Sandbox Best Practices Cheat Sheet

Unprotect [Project] – unprotect.tdgt.org

Thomas Roccia | @fr0gger

VMWARE

Change the default Mac Address. Default first 3 bytes of Mac Address of VMware:

00:0C:29	00:1C:14
00:50:56	00:05:69

Change or remove the following registry keys:

HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0\“Identifier”;“VMWARE”
HKLM\SOFTWARE\VMware, Inc.\VMware Tools
HKLM\HARDWARE\Description\System\ "SystemBiosVersion";"VMWARE"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\ Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\DriverDesc\“Vmware SCSI Controller”
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\ Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\ProviderName\“VMware, Inc.”

Check the name or remove the following processes:

VMwareService.exe
Vmwaretray.exe
TPAutoConnSvc.exe
Vmtoolsd.exe
Vmwareuser.exe

Check the name of default paths or files:

system32\drivers\vmmouse.sys
system32\drivers\vmhgfs.sys
Program Files\VMware

VIRTUALBOX

Change the default Mac Address. Default first 3 bytes of Mac Address of VirtualBox:

08:00:27

Change or remove the following registry keys:

HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0\"Identifier";"VBOX"
HKLM\HARDWARE\Description\System\"SystemBiosVersion";VBOX
HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions
HKLM\HARDWARE\Description\System\"VideoBiosVersion"; "VIRTUALBOX"
HKLM\HARDWARE\ACPI\DSDT\VBOX__
HKLM\HARDWARE\ACPI\FADT\VBOX__
HKLM\HARDWARE\ACPI\RSDT\VBOX__
HKLM\HARDWARE\Description\System\“SystemBiosDate"; "06/23/99"
HKLM\SYSTEM\ControlSet001\Services\VBoxGuest
HKLM\SYSTEM\ControlSet001\Services\VBoxService
HKLM\SYSTEM\ControlSet001\Services\VBoxMouse
HKLM\SYSTEM\ControlSet001\Services\VBoxVideo

Check the name or remove the following processes:

vboxservice.exe
vboxtray.exe
vboxcontrol.exe

Check the name of default paths or files:

C:\WINDOWS\system32\drivers\VBoxMouse.sys
C:\WINDOWS\system32\drivers\VBoxGuest.sys
C:\WINDOWS\system32\drivers\VBoxSF.sys
C:\WINDOWS\system32\drivers\VBoxVideo.sys
C:\WINDOWS\system32\vboxdisp.dll
C:\WINDOWS\system32\vboxhook.dll
C:\WINDOWS\system32\vboxmrxnp.dll
C:\WINDOWS\system32\vboxogl.dll
C:\WINDOWS\system32\vboxoglarrayspu.dll
C:\WINDOWS\system32\vboxoglcrutil.dll
C:\WINDOWS\system32\vboxoglerrorspu.dll
C:\WINDOWS\system32\vboxoglfeedbackspu.dll
C:\WINDOWS\system32\vboxoglpackspu.dll
C:\WINDOWS\system32\vboxoglpassthroughspu.dll
Program Files\oracle\virtualbox guest additions\

QEMU

Change or remove the following registry keys:

HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0\"Identifier";"QEMU"
HKLM\HARDWARE\Description\System\ "SystemBiosVersion";"QEMU"

PARRALLELS

Check the name or remove the following processes:

prl_cc.exe
prl_tools.exe

VIRTUAL PC

Check the name or remove the following processes:

VMSrvc.exe
VMUSrvc.exe

CUCKOO

Check the name or remove the following processes:

Python.exe
Pythonw.exe

Check the name of default paths or files:

C:\cuckoo
\\\\.\\pipe\\cuckoo

XEN

Check the name or remove the following processes:

xenservice.exe

WINE

Change or remove the following registry key:

```
HKLM\SOFTWARE\Wine
```

BOCHS

Change or remove the following registry key:

```
HKLM\HARDWARE\Description\System\
"SystemBiosVersion";"BOCHS"
```

X86 INSTRUCTIONS

The following Assembly instructions are used to detect Virtual Environment:

SIDT
SGDT
SLDT
SMSW
STR
CPUID
IN
RDTSC

LOADED DLL

Sandboxes are loaded DLL to perform actions on the system. Malware are able to detect these DLL.
Check if the following DLL are loaded:

sbiedll.dll (Sandboxie)
dbghelp.dll (vmware)
api_log.dll (SunBelt SandBox)
dir_watch.dll (SunBelt SandBox)
pstorec.dll (SunBelt Sandbox)
vmcheck.dll (Virtual PC)
wpespy.dll (WPE Pro)

GENERIC DETECTION

Malware can detect a sandbox by different ways. The normal user activities should be reproducing to avoid detection.

Reproduce or change the following elements to avoid detection:

Mouse movement
Office recent files
Screen resolution
Wallpaper
Memory size
Hard drive size
Installed software
Hostname
USB drive
Printer
Number of processor

MANUAL ANALYSIS

Sandboxes can be used for automatic analysis but also for manual analysis.

Rename the following analysis tools (NB: all the analysis tools can be detected by malware with the original process name):

Wireshark.exe
Ollydbg.exe
ProcessHacker.exe
TCPview.exe
Autoruns.exe/Autorunsc.exe
filemon.exe
ProcMon.exe
regmon.exe
procexp.exe
HookExplorer.exe
SysInspector.exe
PETools.exe
DumpPcap.exe

TIMING ATTACKS

Malware can delay execution in order to avoid analysis or detection.

Onset delay: Malware will delay execution to avoid analysis by the sandbox.
Stalling code: Stalling code is typically executed before any malicious behaviour.
Extended sleep code: Most of the sandbox have a defined time for the analysis. Malware will use a Sleep function with a big time to avoid analysis by the sandbox.

TOOLS

Different tools exist to harden a sandbox.

Paranoid Fish: Pafish is a demonstration tool that employs several techniques to detect sandboxes and analysis environments in the same way as malware families do. https://github.com/a0rtega/pafish
Al-Khaser: Al-khaser is a PoC malware with good intentions that aims to stress your sandbox system. https://github.com/LordNoteworthy/al-khaser
RocProtect: RocProtect is a POC that emulates a sandbox environment to avoid infection by advanced malware. https://github.com/fr0gger/RocProtect-V1

Unprotect [Project]

Thomas Roccia | @fr0gger_
Version 1.0.