How to secure the keyboard chain

DEF CON 23

Paul Amicelli - Baptiste David - CVO Esiea-Ouest

Creative Commons 2.0 - Attribution - NonCommercial - ShareAlike
The Talk

1. Background
2. Keyloggers forms
3. Main idea of our work
4. Details of our work
5. To go further
6. Finally.
Keyloggers

"A keylogger is a little piece of software or hardware, which is able to retrieve every keystrokes on a computer"
User mode ones

Easy to develop, and really efficient

Quite easy to detect and remove
Kernel mode ones

Quite hard to develop and really, really efficient

Not easy to detect and quite hard to remove
Hardware ones

Require physical access to the computer, but the most efficient technic

Software-undetectable, sometimes easy to remove, sometimes not
Proposed solution

**Encrypt** keystrokes

As close as possible to the hardware

Jamming keyloggers
Basic Understanding

Our work - Main Idea

- APP.exe
- Crscc.exe
- APP.exe

OS - user mode

Device Stack
- Kbdclass
- i8042prt

OS - Kernel

Keyboard
Basic Understanding

- SetWindowsHook
- GetAsyncKeyState
- GetMessage
- Raw Input
Our work - Main Idea

Basic Understanding

- **APP.exe**
- **Crscc.exe**
  - **OS - user mode**
  - **OS - Kernel**
  - **Device Stack**
    - **UpperFilter Driver**
    - **Kbdclass**
    - **i8042prt**
Basic Understanding

- LowerFilter Driver

OS  -  Kernel

Device Stack

Kbdclass

i8042prt

Keyboard
Basic Understanding

- OS - Kernel
  - Device Stack
    - Kbdclass
    - i8042prt
  - Keyboard

• IRQ1 - IDT
Our work - Main Idea

Basic Understanding

OS - user mode

APP

Crscc.exe

APP

OS - Kernel

Kbdclass

Protection Driver

i8042prt

Keyboard
Our work - Details

Keyboard driver stack

- Kbdclass
- Fill IRP
- Protection Driver
- Encrypt
- Queue DPC
- i8042prt
- ISR
- Keyboard
Encryption

Problematic

- Unable to directly encrypt keystrokes with a streamcipher
  - Only known keystrokes are broadcasted by Windows
  - The rest is inhibited
  - Few keystrokes codes authorized
Encryption

White list system for input decision
Encryption

Solution: Jamming

- Currently, a 64bits common key exchanged every 20 keystrokes
- Stream cipher initiated with the common key
- Algorithm based on shuffle of a deck of cards: only
Our work - Details

Encryption Scheme

Input

Key

StreamCipher

Index

Encryption (Permutations)

WhiteList ?

Yes

No

Output
Our work - Details

API-Driver Communication

Diagram showing the communication between different software components in an operating system. The diagram includes boxes labeled API, Client APP, APP, Crcss.exe, Protection Driver, Kbdclass, i8042prt, OS - User mode, and OS - Kernel, with arrows indicating the flow of communication and data transfer.
Protection of the protection

- Monitoring of the keyboard driver stack
- Protection against DLL injection of the API
- Monitoring of the registry
Is it working?
Endless possibilities

- Keystrokes combinations
- **Polymorphic** on-screen keyboard
- **Time** based keystrokes
  - Mini-game, music, colors...
- Keep keystrokes in **ring 0** (GostCrypt)
Our work - Example

GostCrypt

a full ring 0 password version

OS – User Mode

GostCrypt.exe

GostCrypt Format.exe

Requests

OS – Kernel Mode

GostCrypt.sys

Passwd

AntiKeyloggers.sys

Keyboard
State of the project

- Proof of concept
- Available on Github
  (https://github.com/whitekernel/gostxboard.git)
- Educational purpose
- Free and opensource, forever
- Call for participation
Questions?

Maybe answers . . .