



Playing around with Fake CCleaner and Cuckoo

Jakarta, 20 Oktober 2017



Today's Agenda

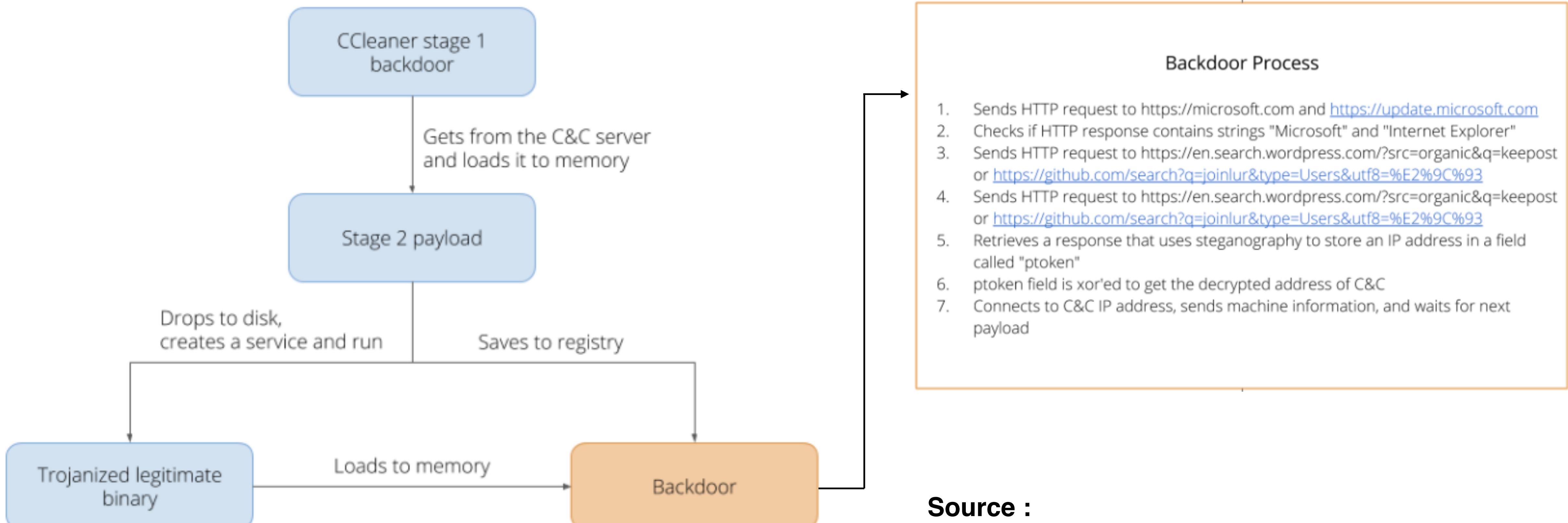
- ▶ Fake CCleaner Overview
- ▶ Clean CCleaner vs Malware CCleaner Comparison
- ▶ More on CCleaner Analysis
- ▶ CCleaner Malware Analysis Report
- ▶ Conclusions

Fake CCleaner Overview (1/3)

- ▶ On September 13, 2017 while conducting customer beta testing of our new exploit detection technology, Cisco Talos identified a specific executable which was triggering our advanced malware protection systems.
- ▶ Upon closer inspection, the executable in question was the installer for CCleaner v5.33, which was being **delivered to endpoints by the legitimate CCleaner download servers**.
- ▶ We identified that even though the downloaded installation executable was signed **using a valid digital signature** issued to Piriform, CCleaner was not the only application that came with the download.
- ▶ During the installation of CCleaner 5.33, the 32-bit CCleaner binary that was included also contained a malicious payload that featured a **Domain Generation Algorithm (DGA) as well as hardcoded Command and Control (C2) functionality**.

<http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>

Fake CCleaner Overview (2/3)



Source :

<http://www.intezer.com/evidence-aurora-operation-still-active-part-2-more-ties-uncovered-between-ccleaner-hack-chinese-hackers/>

Fake CCleaner Overview (3/3)

- ▶ Thanks to the continued work of the **Avast Threat Labs team and the help from US law enforcement personnel**.
- ▶ The server's **IP address was 216.126.225.163**, it featured **the same self-signed SSL certificate (issued for speccy.piriform.com)** and stack-wise, had a typical "LAMP" configuration: CentOS release 6.9 with Apache 2.2.15, PHP 5.3.3, but most importantly, a MySQL database that turned out to contain data going back to August 18
- ▶ Finding from Avast Team
 - The total number of connections to the CnC server was 5,686,677.
 - The total number of unique PCs (unique MAC addresses) that communicated with the CnC server was 1,646,536.
 - The total number of unique PCs that received the 2nd stage payload was 40

| Domain | Industry | Country | Number of impacted PCs |
|---|----------|-----------|------------------------|
| cht.com.tw | Telco | Taiwan | 13 |
| nsl.ad.nec.co.jp | Tech | Japan | 10 |
| samsung samsung.sk samsung.sepml | Tech | Korea | 5 |
| corpnet.asus paskey.corpnet.asus | Tech | Taiwan | 2 |
| ad.fip.fujitsu.com domain.ftsp.ten.fujitsu.com | Tech | Japan | 2 |
| am.sony.com | Tech | Japan | 2 |
| infoview2u.dvrdns.org | Internet | USA | 1 |
| uk.pri.o2.com | Telco | UK | 1 |
| gg.gauselmann.com | Gaming | Germany | 1 |
| singtel | Telco | Singapore | 1 |
| intel.com | Tech | USA | 1 |
| vmware.com | Tech | USA | 1 |

Source : <https://blog.avast.com/additional-information-regarding-the-recent-ccleaner-apt-security-incident>

What is Cuckoo ?



Cuckoo an Overview

Analysis Capability

- Registry Analysis
- Network Analysis
- Memory Analysis
- Process Analysis
- Dropped File Analysis
- Static Analysis

Analysis Packages

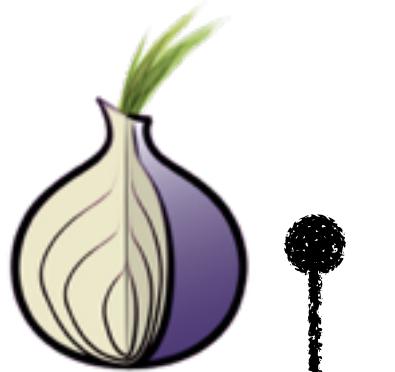
DLL, exe, .doc, HTML, PDF, PPT,
etc

Integration

- Suricata/Snort
- MITM Proxy

Network Analysis Routing

VPN, Non Routing, Inetsim



cuckoo



/* YARA */



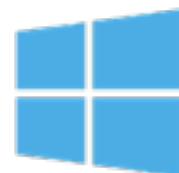
MISP
Threat Sharing



moloch

Malware Analysis Platform

Windows



Windows

Linux

Android



Sandbox Architecture

Virtualbox

- Virtualbox
- VMWare Workstation
- KVM
- Xen Server, etc

Scoring System

Playing Around Case

▶ Cuckoo VM Machine

- Cuckoo with No Anti-VM Guest using WinXP
- Cuckoo with Anti-VM Guest using WinXP (Generated using VMCloak)

▶ Cuckoo Parameter

- Timeout Parameter : normal (120 second), 1200 second, 10.000 second
- Routing : None routing, Tor

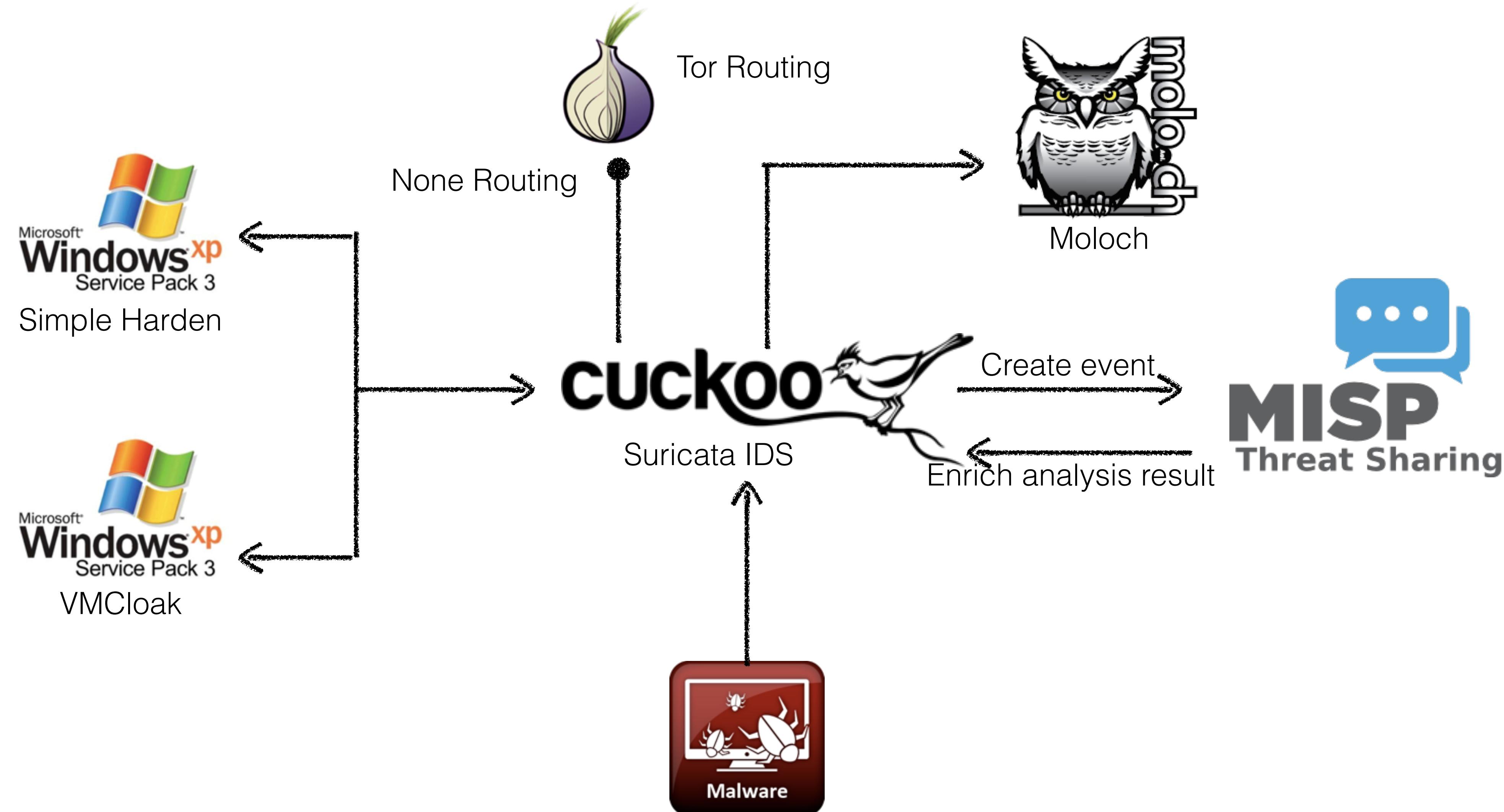
▶ Additional Cuckoo Features

- Full memory dump
- Suricata IDS
- MISP

▶ Submitted File

- Normal CCleaner 5.35
- CCleaner 5.33.6162 Setup.exe (<https://virustotal.com>)
- CCleaner 5.33.6162 Standalone Executable File (<https://www.reverse.it/>)
- Extracted Malware 5.33.6162 (@jaytezer, Jay Rosenberg)

