How to secure the keyboard chain

DEF CON 23

Paul Amicelli - Baptiste David - CVO Esiea-Ouest

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 developp, 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

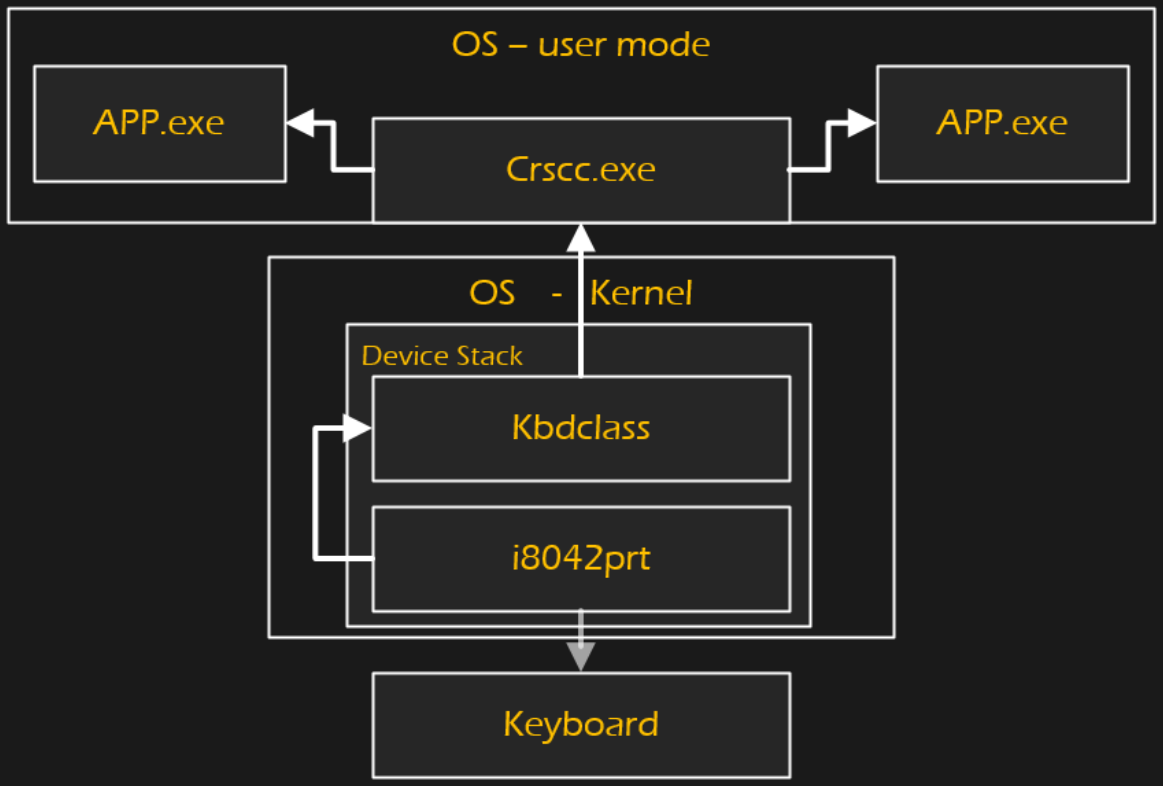
Proposed solution

Encrypt keystrokes

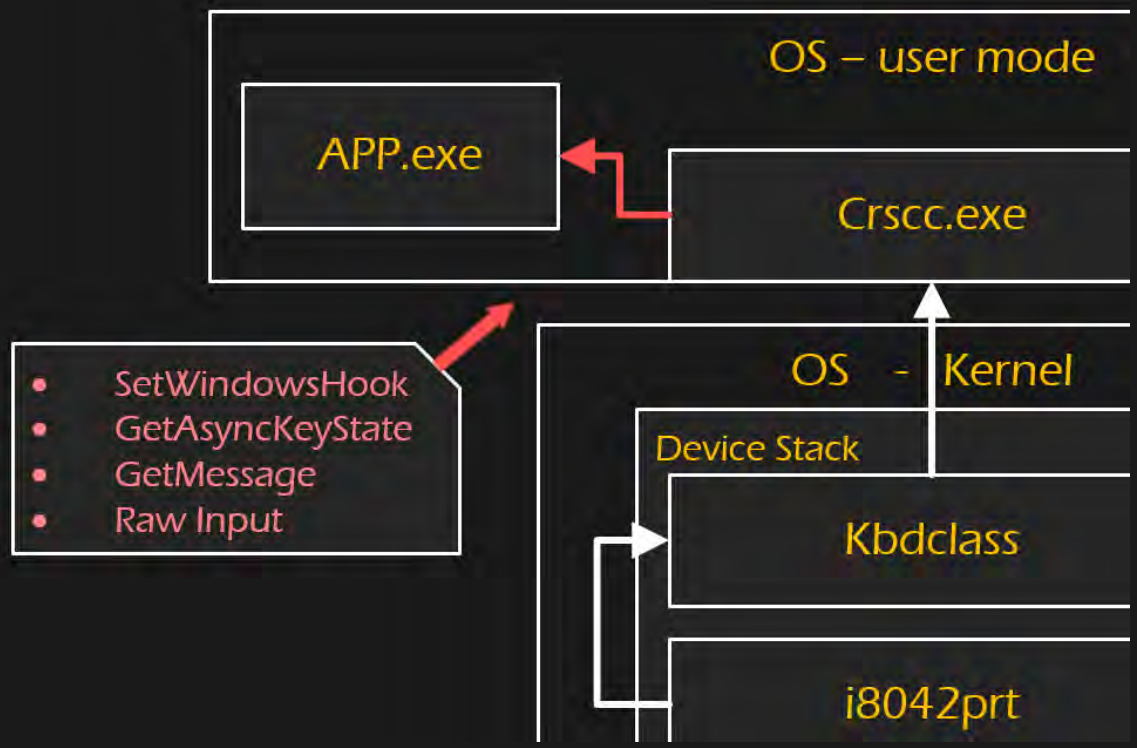
As close as possible to the hardware

Jamming keyloggers

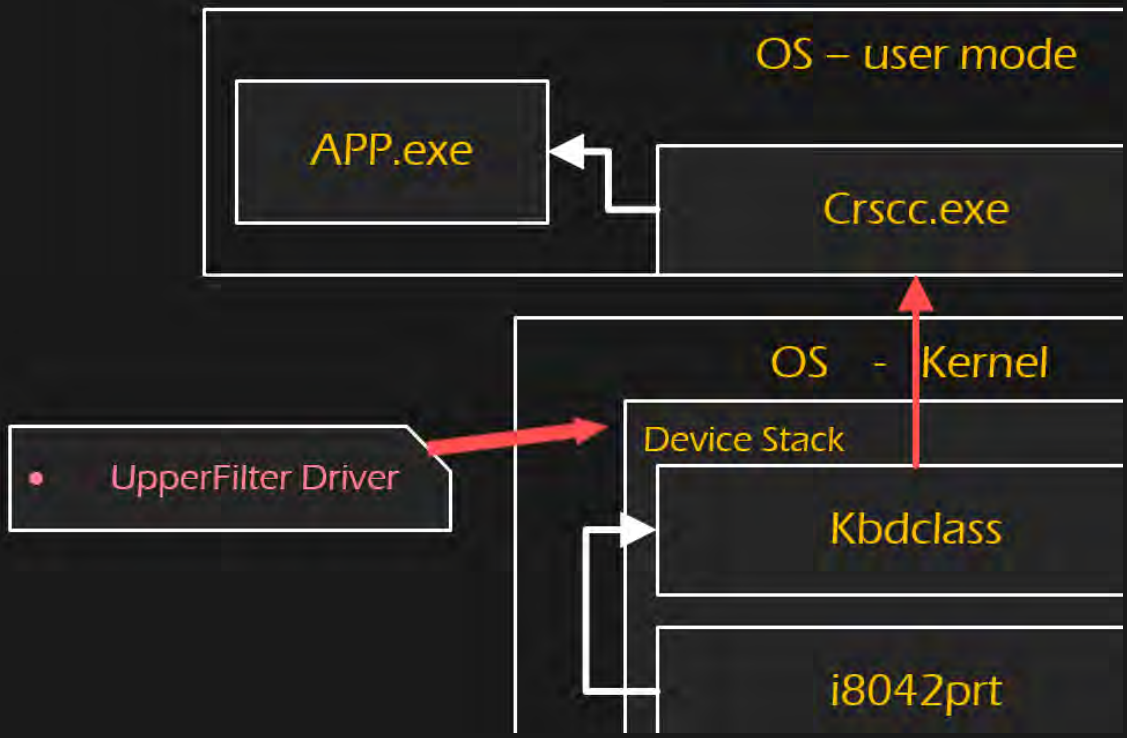
