

Reveal the Hidden!

Signature and Behavioral & malware analysis techniques



UNIVERSITÉ
Grenoble
Alpes

Grenoble
ENSIMAG

Reveal the Hidden!

Signature and Behavioral & malware analysis techniques

Authors:

Federico Turrin

Leonardo Antichi

Academic year:

2017-2018



UNIVERSITÉ
**Grenoble
Alpes**



What is a Keylogger?

A keylogger is a software or hardware device that can capture everything that is written from the keyboard.

We will present:

- A software keylogger developed in C for the Windows environment.

And show:

- How standard antivirus solutions will react to our project?

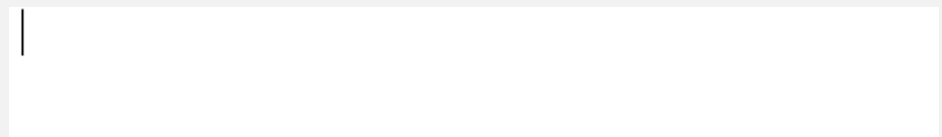
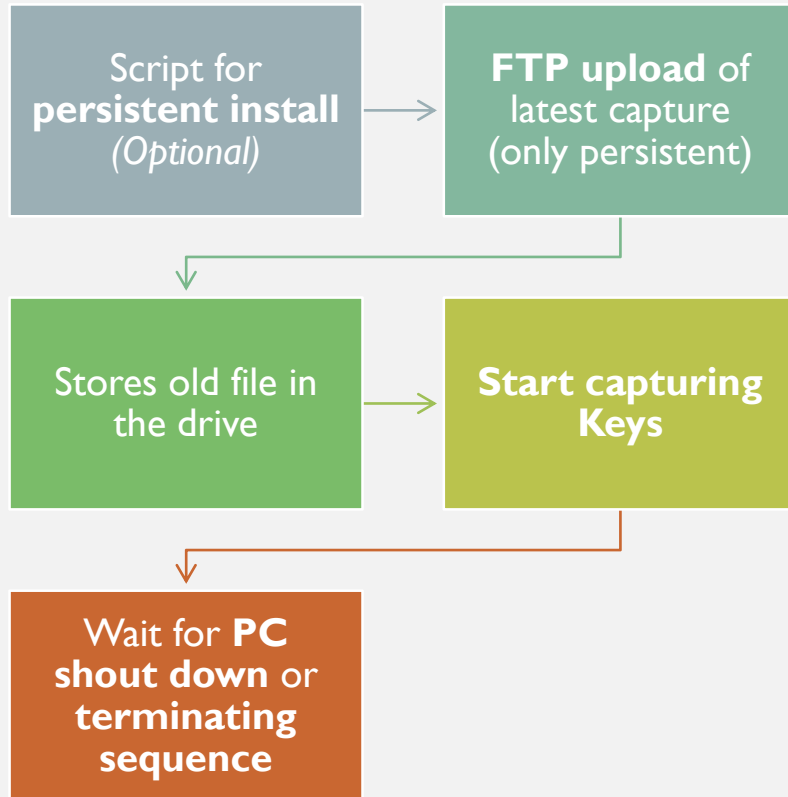


Main features

- ✓ Runs in ***stealth mode***
- ✓ **Compatibility** with every key and every keyboard layout
- ✓ *Persistent* or *portable* operation mode
- ✓ **Auto-lunch** at windows start-up
- ✓ Multiple and Dynamic *log storage*
- ✓ Automatic **FTP upload**
- ✓ **Invisibility** to *signature* antivirus
- ✓ **Code obfuscation**