Cuckoo Sandbox Schema



Guest OS [Windows XP SP3] in Virtual Box

```
C:\Documents and Settings\malwarelabs\My Documents\pafish.exe C:\Documents and Settings\malwarelabs\My Documents\pafish.exe C:\Documents and Settings\malwarelabs\My Documents\pafish.exe
* Pafish <Paranoid fish> *
Some anti(debugger/VM/sandbox) tricks
used by malware for the general public.

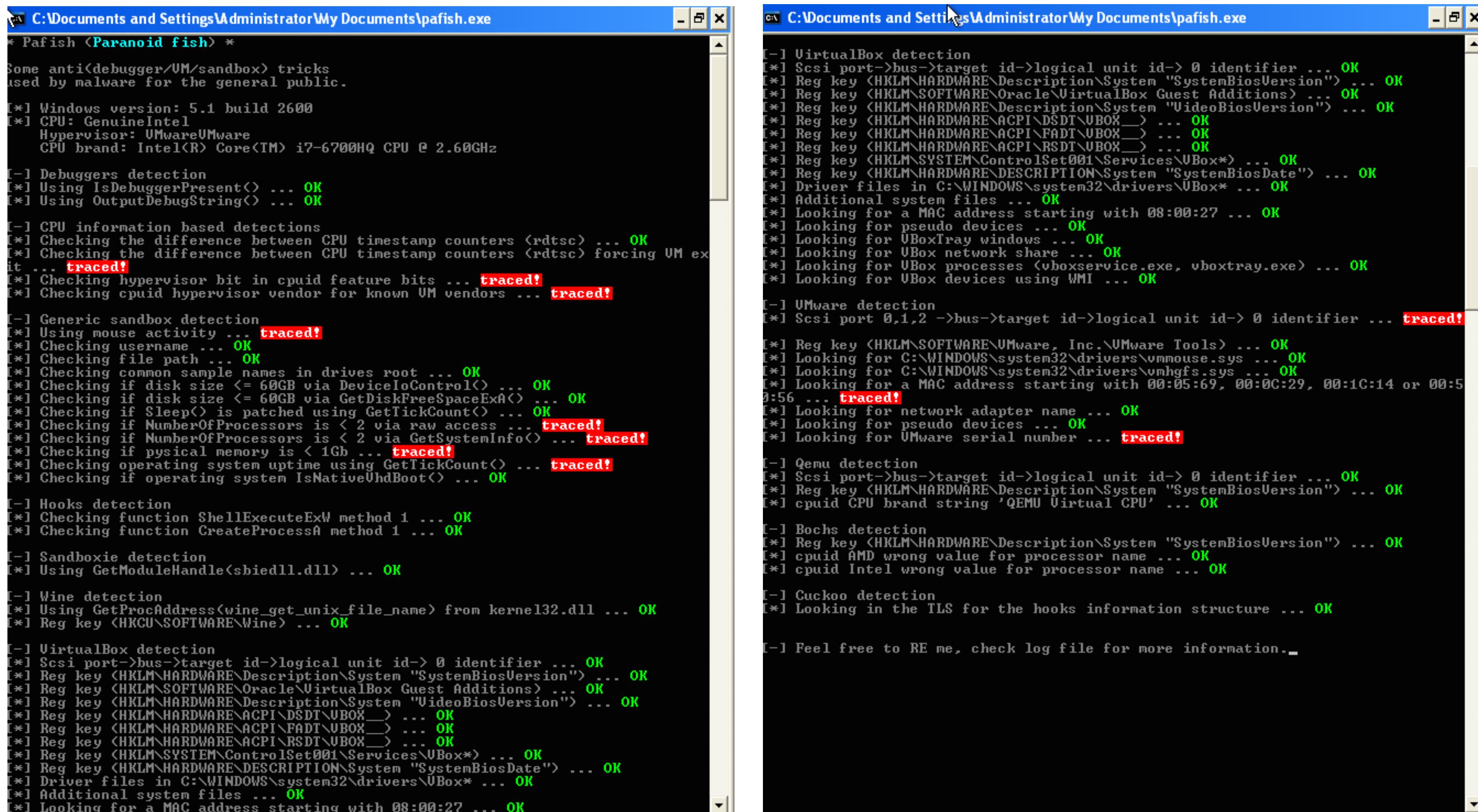
[*] Windows version: 5.1 build 2600
[*] CPU: GenuineIntel
    Hypervisor: UBoxUBoxUBox
    CPU brand: Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz
[-] Debuggers detection
[*] Using IsDebuggerPresent() ... OK
[*] Using OutputDebugString() ... OK
[-] CPU information based detections
[*] Checking the difference between CPU timestamp counter
it ... traced!
[*] Checking the difference between CPU timestamp counter
[*] Checking hypervisor bit in cpuid feature bits ... OK
[*] Checking cpuid hypervisor vendor for known VM vendor
[-] Generic sandbox detection
[*] Using mouse activity ... OK
[*] Checking username ... traced!
[*] Checking file path ... OK
[*] Checking common sample names in drives root ... OK
[*] Checking if disk size <= 60GB via DeviceIoControl()
[*] Checking if disk size <= 60GB via GetDiskFreeSpaceEx()
[*] Checking if Sleep() is patched using GetTickCount()
[*] Checking if NumberOfProcessors is < 2 via raw access
[*] Checking if NumberOfProcessors is < 2 via GetSystemInfo()
[*] Checking if physical memory is < 1Gb ... traced!
[*] Checking operating system uptime using GetTickCount()
[*] Checking if operating system IsNativeVhdBoot() ... OK
[-] Hooks detection
[*] Checking function ShellExecuteExW method 1 ... OK
[*] Checking function CreateProcessA method 1 ... OK
[-] Sandboxie detection
[*] Using GetModuleHandle(sbiedll.dll) ... OK
[-] Wine detection
[*] Using GetProcAddress(wine_get_unix_file_name) from k
[*] Reg key <HKCU\SOFTWARE\Wine> ... OK

[-] Wine detection
[*] Using GetProcAddress(wine_get_unix_file_name) from kernel
[*] Reg key <HKCU\SOFTWARE\Wine> ... OK
[-] VirtualBox detection
[*] Scsi port->bus->target id-> logical unit id-> 0 identified
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVer
[*] Reg key <HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions
[*] Reg key <HKLM\HARDWARE\Description\System "VideoBiosVers
[*] Reg key <HKLM\HARDWARE\ACPI\DSDT\UBOX_> ... OK
[*] Reg key <HKLM\HARDWARE\ACPI\FADT\UBOX_> ... OK
[*] Reg key <HKLM\HARDWARE\ACPI\RSDT\UBOX_> ... OK
[*] Reg key <HKLM\SYSTEM\ControlSet001\Services\UBox*> ... OK
[*] Reg key <HKLM\HARDWARE\DESCRIPTION\System "SystemBiosDat
[*] Driver files in C:\WINDOWS\system32\drivers\UBox* ...
[*] Additional system files ... OK
[*] Looking for a MAC address starting with 08:00:27 ... traced!
[*] Looking for pseudo devices ... OK
[*] Looking for UBoxTray windows ... OK
[*] Looking for UBox network share ... OK
[*] Looking for UBox processes <vboxservice.exe, vboxtray.exe
[*] Looking for UBox devices using WMI ... traced!
[-] Qemu detection
[*] Scsi port->bus->target id-> logical unit id-> 0 identified
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVer
[*] cpuid CPU brand string 'QEMU Virtual CPU' ... OK
[-] Bochs detection
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVer
[*] cpuid AMD wrong value for processor name ... OK
[*] cpuid Intel wrong value for processor name ... OK
[-] Cuckoo detection
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vhgfs.sys ... OK
[*] Looking in the TLS for the hooks information structure
[-] Feel free to RE me, check log file for more information
[*] Looking for network adapter name ... OK
[*] Looking for pseudo devices ... OK
[*] Looking for VMware serial number ... OK
[-] Qemu detection
[*] Scsi port->bus->target id-> logical unit id-> 0 identified
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVer
[*] cpuid CPU brand string 'QEMU Virtual CPU' ... OK
[-] Bochs detection
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVer
[*] cpuid AMD wrong value for processor name ... OK
[*] cpuid Intel wrong value for processor name ... OK

[*] Looking for pseudo devices ... OK
[*] Looking for UBoxTray windows ... OK
[*] Looking for UBox network share ... OK
[*] Looking for UBox processes <vboxservice.exe, vboxtray.exe
[*] Looking for UBox devices using WMI ... traced!
[-] Qemu detection
[*] Scsi port->bus->target id-> logical unit id-> 0 identified
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVer
[*] cpuid CPU brand string 'QEMU Virtual CPU' ... OK
[-] Bochs detection
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVer
[*] cpuid AMD wrong value for processor name ... OK
[*] cpuid Intel wrong value for processor name ... OK

[-] VMware detection
[*] Scsi port 0,1,2 ->bus->target id-> logical unit id-> 0 identified
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVer
[*] cpuid CPU brand string 'QEMU Virtual CPU' ... OK
[-] Cuckoo detection
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vhgfs.sys ... OK
[*] Looking in the TLS for the hooks information structure
[-] Feel free to RE me, check log file for more information
[*] Looking for network adapter name ... OK
[*] Looking for pseudo devices ... OK
[*] Looking for VMware serial number ... OK
[-] Qemu detection
[*] Scsi port->bus->target id-> logical unit id-> 0 identified
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVer
[*] cpuid CPU brand string 'QEMU Virtual CPU' ... OK
[-] Bochs detection
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVer
[*] cpuid AMD wrong value for processor name ... OK
[*] cpuid Intel wrong value for processor name ... OK
```

