Unprotect

[Project]

botconf2016

The botnet fighting conference

30 NOVEMBER - 2 DECEMBER 2016

LYON - FRANCE

4th edition

Unprotect Project

How to Defeat Malware Protection?

@fr0gger_

TM

Thomas ROCCIA | McAfee Foundstone

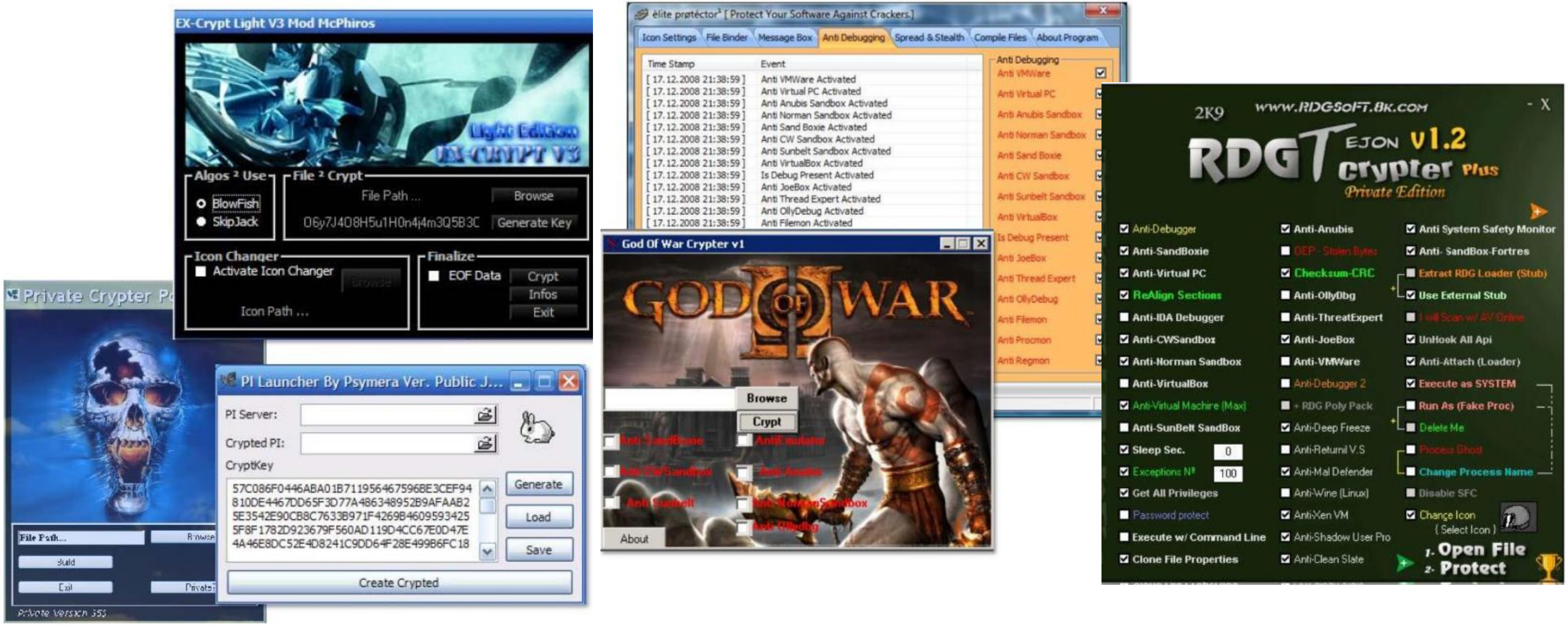
Whoami

- Thomas Roccia | @fr0gger_
- French Security Consultant Researcher Working at McAfee Foundstone
  - Malware Fighting
  - Incident Response
  - Threat Intelligence
  - Red Team
  - Assessment
  - Education

