Input emulation
- Provide a private input channel from hardware to the game
- Client-Safety monitoring



White Case – 360 Anti-Virus

- Loading Driver Detection
- Critical File Deleteion

White Case – NProtect GameGuard

White Case – Tencent QQ

Difficulties for development

Further Research – Virtualization Technology