VMCloak WinXP Result in VMWare

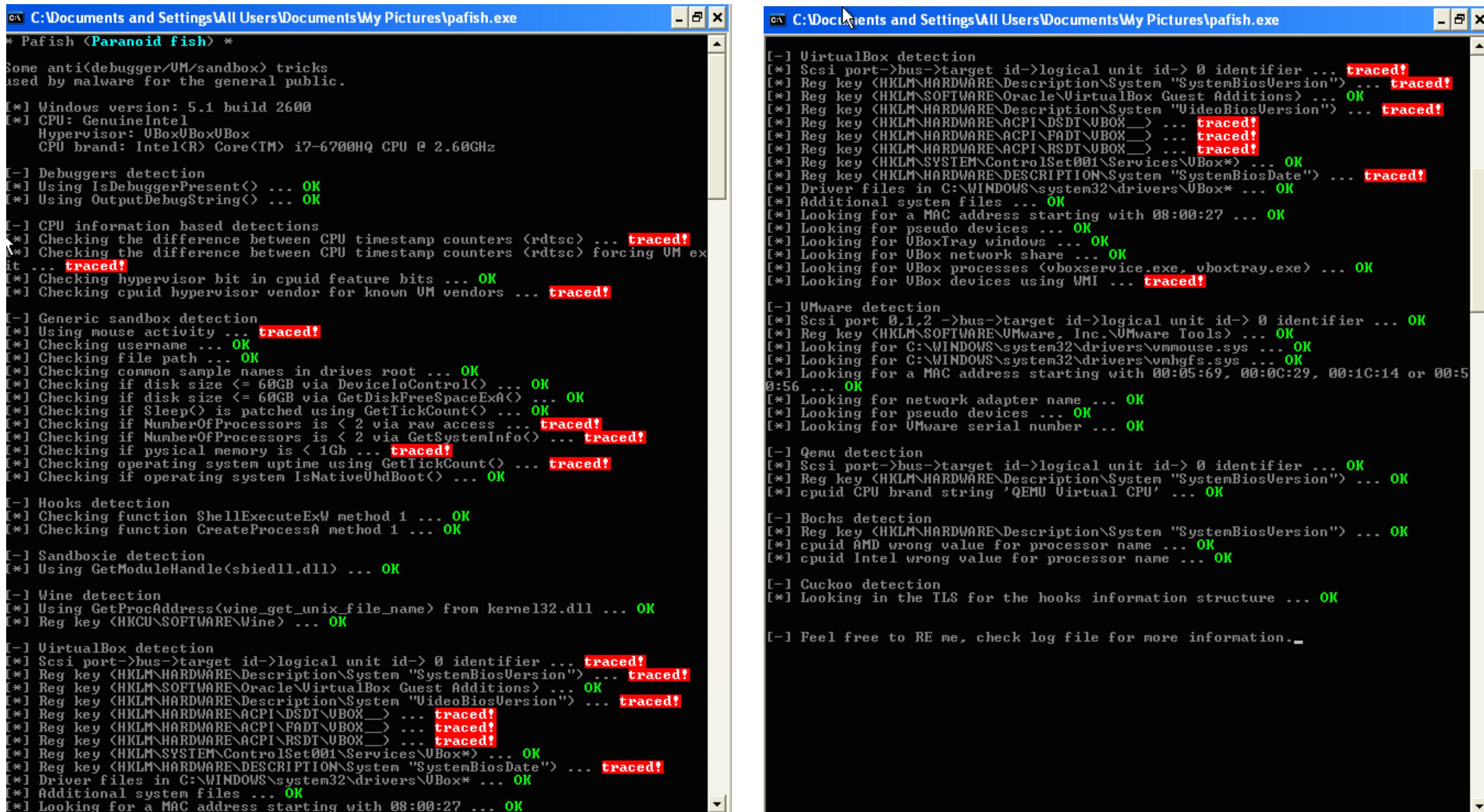


The image shows two windows side-by-side, both titled "C:\Documents and Settings\Administrator\My Documents\pafish.exe". The left window displays the results of the analysis on a VMWare WinXP host, while the right window shows the results on a VMWare Win7 host. Both windows show a series of detections and their outcomes.

VMWare WinXP Host Results (Left Window):

- * Pafish <Paranoid fish>
- Some anti<debugger/VM/sandbox> tricks used by malware for the general public.
- Windows version: 5.1 build 2600
- CPU: GenuineIntel Hypervisor: VMware Hypervisor CPU brand: Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz
- Debuggers detection: OK
- Using IsDebuggerPresent() ... OK
- Using OutputDebugString() ... OK
- GPU information based detections:
 - Checking the difference between CPU timestamp counters (rdtsc) ... OK
 - Checking the difference between CPU timestamp counters (rdtsc) forcing VM exit ... traced!
 - Checking hypervisor bit in cpuid feature bits ... traced!
 - Checking cpuid hypervisor vendor for known VM vendors ... traced!
- Generic sandbox detection:
 - Using mouse activity ... traced!
 - Checking username ... OK
 - Checking file path ... OK
 - Checking common sample names in drives root ... OK
 - Checking if disk size <= 60GB via DeviceIoControl() ... OK
 - Checking if disk size <= 60GB via GetDiskFreeSpaceExA() ... OK
 - Checking if Sleep() is patched using GetTickCount() ... OK
 - Checking if NumberOfProcessors is < 2 via raw access ... traced!
 - Checking if NumberOfProcessors is < 2 via GetSystemInfo() ... traced!
 - Checking if physical memory is < 1Gb ... traced!
 - Checking operating system uptime using GetTickCount() ... traced!
 - Checking if operating system IsNativeUhdBoot() ... OK
- Hooks detection:
 - Checking function ShellExecuteExW method 1 ... OK
 - Checking function CreateProcessA method 1 ... OK
- Sandboxie detection:
 - Using GetModuleHandle<sbiedll.dll> ... OK
- Wine detection:
 - Using GetProcAddress<wine_get_unix_file_name> from kernel32.dll ... OK
 - Reg key <HKCU\SOFTWARE\Wine> ... OK
- VirtualBox detection:
 - Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
 - Reg key <HKLM\HARDWARE\Description\System "SystemBiosVersion"> ... OK
 - Reg key <HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions> ... OK
 - Reg key <HKLM\HARDWARE\Description\System "VideoBiosVersion"> ... OK
 - Reg key <HKLM\HARDWARE\ACPI\DSDT\UBOX> ... OK
 - Reg key <HKLM\HARDWARE\ACPI\FADT\UBOX> ... OK
 - Reg key <HKLM\HARDWARE\ACPI\RSDT\UBOX> ... OK
 - Reg key <HKLM\SYSTEM\ControlSet001\Services\UBox*> ... OK
 - Reg key <HKLM\HARDWARE\DESCRIPTION\System "SystemBiosDate"> ... OK
 - Driver files in C:\WINDOWS\system32\drivers\UBox* ... OK
 - Additional system files ... OK
 - Looking for a MAC address starting with 08:00:27 ... OK

VMCloak WinXP Result in Virtual Box



The image shows two side-by-side windows displaying the output of the Pafish malware detection tool. Both windows have a title bar 'C:\Documents and Settings\All Users\Documents\My Pictures\pafish.exe'.

Left Window Output:

```
* Pafish <Paranoid fish> *
Some anti<debugger/VM/sandbox> tricks
used by malware for the general public.

[*] Windows version: 5.1 build 2600
[*] CPU: GenuineIntel
    Hypervisor: VBoxUBoxUBox
    CPU brand: Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz

[-] Debuggers detection
[*] Using IsDebuggerPresent() ... OK
[*] Using OutputDebugString() ... OK

[-] CPU information based detections
[*] Checking the difference between CPU timestamp counters (rdtsc) ... traced!
[*] Checking the difference between CPU timestamp counters (rdtsc) forcing UM exit ... traced!
[*] Checking hypervisor bit in cpuid feature bits ... OK
[*] Checking cpuid hypervisor vendor for known VM vendors ... traced!

[-] Generic sandbox detection
[*] Using mouse activity ... traced!
[*] Checking username ... OK
[*] Checking file path ... OK
[*] Checking common sample names in drives root ... OK
[*] Checking if disk size <= 60GB via DeviceIoControl() ... OK
[*] Checking if disk size <= 60GB via GetDiskFreeSpaceExA() ... OK
[*] Checking if Sleep() is patched using GetTickCount() ... OK
[*] Checking if NumberOfProcessors is < 2 via raw access ... traced!
[*] Checking if NumberOfProcessors is < 2 via GetSystemInfo() ... traced!
[*] Checking if physical memory is < 1Gh ... traced!
[*] Checking operating system uptime using GetTickCount() ... traced!
[*] Checking if operating system IsNativeUhdBoot() ... OK

[-] Hooks detection
[*] Checking function ShellExecuteExW method 1 ... OK
[*] Checking function CreateProcessA method 1 ... OK

[-] Sandboxie detection
[*] Using GetModuleHandle<sbiedll.dll> ... OK

[-] Wine detection
[*] Using GetProcAddress<wine_get_unix_file_name> from kernel32.dll ... OK
[*] Reg key <HKCU\SOFTWARE\Wine> ... OK

[-] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... traced!
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVersion"> ... traced!
[*] Reg key <HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions> ... OK
[*] Reg key <HKLM\HARDWARE\Description\System "VideoBiosVersion"> ... traced!
[*] Reg key <HKLM\HARDWARE\ACPI\DSDT\UBOX> ... traced!
[*] Reg key <HKLM\HARDWARE\ACPI\FADT\UBOX> ... traced!
[*] Reg key <HKLM\HARDWARE\ACPI\RSDT\UBOX> ... traced!
[*] Reg key <HKLM\SYSTEM\ControlSet001\Services\UBox*> ... OK
[*] Reg key <HKLM\HARDWARE\DESCRIPTION\System "SystemBiosDate"> ... traced!
[*] Driver files in C:\WINDOWS\system32\drivers\UBox* ... OK
[*] Additional system files ... OK
[*] Looking for a MAC address starting with 08:00:27 ... OK
[*] Looking for pseudo devices ... OK
[*] Looking for VBoxTray windows ... OK
[*] Looking for VBox network share ... OK
[*] Looking for VBox processes (vboxservice.exe, vboxtray.exe) ... OK
[*] Looking for VBox devices using WMI ... traced!
```

Right Window Output:

```
[-] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... traced!
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVersion"> ... traced!
[*] Reg key <HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions> ... OK
[*] Reg key <HKLM\HARDWARE\Description\System "VideoBiosVersion"> ... traced!
[*] Reg key <HKLM\HARDWARE\ACPI\DSDT\UBOX> ... traced!
[*] Reg key <HKLM\HARDWARE\ACPI\FADT\UBOX> ... traced!
[*] Reg key <HKLM\HARDWARE\ACPI\RSDT\UBOX> ... traced!
[*] Reg key <HKLM\SYSTEM\ControlSet001\Services\UBox*> ... OK
[*] Reg key <HKLM\HARDWARE\DESCRIPTION\System "SystemBiosDate"> ... traced!
[*] Driver files in C:\WINDOWS\system32\drivers\UBox* ... OK
[*] Additional system files ... OK
[*] Looking for a MAC address starting with 08:00:27 ... OK
[*] Looking for pseudo devices ... OK
[*] Looking for VBoxTray windows ... OK
[*] Looking for VBox network share ... OK
[*] Looking for VBox processes (vboxservice.exe, vboxtray.exe) ... OK
[*] Looking for VBox devices using WMI ... traced!

[-] VMware detection
[*] Scsi port 0,1,2 ->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key <HKLM\SOFTWARE\VMware, Inc.\VMware Tools> ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vhgfs.sys ... OK
[*] Looking for a MAC address starting with 00:05:69, 00:0C:29, 00:1C:14 or 00:05:56 ... OK
[*] Looking for network adapter name ... OK
[*] Looking for pseudo devices ... OK
[*] Looking for VMware serial number ... OK

[-] Qemu detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVersion"> ... OK
[*] cpuid CPU brand string 'QEMU Virtual CPU' ... OK

[-] Bochs detection
[*] Reg key <HKLM\HARDWARE\Description\System "SystemBiosVersion"> ... OK
[*] cpuid AMD wrong value for processor name ... OK
[*] cpuid Intel wrong value for processor name ... OK

[-] Cuckoo detection
[*] Looking in the TLS for the hooks information structure ... OK

[-] Feel free to RE me, check log file for more information.
```