90%

Malware with self-defense and protection capabilities collected

Many tools are available…



06y7J408H5u1H0n4j4m3Q5B3C

```
Time Stamp                Event
[ 17.12.2008 21:38:59 ]   Anti VMWare Activated
[ 17.12.2008 21:38:59 ]   Anti Virtual PC Activated
[ 17.12.2008 21:38:59 ]   Anti Anubis Sandbox Activated
[ 17.12.2008 21:38:59 ]   Anti Norman Sandbox Activated
[ 17.12.2008 21:38:59 ]   Anti Sand Boxie Activated
[ 17.12.2008 21:38:59 ]   Anti CW Sandbox Activated
[ 17.12.2008 21:38:59 ]   Anti Sunbelt Sandbox Activated
[ 17.12.2008 21:38:59 ]   Anti VirtualBox Activated
[ 17.12.2008 21:38:59 ]   Is Debug Present Activated
[ 17.12.2008 21:38:59 ]   Anti JoeBox Activated
[ 17.12.2008 21:38:59 ]   Anti Thread Expert Activated
[ 17.12.2008 21:38:59 ]   Anti OllyDebug Activated
[ 17.12.2008 21:38:59 ]   Anti Filemon Activated
```

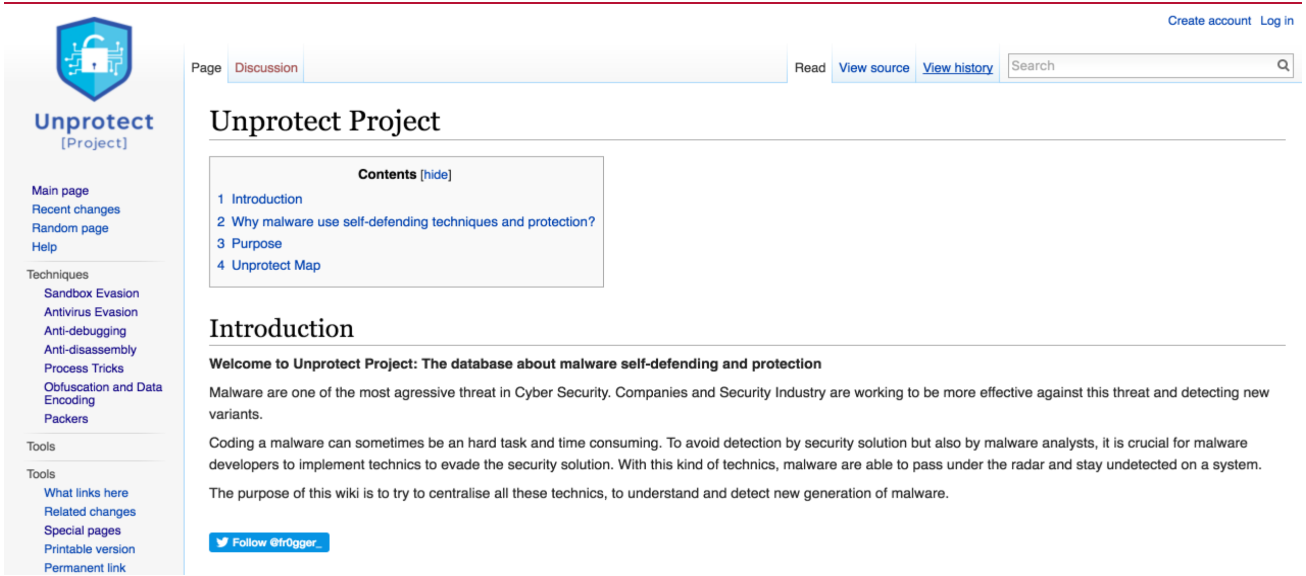
Anti Debugging
- Anti VMWare ☑
- Anti Virtual PC ☑
- Anti Anubis Sandbox ☑
- Anti Norman Sandbox ☑
- Anti Sand Boxie ☑
- Anti CW Sandbox ☑
- Anti Sunbelt Sandbox ☑
- Anti VirtualBox ☑
- Is Debug Present ☑
- Anti JoeBox ☑
- Anti Thread Expert ☑
- Anti OllyDebug ☑
- Anti Filemon ☑
- Anti Procmon ☑
- Anti Regmon ☑

```
57C086F0446ABA01B711956467596BE3CEF94
810DE4467DD65F3D77A486348952B9AFAAB2
5E3542E90CB8C7633B971F4269B4609593425
5F8F1782D923679F560AD119D4CC67E0D47E
4A46E8DC52E4D8241C9DD64F28E499B6FC18
```

