



# Unprotect [Project]

## Unprotect Project

How to Defeat Malware Protection?



@fr0gger\_

Thomas ROCCIA | McAfee Foundstone

**botconf2016**

The botnet fighting conference

30 NOVEMBER - 2 DECEMBER 2016

LYON - FRANCE



4<sup>th</sup> edition

TM

# 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...



# unprotect.tdgt.org

“One place to have an overview of malware self-defense and protection...”



The screenshot shows the main page of the Unprotect Project wiki. At the top right, there are links for "Create account" and "Log in". Below these is a search bar with the text "Search" and a magnifying glass icon. The page title is "Unprotect Project". Underneath the title is a "Contents" section with a "[hide]" link, listing four items: "1 Introduction", "2 Why malware use self-defending techniques and protection?", "3 Purpose", and "4 Unprotect Map". The main heading is "Introduction", followed by a sub-heading "Welcome to Unprotect Project: The database about malware self-defending and protection". The text below explains that malware is a major threat in Cyber Security and that the project aims to centralize information on self-defending techniques. At the bottom of the page, there is a blue button that says "Follow @tr0gger\_". On the left side of the page, there is a sidebar with the Unprotect Project logo (a blue shield with a padlock) and a list of navigation links: "Main page", "Recent changes", "Random page", "Help", "Techniques" (with sub-links for Sandbox Evasion, Antivirus Evasion, Anti-debugging, Anti-disassembly, Process Tricks, Obfuscation and Data Encoding, and Packers), "Tools", and "What links here" (with sub-links for Related changes, Special pages, Printable version, and Permanent link).



*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/Quemu
- 🦠 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
*****
**                                                                    **
**               RooProtect               **
**                                                                    **
**               © 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](mailto:thomas.roccia@intel.com)
- @fr0gger\_

[unprotect.tdgt.org](http://unprotect.tdgt.org)



# Unprotect

[Project]