Basic Understanding



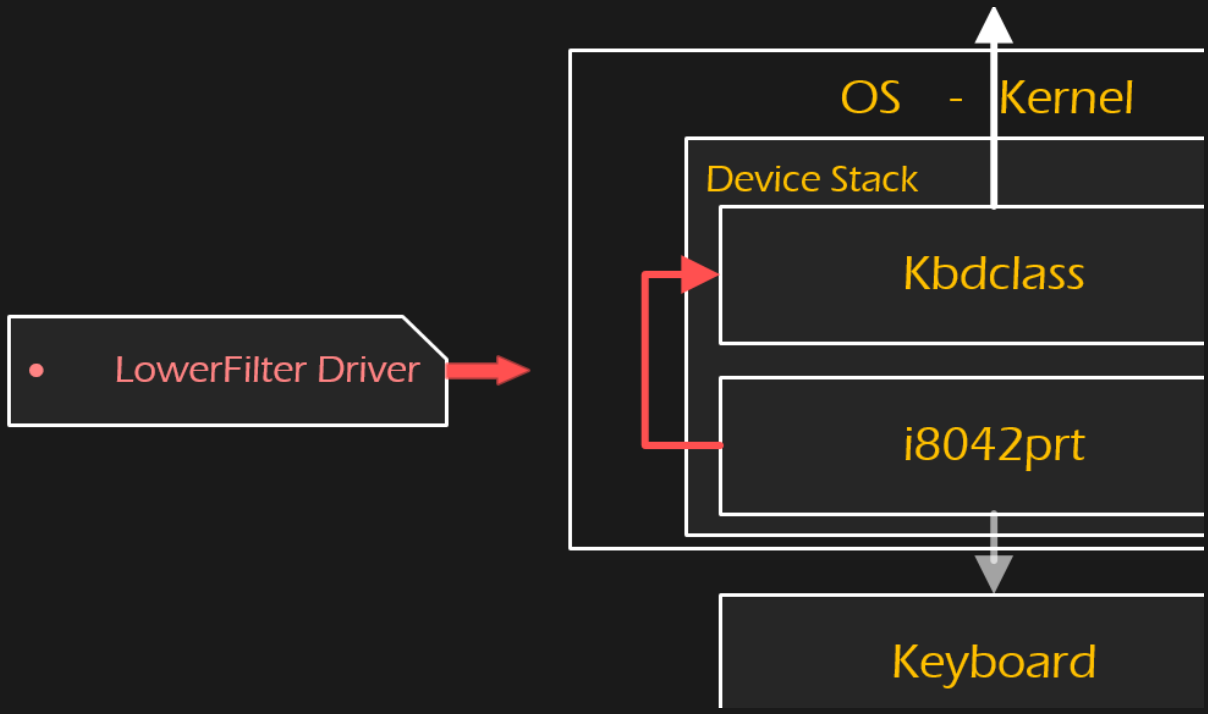
Basic Understanding



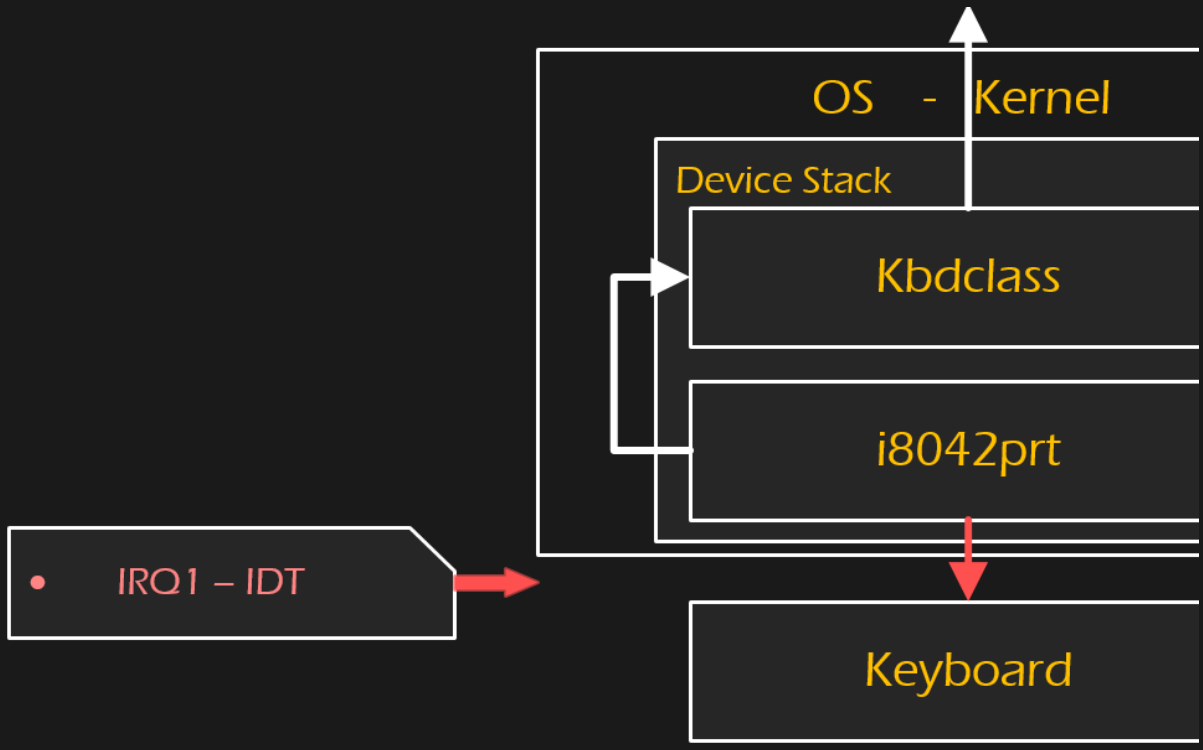
Basic Understanding



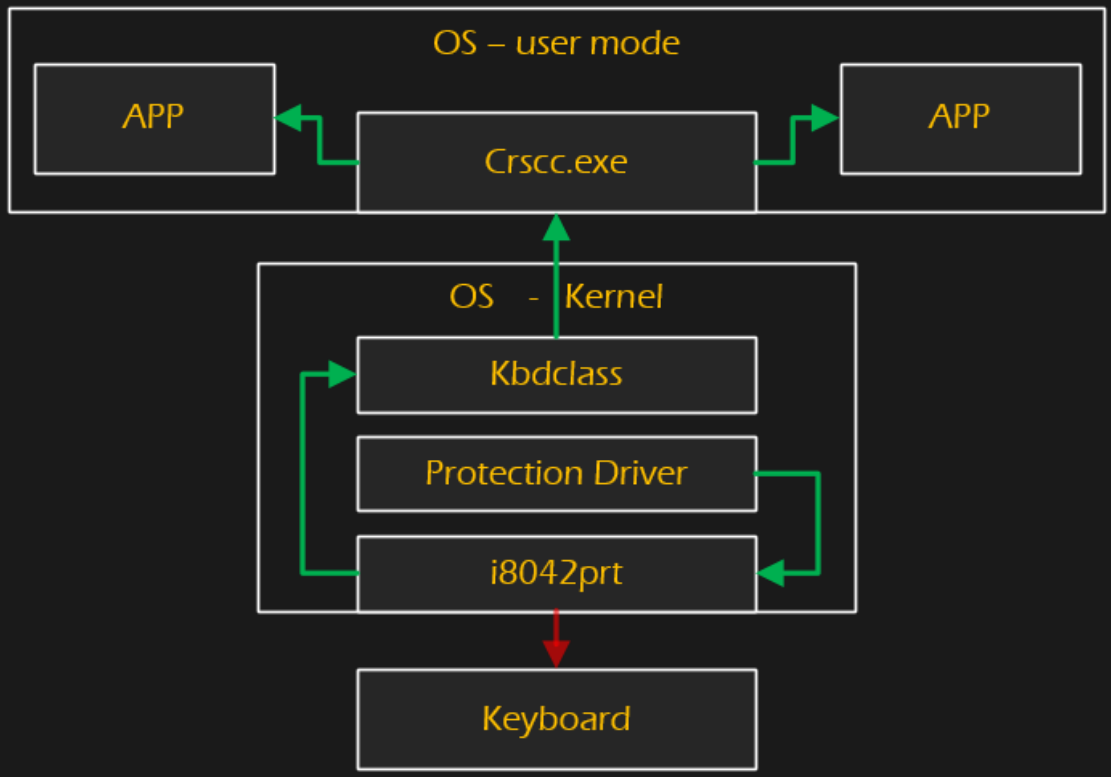
Basic Understanding