Summary VM Guest Comparison Results

| VM Guest Win XP [Simple Harden] | VM Guest Win XP [VMCloak Version] |
|---|---|
| Generic Sandbox Detection | |
| Mouse activity | Traced |
| Looking for VBox devices using WMI | Traced |
| | Number of Processor < 2 via Raw Access |
| | Number of Processor < 2 via Get System Info |
| | Physical Memory < 1 GB |
| | Operating System Uptime |
| VBox Detection | |
| Looking for MAC Address starting with 08:00:27: | Traced |
| Looking for VBox devices using WMI | Traced |
| | SCSI port->bus->target id->0 identifier |
| | System BIOS version |
| | Guest Addition |
| | Video BIOS Version |
| | ACPI/DSDT |

CCleaner 5.35 Setup.exe

- ▶ Try to identify normal properties of applications
- ▶ As a baseline to identify the ‘suspicious’ properties of malicious application (Fake CCleaner)
- ▶ How to generate simple signature baseline
 - Run analysis on 2 different guest machines, and two different timeout
 - Compare the results
 - Generate the simple signatures for delta Analysis

CCleaner 5.35 Setup.exe Highlights

| Signatures | VMCloak | | Simple Harden | |
|---|---|--|---|---|
| | 120 | 1200 | 120 | 1200 |
| A process attempted to delay the analysis task. (3 events) | NA | CCleaner.exe tried to sleep 5456464 seconds, actually delayed analysis time by 5456464 seconds | NA | NA |
| | | ccsetup535.exe tried to sleep 405 seconds, actually delayed analysis time by 405 seconds | | |
| | | explorer.exe tried to sleep 125 seconds, actually delayed analysis time by 125 seconds | | |
| Malfind detects one or more injected processes | 1 event | NA | 1 event | 1 event |
| The executable contains unknown PE section names indicative of a packer (could be false positive) | 1 event (section .ndata) | 1 event (section .ndata) | 1 event (section .ndata) | 1 event (section .ndata) |
| Allocate read-write-execute memory (usually to unpack itself) | 1 event (NProtectVirtualMemory) | 1 event (NProtectVirtualMemory) | 1 event (NProtectVirtualMemory) | 1 event (NProtectVirtualMemory) |
| Uses Windows utilities for basic Windows Functionality | ping -n 1 -w 1000 www.piriform.com | ping -n 1 -w 1000 www.piriform.com | ping -n 1 -w 1000 www.piriform.com | ping -n 1 -w 1000 www.piriform.com |
| DNS | www.piriform.com | time.windows.com , www.piriform.com , service.piriform.com | www.piriform.com | time.windows.com , www.piriform.com |

CCleaner 5.35 Setup.exe Highlights

| Signatures | VMCloak | | Simple Harden | |
|----------------------|---------|------|---------------|------|
| | 120 | 1200 | 120 | 1200 |
| ICMP Traffic | N/A | N/A | N/A | N/A |
| HTTP Traffic | N/A | N/A | N/A | N/A |
| Agomo Registry Value | N/A | N/A | N/A | N/A |

Normal Signature of Cleaner 5.35 Setup

| | | |
|----|---|---------|
| 1 | Queries for the computername (8 events) | |
| 2 | Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event) | |
| 3 | This executable is signed | Info |
| 4 | Tries to locate where the browsers are installed (1 event) | |
| 5 | Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event) | |
| 6 | The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event) | |
| 7 | Allocates read-write-execute memory (usually to unpack itself) (1 event) | |
| 8 | Checks whether any human activity is being performed by constantly checking whether the foreground window changed | |
| 9 | Queries the disk size which could be used to detect virtual machine with small fixed size or dynamic allocation (10 events) | |
| 10 | Checks for known Chinese AV software registry keys (1 event) | |
| 11 | Steals private information from local Internet browsers (22 events) | |
| 12 | Creates a shortcut to an executable file (50 out of 88 events) | |
| 13 | Executes one or more WMI queries (3 events) | Warning |
| 14 | File has been identified by 2 AntiVirus engines on VirusTotal as malicious (2 events) | |
| 15 | Checks adapter addresses which can be used to detect virtual network interfaces (1 event) | |
| 16 | Potentially malicious URLs were found in the process memory dump (7 events) | |
| 17 | Uses Windows utilities for basic Windows functionality (2 events) | |
| 18 | Executes one or more WMI queries which can be used to identify virtual machines (2 events) | |

Normal Signature of Cleaner 5.35 Setup

| | | |
|----|--|-------|
| 19 | Creates an Alternate Data Stream (ADS) (19 events) | |
| 20 | Attempts to identify installed AV products by installation directory (8 events) | |
| 21 | Attempts to identify installed AV products by registry key (12 events) | |
| 22 | Checks for the presence of known windows from debuggers and forensic tools (1 event) | |
| 23 | Looks for the Windows Idle Time to determine the uptime (1 event) | |
| 24 | A process attempted to delay the analysis task. (3 events) | |
| 25 | Checks the CPU name from registry, possibly for anti-virtualization (1 event) | |
| 26 | Installs itself for autorun at Windows startup (2 events) | |
| 27 | Creates or sets a registry key to a long series of bytes, possibly to store a binary or malware config (1 event) | |
| 28 | Creates known Dapato Trojan files, registry keys and/or mutexes (1 event) | Alert |
| 29 | Queries information on disks, possibly for anti-virtualization (2 events) | |
| 30 | Harvests credentials from local FTP client softwares (1 event) | |
| 31 | Harvests credentials from local email clients (2 events) | |
| 32 | Overwrites 169 files indicative of destructive file actions such as from ransomware (50 out of 169 events) | |
| 33 | Appends a known multi-family ransomware file extension to files that have been encrypted (1 event) | |
| 34 | Writes a potential ransom message to disk (1 event) | |
| 35 | Creates known TeamViewer mutexes and/or registry changes. (1 event) | |
| 36 | Malfind detects one or more injected processes (1 event) | |
| 37 | PEB modified to hide loaded modules. DLL very likely not loaded by LoadLibrary (8 events) | |

CCleaner 5.33.6162 Setup.exe

| Guest Machine | WinXP Simple Harden | |
|-----------------------|--|--|
| Timeout (s) | 120 | 1200 |
| | Overwrites 66 files indicative of destructive file actions such as from ransomware (50 out of 66 events) | Overwrites 66 files indicative of destructive file actions such as from ransomware (50 out of 66 events) |
| | One or more thread handles in other processes (1 event) | One or more thread handles in other processes (1 event) |
| Signatures Comparison | Malfind detects one or more injected processes (1 event) | Malfind detects one or more injected processes (1 event) |
| | PEB modified to hide loaded modules. DLL very likely not loaded by LoadLibrary (5 events) | PEB modified to hide loaded modules. DLL very likely not loaded by LoadLibrary (5 events) |
| | File has been identified by 48 AntiVirus engines on VirusTotal as malicious (48 events) | File has been identified by 48 AntiVirus engines on VirusTotal as malicious (48 events) |
| ICMP Traffic | N/A | N/A |
| HTTP Traffic | N/A | N/A |
| DNS | www.piriform.com (151.101.8.64) | time.windows.com , www.piriform.com (151.101.8.64) |

CCleaner 5.33.6162 Setup.exe

| Guest Machine | VMCloak | |
|-----------------------|---|---|
| Timeout (s) | 120 | 1200 |
| | One or more thread handles in other processes (1 event) | One or more thread handles in other processes (1 event) |
| | | The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event) |
| | PEB modified to hide loaded modules. Dll very likely not loaded by LoadLibrary (7 events) | PEB modified to hide loaded modules. Dll very likely not loaded by LoadLibrary (13 events) |
| | Malfind detects one or more injected processes (1 event) | Malfind detects one or more injected processes (1 event) |
| Signatures Comparison | | Generates some ICMP traffic |
| | | Connects to an IP address that is no longer responding to requests (legitimate services will remain up-and-running usually) (1 event) |
| | File has been identified by 50 AntiVirus engines on VirusTotal as malicious (50 events) | File has been identified by 50 AntiVirus engines on VirusTotal as malicious (50 events) |
| | | Raised Suricata alerts (1 event) |
| | | Network activity contains more than one unique useragent (3 events) |
| | | Collects information about installed applications (45 events) |

CCleaner 5.33.6162 Setup.exe

| Guest Machine | VMCloak | |
|------------------------------|--|-----------|
| Timeout (s) | 120 | 1200 |
| HTTP Traffic | N/A | N/A |
| DNS | www.piriform.com (151.101.8.64) service.piriform.com (151.101.8.64) ab890e964c34.com (72.5.65.111) | |
| ICMP Traffic | N/A | Available |
| IDS Alert | N/A | Available |
| Connected to Dead IP Address | N/A | Available |
| Agomo Registry Value | N/A | Available |

CCleaner / VMCloak / 1200

Raised Suricata alerts (1 event)

suricata ET TROJAN CCleaner Backdoor DGA Oct 2017

A process attempted to delay the analysis task. (3 events)

description CCleaner.exe tried to sleep 5456673 seconds, actually delayed analysis time by 5456673 seconds

description 1a4a5123d7b2c534cb3e3168f7032cf9ebf38b9a2a97226d0fdb7933cf6030ff.exe tried to sleep 126 seconds, actually delayed analysis time by 126 seconds

description explorer.exe tried to sleep 306 seconds, actually delayed analysis time by 306 seconds

Network activity contains more than one unique useragent (3 events)

process 1a4a5123d7b2c534cb3e3168f7032cf9ebf38b9a2a97226d0fdb7933cf6030ff.exe useragent NSIS

process CCleaner.exe useragent Mozilla/4.0 (CCleaner, 5.33.6162)

process CCleaner.exe useragent

Connects to an IP address that is no longer responding to requests (legitimate services will remain up-and-running usually) (1 event)

dead_host 216.126.225.148:443

CCleaner / VMCloak / 1200

ICMP traffic

| Source | Destination | ICMP Type | Data |
|--------------|-------------|-----------|--|
| 192.168.56.2 | 224.0.0.0 | 8 | \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |
| 192.168.56.2 | 224.0.0.0 | 8 | \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |
| 192.168.56.2 | 224.0.0.0 | 8 | \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |
| 192.168.56.2 | 224.0.0.0 | 8 | \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |