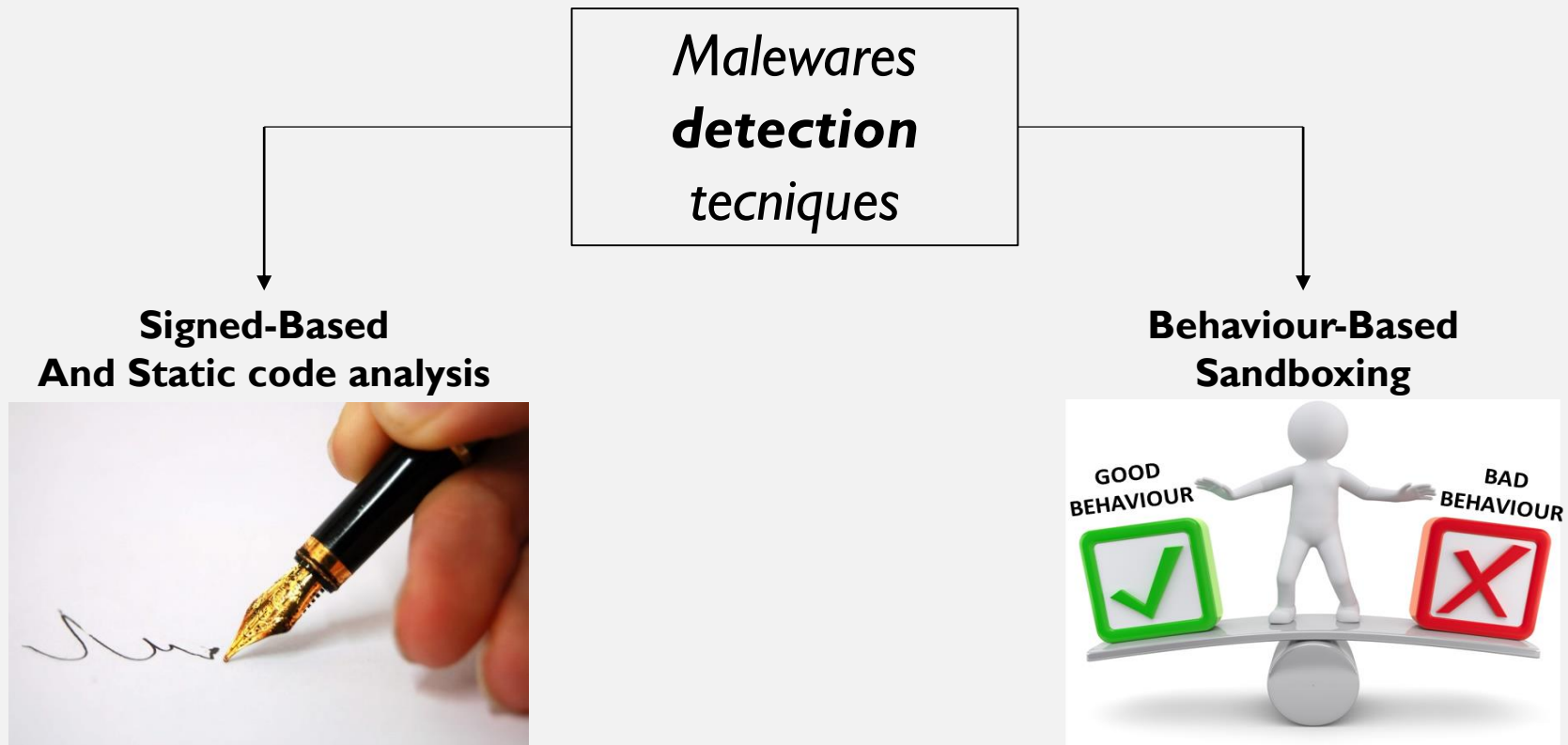


How it works?



Antivirus

No general definition but, nevertheless, we can distinguish two main kind of malware detection:



Antivirus SIGN-BASED



Detection based mainly on the Hash of the file, using also additional heuristic and more advanced features.

PROs:



Immediate recognition



Database with a great history...

CONs:



Can't detect Polymorphic code



... But it requires continuous updating



Impossibility to recognize new viruses

New antiviruses benefit of *advanced* **heuristic** feature for function recognition and **static code analysis**



Antivirus BEHAVIOUR-BASED

Behavioral detection based on sandboxing of malware

PROs:



Recognizes viruses even if not present in the database



Can find viruses based on polymorphic code

CONs:



A single suspicious attribute might not be enough to flag the file as malicious...



Can inadvertently flag legitimate files as malicious



A scan can required several times (120-300sec)



Antivirus Recognition

For each stage, scan where performed with VirusTotal, Eset Heuristic scan, VirusTotal Sandbox, lobit sandbox, Vichex Sandbox, Tencent HABO

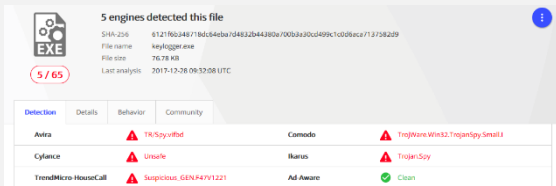
Signed-Based analysis

Malwares detection techniques

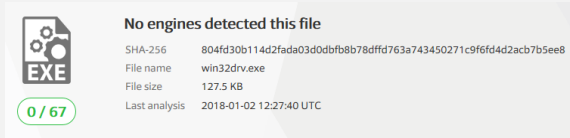
Behaviour-Based Sandboxing



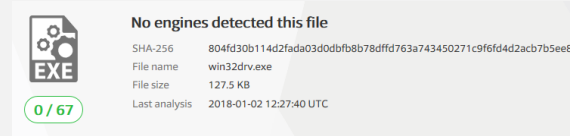
ALPHA VERSION:
5/65 Detection



BETA VERSION:
0/67 Detection
CLEAN!