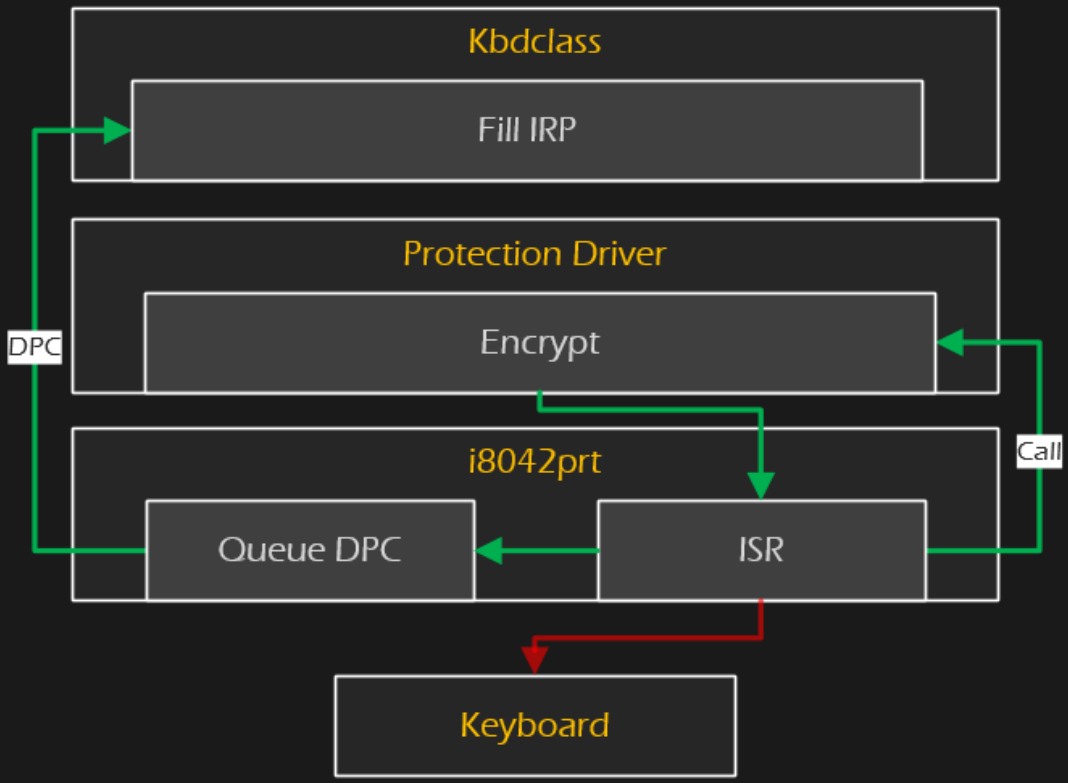
Basic Understanding



Basic Understanding



Keyboard driver stack



Encryption

Problematic

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

Encryption

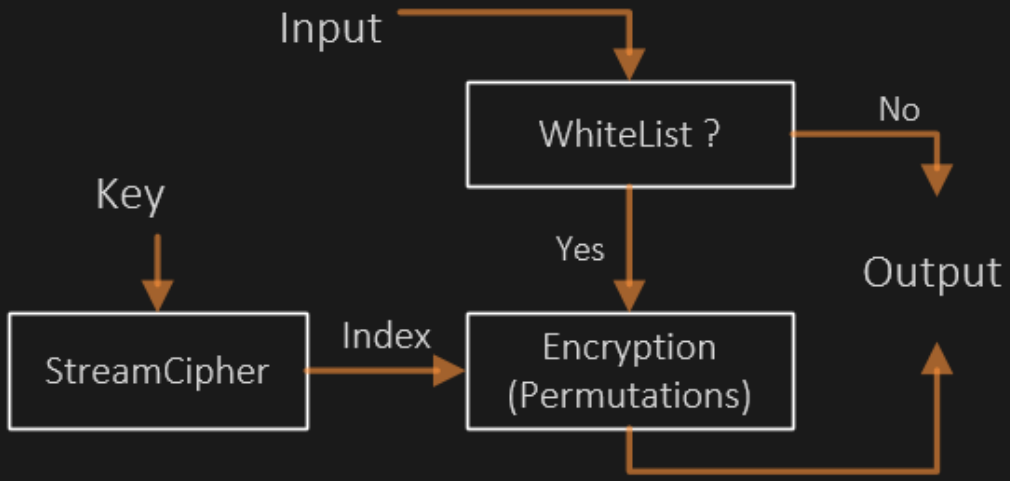