DNS

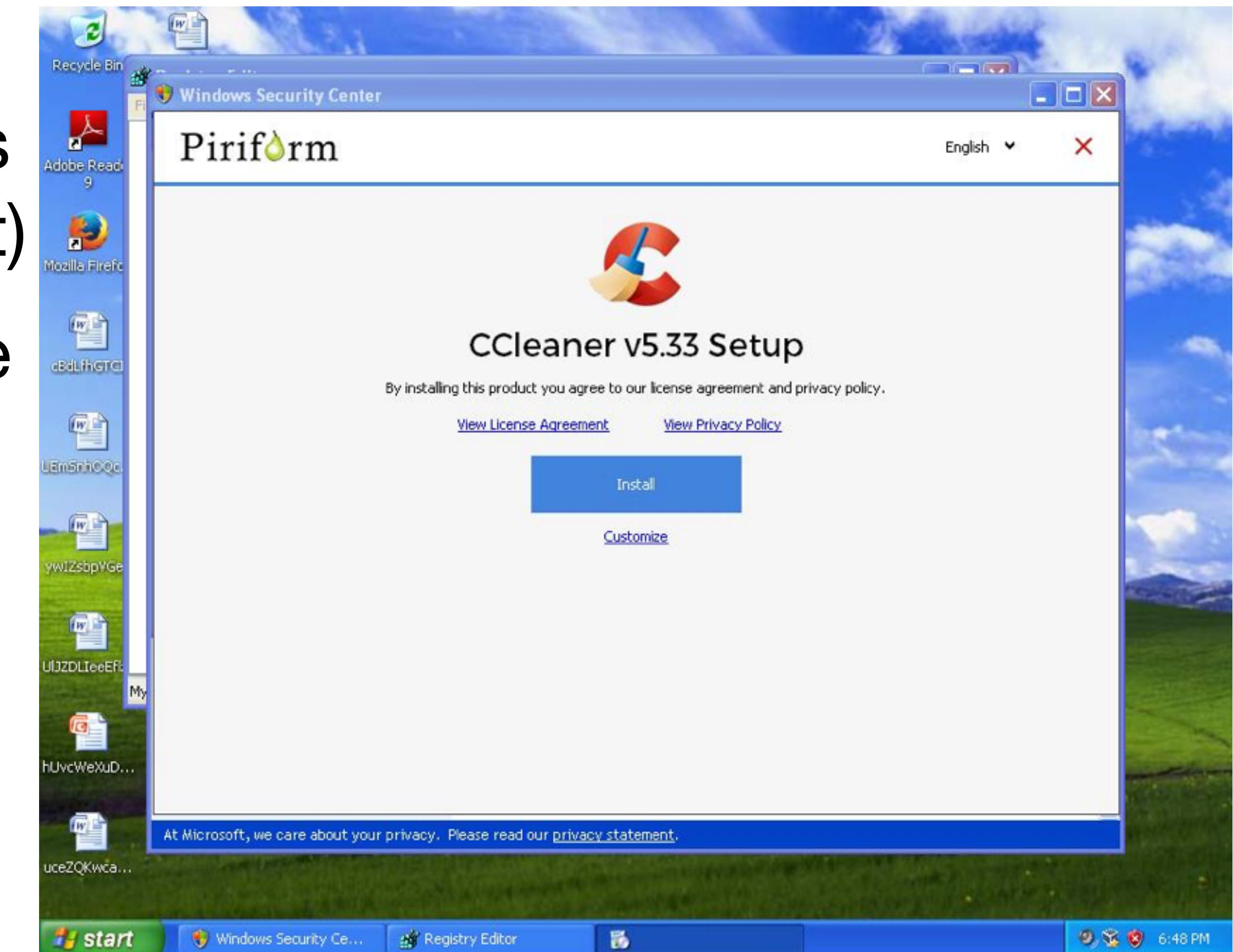
| Name | Response | Post-Analysis Lookup |
|----------------------|----------|----------------------|
| time.windows.com | | |
| service.piriform.com | | 151.101.8.64 |
| ab890e964c34.com | | 72.5.65.111 |
| www.piriform.com | | 151.101.8.64 |

Suricata Alerts

| Flow | SID | Signature | Category |
|--------------------------------------|---------|--|-------------------------------|
| UDP 192.168.56.2:58524 -> 8.8.8.8:53 | 2024716 | ET TROJAN CCleaner Backdoor DGA Oct 2017 | A Network Trojan was detected |
| UDP 192.168.56.2:58524 -> 8.8.8.8:53 | 2024716 | ET TROJAN CCleaner Backdoor DGA Oct 2017 | A Network Trojan was detected |
| UDP 192.168.56.2:58524 -> 8.8.8.8:53 | 2024716 | ET TROJAN CCleaner Backdoor DGA Oct 2017 | A Network Trojan was detected |
| UDP 192.168.56.2:58524 -> 8.8.8.8:53 | 2024716 | ET TROJAN CCleaner Backdoor DGA Oct 2017 | A Network Trojan was detected |
| UDP 192.168.56.2:58524 -> 8.8.8.8:53 | 2024716 | ET TROJAN CCleaner Backdoor DGA Oct 2017 | A Network Trojan was detected |

CCleaner 5.33.6162 Setup.exe

- ▶ Analysis using VM WindowsXP (simple harden), score 5.4 (120 s timeout) and 5.4 (1200 s timeout)
 - not simulate all the case in the installation process
 - URL Found
 - Timeout 120 :
www.piriform.com
 - Timeout 1200 :
time.windows.com,
www.piriform.com



CCleaner 5.33.6162 Portable Apps

| Guest Machine | WinXP Simple Harden | |
|-----------------------|---|---|
| Timeout (s) | 120 | 1200 |
| | This executable has a PDB path (1 event) | This executable has a PDB path (1 event) |
| | The binary likely contains encrypted or compressed data indicative of a packer (2 events) | The binary likely contains encrypted or compressed data indicative of a packer (2 events) |
| | One or more thread handles in other processes (1 event) | One or more thread handles in other processes (1 event) |
| Signatures Comparison | PEB modified to hide loaded modules. Dll very likely not loaded by LoadLibrary (4 events) | PEB modified to hide loaded modules. Dll very likely not loaded by LoadLibrary (13 events) |
| | Malfind detects one or more injected processes (1 event) | Malfind detects one or more injected processes (1 event) |
| | Generates some ICMP traffic | Generates some ICMP traffic |
| | File has been identified by 49 AntiVirus engines on VirusTotal as malicious (49 events) | File has been identified by 49 AntiVirus engines on VirusTotal as malicious (49 events) |
| | | Connects to an IP address that is no longer responding to requests (legitimate services will remain up-and-running usually) (1 event) |
| | | Collects information about installed applications (38 events) |
| | | Network activity contains more than one unique useragent (2 events) |

CCleaner 5.33.6162 Portable Apps

| Guest Machine | VMCloak | |
|-----------------------|---|--|
| Timeout (s) | 120 | 1200 |
| Signatures Comparison | This executable has a PDB path (1 event) | This executable has a PDB path (1 event) |
| | One or more thread handles in other processes (1 event) | One or more thread handles in other processes (1 event) |
| | The binary likely contains encrypted or compressed data indicative of a packer (2 events) | The binary likely contains encrypted or compressed data indicative of a packer (2 events) |
| | | Raised Suricata alerts (1 event) |
| | File has been identified by 49 AntiVirus engines on VirusTotal as malicious (49 events) | File has been identified by 49 AntiVirus engines on VirusTotal as malicious (49 events) |
| | PEB modified to hide loaded modules. Dll very likely not loaded by LoadLibrary (6 events) | PEB modified to hide loaded modules. Dll very likely not loaded by LoadLibrary (13 events) |
| | Malfind detects one or more injected processes (1 event) | Malfind detects one or more injected processes (1 event) |
| | Generates some ICMP traffic | Generates some ICMP traffic |
| | | Collects information about installed applications (44 events) |
| | | Raised Suricata alerts (1 event) |

Portable Apps - Simple Harden / 120

Signatures

This executable has a PDB path (1 event)

pdb_path s:\workspace\ccleaner\branches\v5.33\bin\CCleaner\Release\CCleaner.pdb

The binary likely contains encrypted or compressed data indicative of a packer (2 events)

section {u'size_of_data': u'0x00288200', u'vertual_address': u'0x00691000', u'entropy': 6.800257473603851, u'name': 'entropy', u'.rsrc', u'vertual_size': u'0x00288188'} A section with a high entropy has been found

entropy 0.346289989 description Overall entropy of this PE file is high

ICMP & others

| Source | Destination | ICMP Type | Data |
|----------------|-------------|-----------|--|
| 192.168.56.101 | 224.0.0.0 | | 8 \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |
| 192.168.56.101 | 224.0.0.0 | | 8 \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |
| Agomo | NA | | |

Portable Apps - Simple Harden / 1200

This executable has a PDB path (1 event)

pdb_path s:\workspace\ccleaner\branches\v5.33\bin\CCleaner\Release\CCleaner.pdb

The binary likely contains encrypted or compressed data indicative of a packer (2 events)

| | | | | | |
|---------|---|-------------|-------------|---|--|
| section | {u'size_of_data': u'0x00288200', u'vertual_address': u'0x00691000', u'entropy': 6.800257473603851, u'name': u'.rsrc', u'vertual_size': u'0x00288188'} | entropy | 6.800257474 | description | A section with a high entropy has been found |
| entropy | | 0.346289989 | description | Overall entropy of this PE file is high | |

Allocates read-write-execute memory (usually to unpack itself) (1 event)

| Time & API | Arguments | Status | Return | Repeated |
|-------------------------|--|---------|--------|----------|
| Oct. 3, 2017, 9:23 a.m. | | | | |
| NtAllocateVirtualMemory | process_identifier: 836 region_size: 262144 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x01840000 allocation_type: 8192 (MEM_RESERVE) process_handle: 0xffffffff | success | 0 | 0 |

Network activity contains more than one unique useragent (2 events)

| | | | |
|---------|--|-----------|-----------------------------------|
| process | 6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9 (copy).exe | useragent | Mozilla/4.0 (CCleaner, 5.33.6162) |
| process | 6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9 (copy).exe | useragent | |

A process attempted to delay the analysis task. (1 event)

| | |
|-------------|---|
| description | 6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9 (copy).exe tried to sleep 2728168 seconds, actually delayed analysis time by 2728168 seconds |
|-------------|---|

Portable Apps - Simple Harden / 1200

ICMP traffic

| Source | Destination | ICMP Type | Data |
|----------------|-------------|-----------|--|
| 192.168.56.101 | 224.0.0.0 | 8 | \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |
| 192.168.56.101 | 224.0.0.0 | 8 | \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |

DNS

| Name | Response | Post-Analysis Lookup |
|------------------|-----------|----------------------|
| time.windows.com | | |
| ab890e964c34.com | | 72.5.65.111 |
| www.piriform.com | | 151.101.8.64 |
| Agomo | Available | |

| | Oct. 3, 2017, 9:33 a.m. RegSetValueExA | key_handle: 0x00000100 regkey_r: MUID reg_type: 4 (REG_DWORD) value: 45124707 regkey: HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\Agomo\MUID | | succes | 0 | 0 |
|--|--|--|--|--------|---|---|
| | Oct. 3, 2017, 9:33 a.m. RegOpenKeyExA | regkey_r: SOFTWARE\Piriform\Agomo base_handle: 0x80000002 key_handle: 0x00000260 options: 0 access: 0x00000001 regkey: HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\Agomo | | succes | 0 | 0 |