- ☑ Anti-Debugger
- ☑ Anti-SandBoxie
- ☑ Anti-Virtual PC
- ☑ ReAlign Sections
- □ Anti-IDA Debugger
- ☑ Anti-CWSandbox
- ☑ Anti-Norman Sandbox
- □ Anti-VirtualBox
- ☑ Anti-Virtual Machine (Max)
- □ Anti-SunBelt SandBox
- ☑ Sleep Sec. 0
- ☑ Exceptions Nº 100
- ☑ Get All Privileges
- □ Password protect
- □ Execute w/ Command Line
- ☑ Clone File Properties
- ☑ Anti-Anubis
- □ OEP - Stolen Bytes
- ☑ Checksum-CRC
- □ Anti-OllyDbg
- □ Anti-ThreatExpert
- ☑ Anti-JoeBox
- □ Anti-VMWare
- □ Anti-Debugger 2
- □ + RDG Poly Pack
- ☑ Anti-Deep Freeze
- □ Anti-Returnil V.S
- ☑ Anti-Mal Defender
- □ Anti-Wine (Linux)
- ☑ Anti-Xen VM
- ☑ Anti-Shadow User Pro
- ☑ Anti-Clean Slate
- ☑ Anti System Safety Monitor
- ☑ Anti- SandBox-Fortres
- □ Extract RDG Loader (Stub)
- ☑ Use External Stub
- □ I will Scan w/ AV Online
- ☑ UnHook All Api
- ☑ Anti-Attach (Loader)
- ☑ Execute as SYSTEM
- □ Run As (Fake Proc)
- □ Delete Me
- □ Process Ghost
- □ Change Process Name
- □ Disable SFC
- ☑ Change Icon (Select Icon)

unprotect.tdgt.org

"One place to have an overview of malware self-defense and protection…"



Unprotect Project

Introduction

Welcome to Unprotect Project: The database about malware self-defending and protection

Malware are one of the most agressive threat in Cyber Security. Companies and Security Industry are working to be more effective against this threat and detecting new variants.

Coding a malware can sometimes be an hard task and time consuming. To avoid detection by security solution but also by malware analysts, it is crucial for malware developers to implement technics to evade the security solution. With this kind of technics, malware are able to pass under the radar and stay undetected on a system.

The purpose of this wiki is to try to centralise all these technics, to understand and detect new generation of malware.