White list system for input decision

Encryption

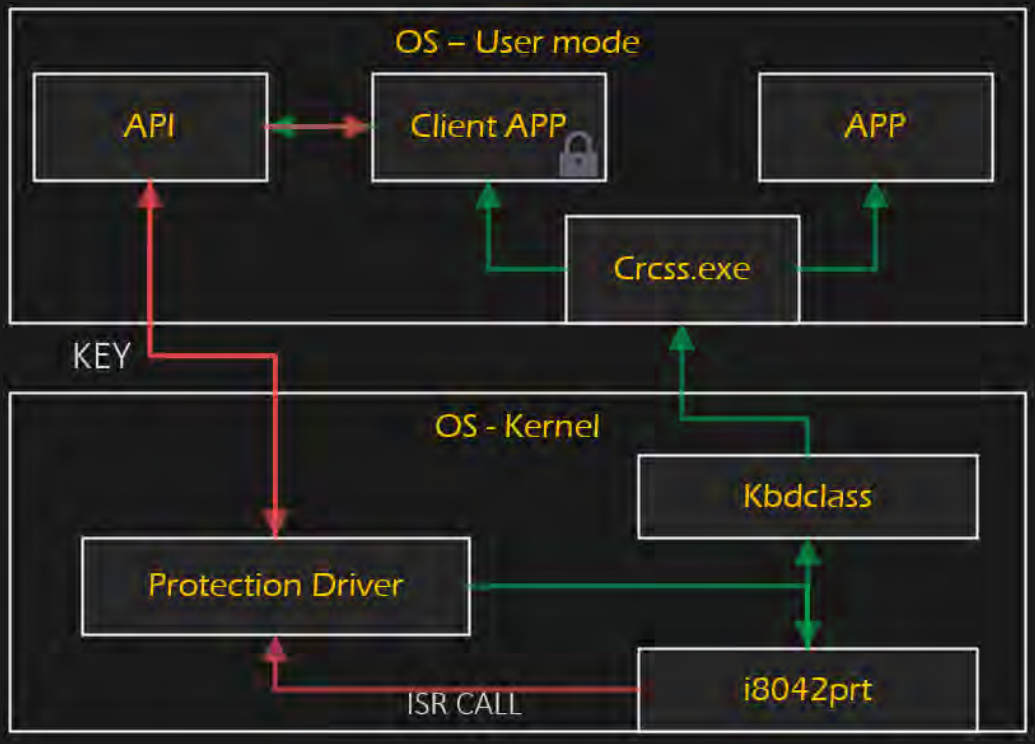
Solution : Jamming

- 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

Encryption Scheme



API-Driver Communication