Portable Apps - VMCloak / 120

This executable has a PDB path (1 event)

pdb_path s:\workspace\ccleaner\branches\v5.33\bin\CCleaner\Release\CCleaner.pdb

The binary likely contains encrypted or compressed data indicative of a packer (2 events)

| | | | | |
|---------|---|-------------|---|--|
| section | {u'size_of_data': u'0x00288200', u'vertual_address': u'0x00691000', u'entropy': 6.800257473603851, u'name': u'.rsrc', u'vertual_size': u'0x00288188'} | entropy | 6.800257474 | description A section with a high entropy has been found |
| entropy | 0.346289989 | description | Overall entropy of this PE file is high | |

A process attempted to delay the analysis task. (1 event)

| | |
|-------------|---|
| description | 6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9 (copy).exe tried to sleep 2728177 seconds, actually delayed analysis time by 2728177 seconds |
|-------------|---|

ICMP traffic

| Source | Destination | ICMP Type | Data |
|--------------|-------------|-----------|--|
| 192.168.56.2 | 224.0.0.0 | 8 | \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |
| 192.168.56.2 | 224.0.0.0 | 8 | \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |

| Name | Response | Post-Analysis Lookup |
|------------------|----------|----------------------|
| www.piriform.com | | 151.101.8.64 |
| Agomo | NA | |

Portable Apps - VMCloak / 1200

This executable has a PDB path (1 event)

pdb_path s:\workspace\ccleaner\branches\v5.33\bin\CCleaner\Release\CCleaner.pdb

The binary likely contains encrypted or compressed data indicative of a packer (2 events)

| | | | | | |
|---------|---|---------|-------------|-------------|--|
| section | {u'size_of_data': u'0x00288200', u'vertual_address': u'0x00691000', u'entropy': 6.800257473603851, u'name': u'.rsrc', u'vertual_size': u'0x00288188'} | entropy | 6.800257474 | description | A section with a high entropy has been found |
|---------|---|---------|-------------|-------------|--|

| | | | |
|---------|-------------|-------------|---|
| entropy | 0.346289989 | description | Overall entropy of this PE file is high |
|---------|-------------|-------------|---|

Raised Suricata alerts (1 event)

| | |
|----------|--|
| suricata | ET TROJAN CCleaner Backdoor DGA Oct 2017 |
|----------|--|

A process attempted to delay the analysis task. (1 event)

| | |
|-------------|---|
| description | 6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9 (copy).exe tried to sleep 2728180 seconds, actually delayed analysis time by 2728180 seconds |
|-------------|---|

Network activity contains more than one unique useragent (2 events)

| | | | |
|---------|---|-----------|-----------------------------------|
| process | 6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9 (copy).exe | useragent | Mozilla/4.0 (CCleaner, 5.33.6162) |
|---------|---|-----------|-----------------------------------|

| | | |
|---------|---|-----------|
| process | 6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9 (copy).exe | useragent |
|---------|---|-----------|

Connects to an IP address that is no longer responding to requests (legitimate services will remain up-and-running usually) (1 event)

| | |
|-----------|---------------------|
| dead_host | 216.126.225.148:443 |
|-----------|---------------------|

Portable Apps - VMCloak / 1200

ICMP traffic

| Source | Destination | ICMP Type | Data |
|--------------|-------------|-----------|--|
| 192.168.56.2 | 224.0.0.0 | 8 | \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M |
| 192.168.56.2 | 224.0.0.0 | 8 | \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M |

Suricata Alerts

| Flow | SID | Signature | Category |
|--------------------------------------|---------|--|-------------------------------|
| UDP 192.168.56.2:53618 -> 8.8.8.8:53 | 2024716 | ET TROJAN CCleaner Backdoor DGA Oct 2017 | A Network Trojan was detected |
| UDP 192.168.56.2:53618 -> 8.8.8.8:53 | 2024716 | ET TROJAN CCleaner Backdoor DGA Oct 2017 | A Network Trojan was detected |
| UDP 192.168.56.2:53618 -> 8.8.8.8:53 | 2024716 | ET TROJAN CCleaner Backdoor DGA Oct 2017 | A Network Trojan was detected |
| UDP 192.168.56.2:53618 -> 8.8.8.8:53 | 2024716 | ET TROJAN CCleaner Backdoor DGA Oct 2017 | A Network Trojan was detected |
| UDP 192.168.56.2:53618 -> 8.8.8.8:53 | 2024716 | ET TROJAN CCleaner Backdoor DGA Oct 2017 | A Network Trojan was detected |

| DNS | Response | Post-Analysis Lookup |
|------------------|----------|----------------------|
| time.windows.com | | |
| ab890e964c34.com | | 72.5.65.111 |
| www.piriform.com | | 151.101.8.64 |

| IP Address | Status | Action |
|-----------------|--------|--------|
| 216.126.225.148 | Active | Moloch |
| 8.8.8.8 | Active | Moloch |

Moloch Data

Sessions | SPI View | SPI Graph | Connections | Files | Users | Stats | Settings moloch v0.17.0

All ip == 8.8.8.8 Search Actions

sessions zoom out

2.5
2
1
0.5
0

2017/10/18 07:00:00 2017/10/18 07:02:00 2017/10/18 07:04:00 2017/10/18 07:06:00 2017/10/18 07:08:00 2017/10/18 07:10:00 2017/10/18 07:12:00 2017/10/18 07:14:00 2017/10/18 07:16:00 2017/10/18 07:18:00 2017/10/18 07:20:00 2017/10/18 07:22:00 2017/10/18 07:24:00 2017/10/18 07:26:00 2017/10/18 07:28:00 2017/10/18 07:30:00 2017/10/18 07:32:00 2017/10/18 07:34:00

D S

moloch v0.17.0

Search Actions

Showing 1 to 2 of 2 entries (filtered from 107 total entries) Column visibility First Previous 1 Next Last

| | Start | Stop | Src IP | Src Port | Dst IP | Dst Port | Packets | Bytes | Node | Info |
|---|---------------------|---------------------|--------------|----------|-------------|----------|---------|-----------|--------|------------------|
| + | 2017/10/18 07:50:04 | 2017/10/18 07:50:12 | 192.168.56.2 | 51560 | 8.8.8.8 USA | 53 | 5 | 340 / 380 | cuckoo | www.piriform.com |
| + | 2017/10/18 07:59:51 | 2017/10/18 07:59:53 | 192.168.56.2 | 64514 | 8.8.8.8 USA | 53 | 3 | 204 / 228 | cuckoo | ab890e964c34.com |

Showing 1 to 22 of 22 entries (filtered from 109 total entries) Column visibility First Previous 1 Next Last

| | Start | Stop | Src IP | Src Port | Dst IP | Dst Port | Packets | Bytes | Node | Info |
|---|---------------------|---------------------|-----------------|----------|-------------|----------|---------|-----------|---------|---|
| + | 2017/10/18 06:44:22 | 2017/10/18 06:44:22 | 192.168.113.147 | 5353 | 224.0.0.251 | 5353 | 1 | 79 / 87 | osboxes | _ipps_tcp.local _ipp_tcp.local |
| + | 2017/10/18 07:18:50 | 2017/10/18 07:19:17 | 192.168.113.1 | 5353 | 224.0.0.251 | 5353 | 4 | 284 / 316 | osboxes | _scanner_tcp.local |
| + | 2017/10/18 07:19:18 | 2017/10/18 07:19:21 | 192.168.113.147 | 5353 | 224.0.0.251 | 5353 | 3 | 215 / 239 | osboxes | _sane-port_tcp.local _scanner_tcp.local |
| + | 2017/10/18 07:19:54 | 2017/10/18 07:21:03 | 192.168.113.1 | 5353 | 224.0.0.251 | 5353 | 5 | 363 / 403 | osboxes | _scanner_tcp.local _ipps_tcp.local _ipp_tcp.local |
| + | 2017/10/18 07:24:02 | 2017/10/18 07:24:53 | 192.168.113.1 | 5353 | 224.0.0.251 | 5353 | 6 | 426 / 474 | osboxes | _scanner_tcp.local |
| + | 2017/10/18 07:25:34 | 2017/10/18 07:25:58 | 192.168.113.1 | 5353 | 224.0.0.251 | 5353 | 4 | 284 / 316 | osboxes | _scanner_tcp.local |
| + | 2017/10/18 07:25:35 | 2017/10/18 07:25:36 | 192.168.113.147 | 5353 | 224.0.0.251 | 5353 | 2 | 142 / 158 | osboxes | _scanner_tcp.local |

Little Bit Memory Analysis

Luckily we have impscan
in volatility

“Impscan identifies calls
to APIs without parsing a
PE's IAT. It even works if
malware completely
erases the PE header, and
it works on kernel drivers.”

```
osboxes@osboxes:~/cuckoo/storage/analyses/8$ vol.py -f memory.dmp --profile=WinXPSP3x86 malfind
Volatility Foundation Volatility Framework 2.6
Process: csrss.exe Pid: 584 Address: 0x7f6f0000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6
0x7f6f0000 c8 00 00 00 3f 01 00 00 ff ee ff ee 08
0x7f6f0010 08 00 00 00 00 fe 00 00 00 00 10 00 00
0x7f6f0020 00 02 00 00 00 20 00 00 8d 01 00 00 ff
0x7f6f0030 03 00 08 06 00 00 00 00 00 00 00 00 00 00
0x7f6f0000 c8000000    ENTER 0x0, 0x0
0x7f6f0004 3f          AAS
0x7f6f0005 0100        ADD [EAX], EAX
0x7f6f0007 00ff        ADD BH, BH
0x7f6f0009 ee          OUT DX, AL
0x7f6f000a ff          DB 0xff
0x7f6f000b ee          OUT DX, AL
0x7f6f000c 087000      OR [EAX+0x0], DH
0x7f6f000f 0008        ADD [EAX], CL
0x7f6f0011 0000        ADD [EAX], AL
0x7f6f0013 0000        ADD [EAX], AL
0x7f6f0015 fe00        INC BYTE [EAX]
0x7f6f0017 0000        ADD [EAX], AL
0x7f6f0019 0010        ADD [EAX], DL
0x7f6f001b 0000        ADD [EAX], AL
0x7f6f001d 2000        AND [EAX], AL
0x7f6f001f 0000        ADD [EAX], AL
0x7f6f0021 0200        ADD AL, [EAX]
0x7f6f0023 0000        ADD [EAX], AL
0x7f6f0025 2000        AND [EAX], AL
0x7f6f0027 008d010000ff ADD [EBP-0xffffffff], CL
0x7f6f002d ef          OUT DX, EAX
0x7f6f002e fd          STD
0x7f6f002f 7f03        JG 0x7f6f0034
0x7f6f0031 0008        ADD [EAX], CL
0x7f6f0033 06          PUSH ES
0x7f6f0034 0000        ADD [EAX], AL
0x7f6f0036 0000        ADD [EAX], AL
0x7f6f0038 0000        ADD [EAX], AL
0x7f6f003a 0000        ADD [EAX], AL
0x7f6f003c 0000        ADD [EAX], AL
0x7f6f003e 0000        ADD [EAX], AL
Process: CCleaner.exe Pid: 1676 Address: 0x1880000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x01880000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01880010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01880020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01880030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x01880000 0000        ADD [EAX], AL
0x01880002 0000        ADD [EAX], AL
0x01880004 0000        ADD [EAX], AL
0x01880006 0000        ADD [EAX], AL
0x01880008 0000        ADD [EAX], AL
0x0188000a 0000        ADD [EAX], AL
0x0188000c 0000        ADD [EAX], AL
0x0188000e 0000        ADD [EAX], AL
0x01880010 0000        ADD [EAX], AL
0x01880012 0000        ADD [EAX], AL
0x01880014 0000        ADD [EAX], AL
0x01880016 0000        ADD [EAX], AL
0x01880018 0000        ADD [EAX], AL
0x0188001a 0000        ADD [EAX], AL
0x0188001c 0000        ADD [EAX], AL
0x0188001e 0000        ADD [EAX], AL
0x01880020 0000        ADD [EAX], AL
0x01880022 0000        ADD [EAX], AL
0x01880024 0000        ADD [EAX], AL
0x01880026 0000        ADD [EAX], AL
0x01880028 0000        ADD [EAX], AL
0x0188002a 0000        ADD [EAX], AL
0x0188002c 0000        ADD [EAX], AL
0x0188002e 0000        ADD [EAX], AL
0x01880030 0000        ADD [EAX], AL
0x01880032 0000        ADD [EAX], AL
0x01880034 0000        ADD [EAX], AL
0x01880036 0000        ADD [EAX], AL
0x01880038 0000        ADD [EAX], AL
0x0188003a 0000        ADD [EAX], AL
0x0188003c 0000        ADD [EAX], AL
0x0188003e 0000        ADD [EAX], AL
```

