Unprotect
[Project]

botconf2016
The botnet fighting conference
30 NOVEMBER - 2 DECEMBER 2016
LYON - FRANCE
4th edition

Unprotect Project

How to Defeat Malware Protection?

@fr0gger_

Thomas ROCCIA | McAfee Foundstone

TM

Whoami

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

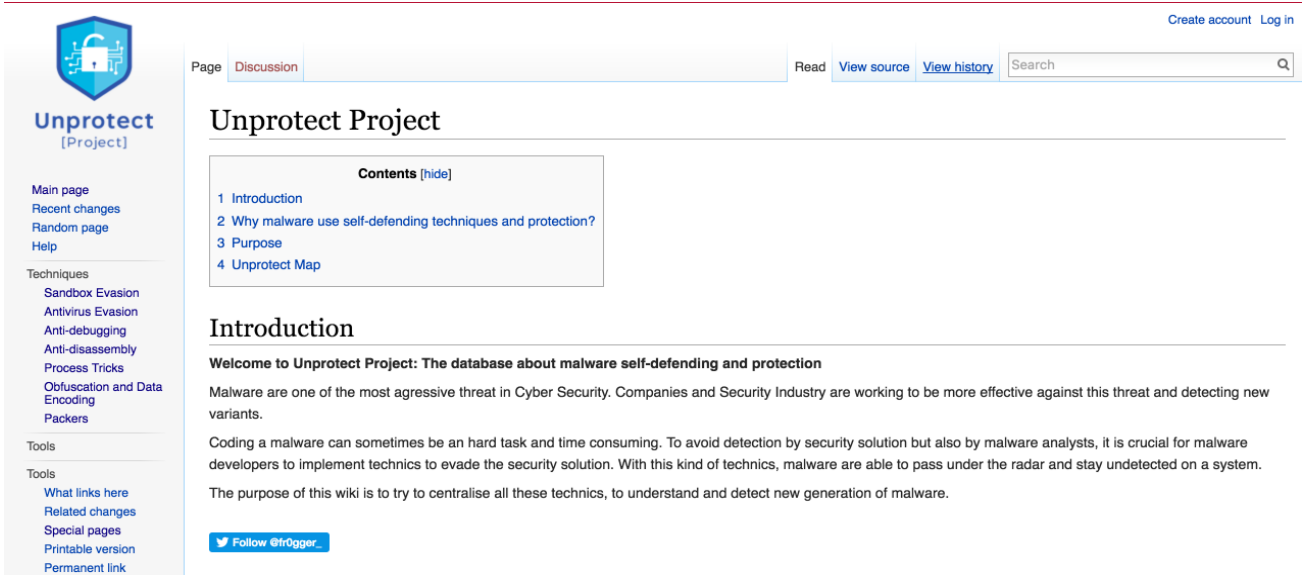
90%

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…"



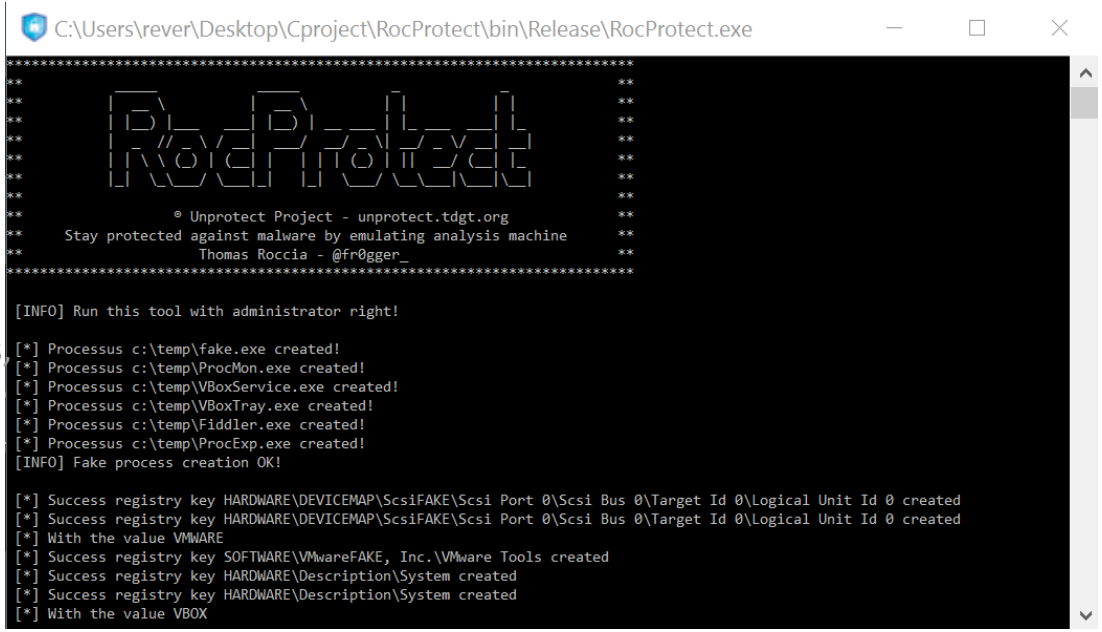
What's happen if I create fake artifacts in my real machine?

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



Thank you

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

Unprotect
[Project]

unprotect.tdgt.org