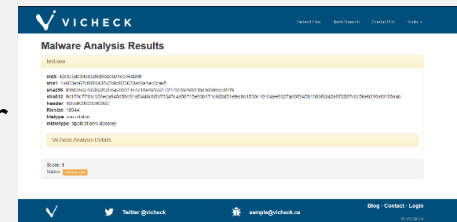
FINAL VERSION:
0/67 Detection
CLEAN!



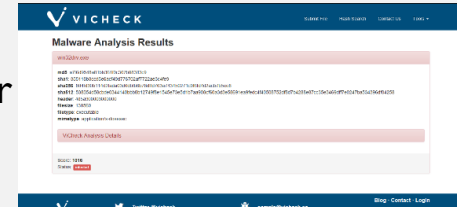
ALPHA VERSION:
ALL CLEAN



BETA VERSION:
SUSPICIOUS only for
ViCheck





FINAL VERSION:
INFECTED ONLY for
ViCheck



Can we have more, for free?

The first time ViCheck got us, but, by only switching platform compiling the program is not able anymore to recognize our malware.

	Project1.exe SHA256: a4a48c75088ab0eac078f6343e7edb04b8bdc7d9c5488455067705d41a001c69	153.09 KB
	Project1.exe SHA256: b29ddaf42fd636d07322402543b8258dfc3736a7fdc97fa210f7f7582fef1dd6	130.56 KB

By the way, who use 32 bit anymore?

32bit

Project1.exe

md5: d2a4fe5b626dc5665c181e9b1d9b42a8
sha1: dba62f804981187ed5c1c8e7b5ebe3d3d0dc1d66
sha256: b29ddaf42fd636d07322402543b8258dfc3736a7fdc97fa210f7f7582fef1dd6
sha512: 961f309778767753459402c94c918420a18b1f06e5c1384dae330d3cedec29d9afaa18c009f5cb20fee0d380d8ba6e591acc4249f
header: 4d5a900003000000
filesize: 130560
filetype: executable
mimetype: application/x-dosexec

ViCheck Analysis Details

Score: 1016
Status: infected

64bit

Project1.exe

md5: 56106be24d09d4da59524713c2342287
sha1: dbcb36d73fe3b3303f1482053bf43d6c123da0a5
sha256: a4a48c75088ab0eac078f6343e7edb04b8bdc7d9c5488455067705d41a001c69
sha512: 3cecd3ab2804ad74aaca850ccdfaf17cb80e71e80f26ebe1e10ebcc5141c1a64374d828225f3e1f8700ce8604680d03d34745753ba2c7a65d70dce481341719
header: 4d5a900003000000
filesize: 153088
filetype: executable
mimetype: application/x-dosexec

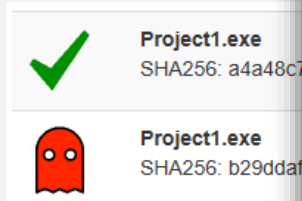
ViCheck Analysis Details

Score: 6
Status: clean

Can we have more, for free?

The first time ViCheck got the program is not able anymore

from compiling the



153.09 KB

130.56 KB

way, who use 32 bit anymore?

32bit

Project1.exe

md5: d2a4fe5b626dc5665c181e9b1d9b42a8
sha1: dba62f804981187ed5c1c8e7b5ebe3d3d0dc1d66
sha256: b29ddaf42fd636d07322402543b8258dfc3736a7f97fa210f7f7582fef1dd6
sha512: 961f309778767753459402c94c918420a18b1f06e5c1384dae330d3cedec29d9afaa18c009f5cb20fee0d380d8ba6e591acc4249f
header: 4d5a900003000000
filesize: 130560
filetype: executable
mimetype: application/x-dosexec

ViCheck Analysis Details

Score: 1016
Status: infected

sha512: 3cecd3ab2804ad74aaca850ccdfaf17cb80e71e80f26ebe1e10ebcc5141c1a64374d828225f3e1f8700ce8604680d03d34745753ba2c7a65d70dce481341719
header: 4d5a900003000000
filesize: 153088
filetype: executable
mimetype: application/x-dosexec

ViCheck Analysis Details

Score: 6
Status: clean

WDC WD WD

SAMSUNG UNG

Hitachi

Maxtor

SEAGATE

WDC WD

TOSHIBA

Thank You for listening!

Any question?