Little Bit Memory Analysis

The image shows two terminal windows side-by-side. The left window, titled 'osboxes@osboxes: ~/Documents/Extract', runs the command 'strings ccleanup_malware.sample'. It lists various strings found in the sample, including assembly-like labels like '.text', '.reloc', 'B.imports', and various symbols such as 'jaZj', 'Wj?3', 'HtIHup', 'tnHt-H', 'hDIUM', 'hDICT', 'hDICT', 'hDIN', 'hDIN', 'SVW', 'j@VVj', 'QQSV', 'u2!E', 'X_^[', 'Wj\$Y3', '<SW3', 'YPj(', 'j Y_', 'j Y_^[', 'WSSSSS', 'VhTSOP', '\$PTTH', '\$1.1/', 'j,Pj', 'j@_W', 'FHPj', 'tej@', 'X_^[', 'advapi32.dll', 'LookupPrivilegeValueA', 'AdjustTokenPrivileges', 'RegOpenKeyExA', 'RegCloseKey', 'OpenProcessToken', 'kernel32.dll', and 'VirtualAlloc'. The right window, titled 'osboxes@osboxes: ~/.cuckoo/storage/analyses/7/malfind', runs 'strings process.0x86302248.0x1880000.dmp'. It displays the entropy value '2.56544837182' in large yellow text. Below it, the command 'python entropy.py process.0x86314358.0x1880000.dmp' is run, showing the input string 'aabccccdddeffffg', the alphabet of symbols ('['a', 'c', 'b', 'e', 'd', 'g', 'f']'), frequencies of symbols ([0.15384615384615385, 0.07692307692307693, 0.07692307692307693, 0.07692307692307693, 0.07692307692307693, 0.23076923076923078]), and Shannon entropy '2.56544837182'. A large yellow box highlights the entropy value.

```
osboxes@osboxes: ~/Documents/Extract$ strings ccleanup_malware.sample
.text
.reloc
B.imports
A;L$ jaZj
Wj?3 Wj?3
HtIHup HtIHup
tnHt-H tnHt-H
hDIUM hDIUM
hDICT hDICT
hDICT hDICT
hDIN hDIN
SVW j@VVj
QQSV Input string:
u2!E u2!E
X_^[ aabccccdddeffffg
Wj$Y3 Alphabet of symbols in the string:
<SW3 ['a', 'c', 'b', 'e', 'd', 'g', 'f']
YPj( Frequencies of alphabet symbols:
j Y_ [0.15384615384615385, 0.07692307692307693, 0.07692307692307693, 0.07692307692307693, 0.07692307692307693, 0.23076923076923078]
j Y_^[ 693, 0.3076923076923077, 0.07692307692307693, 0.23076923076923078]
WSSSSS VhTSOP
VhTSOP $PTTH
$PTTH $1.1/
$1.1/ j,Pj
j,Pj j@_W
j@_W FHPj
FHPj tej@
tej@ X_^[
X_^[ advapi32.dll
LookupPrivilegeValueA
AdjustTokenPrivileges
RegOpenKeyExA
RegCloseKey
OpenProcessToken
kernel32.dll
VirtualAlloc

osboxes@osboxes: ~/cuckoo/storage/analyses/7/malfind$ strings process.0x86302248.0x1880000.dmp
A;L$ jaZj
Wj?3 Wj?3
HtIHup HtIHup
tnHt-H tnHt-H
hDIUM hDIUM
hDICT hDICT
hDICT hDICT
hDIN hDIN
SVW j@VVj
QQSV Input string:
u2!E u2!E
X_^[ aabccccdddeffffg
Wj$Y3 Alphabet of symbols in the string:
<SW3 ['a', 'c', 'b', 'e', 'd', 'g', 'f']
YPj( Frequencies of alphabet symbols:
j Y_ [0.15384615384615385, 0.07692307692307693, 0.07692307692307693, 0.07692307692307693, 0.07692307692307693, 0.23076923076923078]
j Y_^[ 693, 0.3076923076923077, 0.07692307692307693, 0.23076923076923078]
WSSSSS VhTSOP
VhTSOP $PTTH
$PTTH $1.1/
$1.1/ j,Pj
j,Pj j@_W
j@_W FHPj
FHPj tej@
tej@ X_^[
X_^[ osboxes@osboxes: ~/cuckoo/storage/analyses/7/malfind$
```

The Entropy Value is
2.56544837182

Extracted from Memory using
CCSetup 5.33.6162

Sample from @jaytezer in
VirusTotal

Little Bit Memory Analysis

```
osboxes@osboxes:~/cuckoo/storage/analyses/8$ vol.py -f memory.dmp --profile=WinXPSP3x86 -p 1676 impscan -b 0x1880000
Volatility Foundation Volatility Framework 2.6
IAT      Call      Module      Function
-----  
Files    0x77dfc238 ADVAPI32.dll      LookupPrivilegeValueA  
0x01881004 0x77ddf00c ADVAPI32.dll      AdjustTokenPrivileges  
0x01881008 0x77dd7852 ADVAPI32.dll      RegOpenKeyExA  
0x0188100c 0x77dd6c27 ADVAPI32.dll      RegCloseKey  
0x01881010 0x77dd798b ADVAPI32.dll      OpenProcessToken  
0x01881018 0x7c809af1 kernel32.dll      VirtualAlloc  
0x0188101c 0x7c8099cf kernel32.dll      LocalFree  
0x01881020 0x7c809a2d kernel32.dll      LocalAlloc  
0x01881024 0x7c80bb41 kernel32.dll      lstrcmpiA  
0x01881028 0x7c813499 kernel32.dll      OpenProcess  
0x0188102c 0x7c810830 kernel32.dll      GetVersionExA  
0x01881030 0x7c809b84 kernel32.dll      VirtualFree  
0x01881034 0x7c80a874 kernel32.dll      GetLocalTime  
0x01881038 0x7c802446 kernel32.dll      Sleep  
0x0188103c 0x7c8587eb kernel32.dll      GetComputerNameExA  
0x01881040 0x7c822dcc kernel32.dll      GetComputerNameA  
0x01881044 0x7c80c0f8 kernel32.dll      ExitThread  
0x01881048 0x7c811ab4 kernel32.dll      GetFileAttributesA  
0x0188104c 0x7c801d7b kernel32.dll      LoadLibraryA  
0x01881050 0x7c80ae40 kernel32.dll      GetProcAddress  
0x01881054 0x7c80934a kernel32.dll      GetTickCount  
0x01881058 0x7c810707 kernel32.dll      CreateThread  
0x0188105c 0x7c80de95 kernel32.dll      GetCurrentProcess  
0x01881060 0x7c809be7 kernel32.dll      CloseHandle  
0x01881068 0x77c4aecf msvcrt.dll      time  
0x0188106c 0x77c3f931 msvcrt.dll      sprintf  
0x01881070 0x77c478a0 msvcrt.dll      strlen  
0x01881074 0x77c47a90 msvcrt.dll      strncpy  
0x01881078 0x77c46f70 msvcrt.dll      memcpy  
0x0188107c 0x77c371bc msvcrt.dll      srand  
0x01881080 0x77c371d3 msvcrt.dll      rand  
0x01881088 0x76bf204d PSAPI.DLL      GetModuleFileNameExA  
0x01881090 0x7ca0ec53 SHELL32.dll      IsUserAnAdmin  
0x01881098 0x77fa1999 SHLWAPI.dll      SHEnumKeyExA  
0x0188109c 0x77f70123 SHLWAPI.dll      SHGetValueA  
0x018810a0 0x77f768fb SHLWAPI.dll      SHSetValueA  
0x018810a8 0x3d952128 WININET.dll      InternetCloseHandle  
0x018810ac 0x3d94f5eb WININET.dll      InternetReadFile  
0x018810b0 0x3d955023 WININET.dll      InternetQueryDataAvailable  
0x018810b4 0x3d947021 WININET.dll      HttpSendRequestA  
0x018810b8 0x3d94c39a WININET.dll      InternetSetOptionA  
0x018810bc 0x3d940099 WININET.dll      InternetQueryOptionA  
0x018810c0 0x3d955fee WININET.dll      HttpAddRequestHeadersA  
0x018810c4 0x3d956f4e WININET.dll      InternetConnectA  
0x018810c8 0x3d945828 WININET.dll      InternetOpenA  
0x018810cc 0x3d9565a8 WININET.dll      HttpOpenRequestA  
0x018810d4 0x71ab6a55 WS2_32.dll      WSAStartup  
0x018810d8 0x71ab5355 WS2_32.dll      gethostbyname  
0x018810e0 0x76f51454 WTSAPI32.dll      WTSFreeMemory
```

Seems we have something suspicious at address 0x1880000 and PID 1676

., IP address, domain, or file hash

2 engines detected this file

| SHA-256 | File name | File size | Last analysis |
|--|----------------------------------|-----------|-------------------------|
| 13bef97d0dd9baa05f44766a2f9d9aa7f1c6e07b12a71453f91229dc5d5087fc | process.0x86314358.0x1880000.dmp | 16 KB | 2017-10-19 11:29:17 UTC |

Detection Details Community

| Avast | AVG | AegisLab |
|-----------------------|-----------------------|----------|
| ⚠ Win32:CCAPT-D [Trj] | ⚠ Win32:CCAPT-D [Trj] | Clean |
| Clean | | Clean |

CCleaner 5.33.6162 Extracted Malware

| Guest Machine | Simple Harden | VMCloak |
|---------------|---|---|
| Timeout | 120 | 120 |
| | The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event) | The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event) |
| | One or more thread handles in other processes (1 event) | File has been identified by 49 AntiVirus engines on VirusTotal as malicious (49 events) |
| | PEB modified to hide loaded modules. DLL very likely not loaded by LoadLibrary (4 events) | |
| Signature | Malfind detects one or more injected processes (1 event) | |
| | File has been identified by 47 AntiVirus engines on VirusTotal as malicious (47 events) | |