Protection of the protection

- Monitoring of the keyboard driver stack
- Protection against DLL injection of the API
- Monitoring of the registry

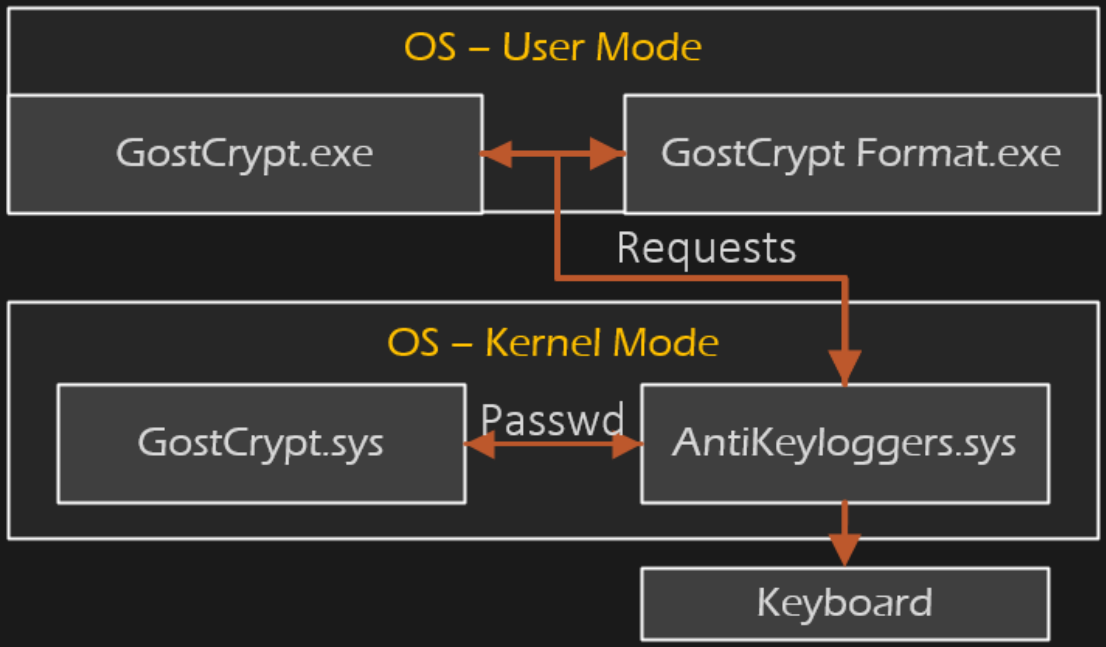
Is it working ?

Endless possibilities

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

GostCrypt

a full ring 0 password version



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 . . .

paul.amicelli@gostcrypt.org - baptiste.david@gostcrypt.org