Follow @fr0gger_

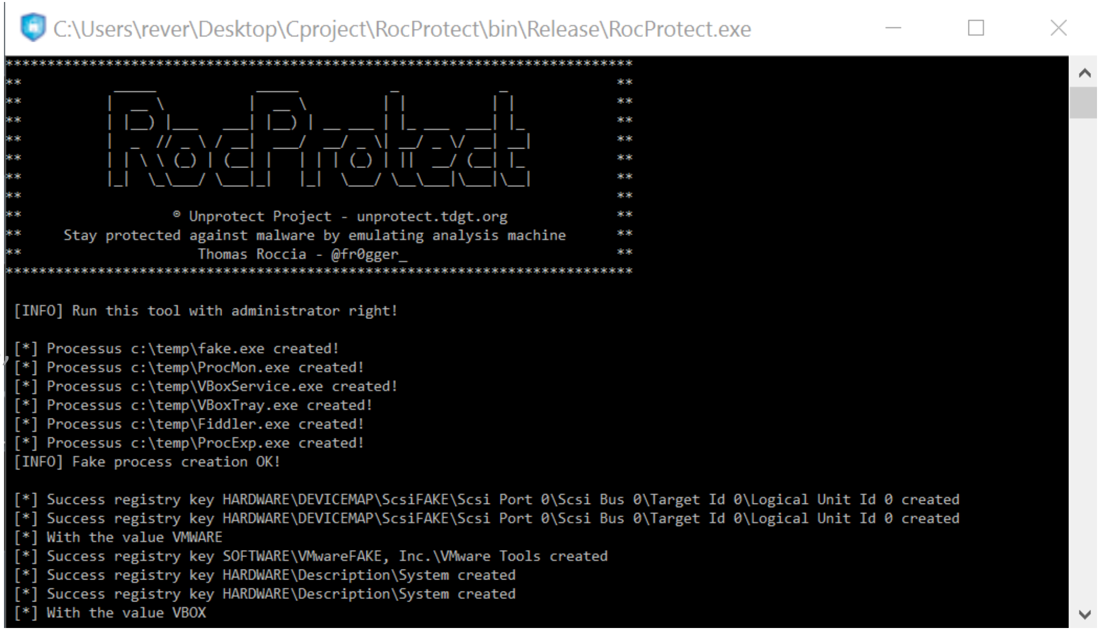
? *What’s happen if I create fake artifacts in my real machine?*

✓ *YES! If a malware detects my fake environment, it will not run and I will not get infected* ☺

A quick & dirty POC

Stay protected by emulating a malware analysis machine

- Coded in C++
- Create:
  - Fake registry keys of Vmware/VirtualBox/Qemu
  - Fake processes (VmwareTray.exe, VboxService.exe, wireshark.exe...)
  - Fake directories (Wine, Vmware Tools, VirtualBox Tools...)
  - Fake files (vmouse.sys, vboxhook.dll, VboxGuest.sys...)
  - Fake MAC address related to Vmware or VirtualBox



C:\Users\rever\Desktop\Cproject\RocProtect\bin\Release\RocProtect.exe

```
*************************************************************************************
**                                                                                 **
**            _____            _____           _            _                      **
**           |  __ \          |  __ \         | |          | |                     **
**           | |__) |___   ___| |__) | __ ___ | |_ ___  ___| |_                    **
**           |  _  // _ \ / __|  ___/ '__/ _ \| __/ _ \/ __| __|                   **
**           | | \ \ (_) | (__| |   | | | (_) | ||  __/ (__| |_                    **
**           |_|  \_\___/ \___|_|   |_|  \___/ \__\___|\___|\__|                   **
**                                                                                 **
**                     © Unprotect Project - unprotect.tdgt.org                    **
**        Stay protected against malware by emulating analysis machine             **
**                          Thomas Roccia - @fr0gger_                              **
*************************************************************************************

 [INFO] Run this tool with administrator right!

 [*] Processus c:\temp\fake.exe created!
 [*] Processus c:\temp\ProcMon.exe created!
 [*] Processus c:\temp\VBoxService.exe created!
 [*] Processus c:\temp\VBoxTray.exe created!
 [*] Processus c:\temp\Fiddler.exe created!
 [*] Processus c:\temp\ProcExp.exe created!
 [INFO] Fake process creation OK!

 [*] Success registry key HARDWARE\DEVICEMAP\ScsiFAKE\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0 created
 [*] Success registry key HARDWARE\DEVICEMAP\ScsiFAKE\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0 created
 [*] With the value VMWARE
 [*] Success registry key SOFTWARE\VMwareFAKE, Inc.\VMware Tools created
 [*] Success registry key HARDWARE\Description\System created
 [*] Success registry key HARDWARE\Description\System created
 [*] With the value VBOX
```

Thank you

- Thomas Roccia
- thomas.roccia [at] intel.com
- @fr0gger_

unprotect.tdgt.org

Unprotect

[Project]