CCleaner 5.33.6162 Extracted Malware - Strings

| advapi32.dll | kernel32.dll | msvcrt.dll | psapi.dll | ws2_32.dll |
|-----------------------|---------------------|--------------------|----------------------------|---------------------|
| LookupPrivilegeValueA | VirtualAlloc | sprintf | GetModuleFileNameExA | WSAStartup |
| AdjustTokenPrivileges | LocalFree | strlen | | gethostbyname |
| RegOpenKeyExA | LocalAlloc | strncpy | wininet.dll | |
| RegCloseKey | IstrcmpiA | memcpy | InternetCloseHandle | iphlpapi.dll |
| OpenProcessToken | OpenProcess | | InternetReadFile | IcmpCreateFile |
| | GetVersionExA | shlwapi.dll | InternetQueryDataAvailable | IcmpSendEcho |
| shell32.dll | VirtualFree | SHEnumKeyExA | HttpSendRequestA | IcmpCloseHandle |
| IsUserAnAdmin | GetLocalTime | SHGetValueA | InternetSetOptionA | GetAdaptersInfo |
| | GetComputerNameExA | SHSetValueA | InternetQueryOptionA | |
| wtsapi32.dll | GetComputerNameA | | HttpAddRequestHeadersA | |
| WTSFreeMemory | ExitThread | | InternetConnectA | |
| WTSEnumerateProcesses | GetFileAttributesA | | InternetOpenA | |
| | LoadLibraryA | | HttpOpenRequestA | |
| | GetProcAddress | | | |
| | GetTickCount | | | |
| | CreateThread | | | |
| | GetCurrentProcess | | | |
| | CloseHandle | | | |

Score Summary

| Guest Machine | Simple Harden VM | VMCloak |
|------------------------------|------------------|---------|
| Timeout | 120 | 1200 |
| CCleaner Setup 5.35 (Normal) | 7.4 | 7.8 |
| Portable CC 5.33.6162 | 12 | 14.2 |
| CCleaner Setup 5.33.6162 | 5.4 | 5.4 |
| Extracted Malware | 3 **) | - |
| | | 1.4 **) |

*) Test result using global routing options

**) as execute file

MISP Results

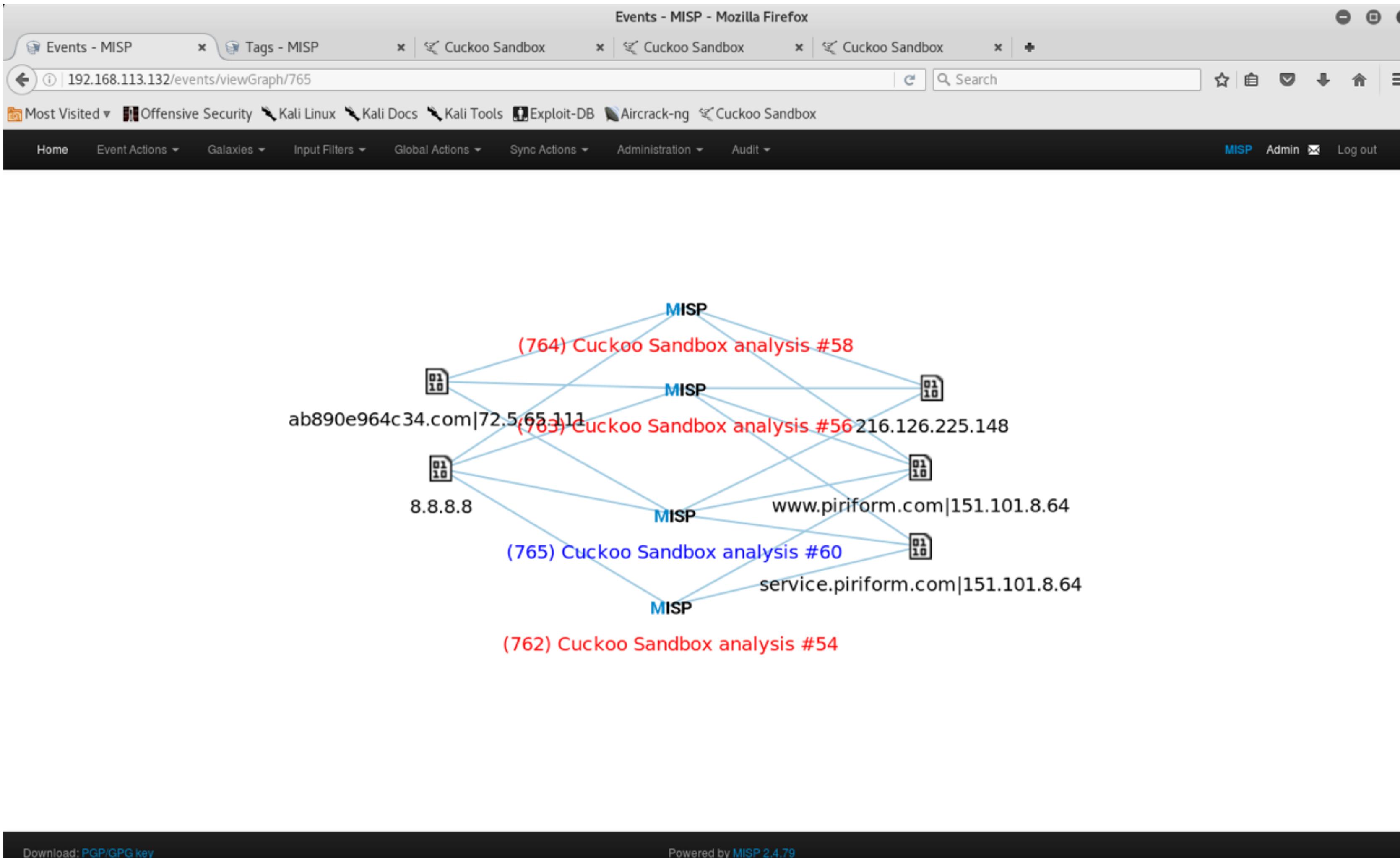
The screenshot shows the MISP web interface with the title "Events - MISP - Mozilla Firefox". The main content area displays a table of events. The fourth row in the table is highlighted with a red box. The event details are as follows:

| Published | Org | Owner Org | ID | Clusters | Tags | #Attr. | #Corr. | Email | Date | Threat Level | Analysis | Info | Distribution | Actions | | | | |
|--------------------------|-----|-----------|------|----------|---|--------|--------|-------|---------------------|--------------|-----------|-----------|--|---------|--|--|--|--|
| <input type="checkbox"/> | | MISP | MISP | 765 | | | 11 | 3 | admin@misp.training | 2017-10-12 | Undefined | Completed | Cuckoo Sandbox analysis #60 | All | | | | |
| <input type="checkbox"/> | | MISP | MISP | 764 | | | 10 | 3 | admin@misp.training | 2017-10-11 | Undefined | Completed | Cuckoo Sandbox analysis #58 | All | | | | |
| <input type="checkbox"/> | | MISP | MISP | 763 | | | 10 | 3 | admin@misp.training | 2017-10-11 | Undefined | Completed | Cuckoo Sandbox analysis #56 | All | | | | |
| <input type="checkbox"/> | | MISP | MISP | 762 | | | 8 | 3 | admin@misp.training | 2017-10-11 | Undefined | Completed | Cuckoo Sandbox analysis #54 | All | | | | |
| <input type="checkbox"/> | | | MISP | 760 | Type:OSINT tip:white osint:source-type="blog-post" | | 80 | | admin@misp.training | 2017-07-13 | Low | Completed | OSINT - Meet Ovidiy Stealer: Bringing credential theft to the masses | All | | | | |
| <input type="checkbox"/> | | | MISP | 746 | Type:OSINT tip:white osint:source-type="blog-post" circ:incident-classification="malware" | | 418 | 1 | admin@misp.training | 2017-07-18 | Low | Completed | OSINT - Threat Spotlight: Is Fireball Adware or Malware? | All | | | | |
| <input type="checkbox"/> | | | MISP | 742 | Type:OSINT tip:white osint:source-type="blog-post" ms-caro-malware-full:malware-type="Backdoor" | | 210 | | admin@misp.training | 2017-07-17 | Low | Completed | OSINT - Android Backdoor GhostCtrl can Silently Record Your Audio, Video, and More | All | | | | |
| <input type="checkbox"/> | | | MISP | 756 | Type:OSINT tip:white circ:incident-classification="malware" osint:source-type="blog-post" | | 140 | | admin@misp.training | 2017-08-22 | Low | Completed | OSINT - Malware uncovered by ESET researchers aimed at gamers | All | | | | |
| <input type="checkbox"/> | | | MISP | 757 | Type:OSINT tip:white | | 16 | | admin@misp.training | 2017-08-23 | Low | Completed | OSINT - Malicious script | All | | | | |

Download: PGP/GPG key Powered by MISP 2.4.79

Cuckoo analysis result are fed into MISP events

MISP : Sharing is Caring

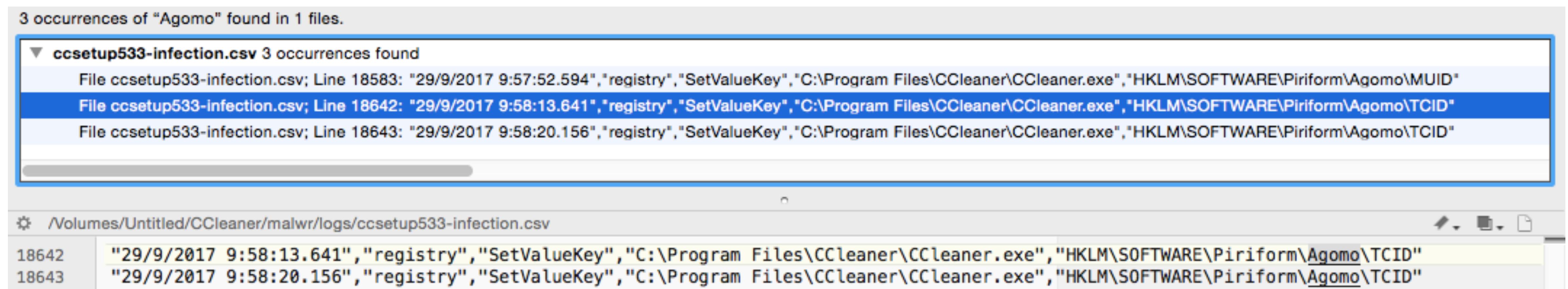


- ▶ MISP node represent an organisation
- ▶ The same colour in the text represent the similar input events (with different ID)
- ▶ Cuckoo results feeds into MISP, then MISP can make a correlation
- ▶ Imagine if we can integrated all the effort, there will be no more redundant analysis and we can easily aware about the ‘new’ malware attack

Manual Time

CaptureBAT

- ▶ This is a behavioral analysis tool of applications for the Win32 operating system family.
- ▶ Capture BAT is able to monitor the state of a system during the execution of applications and processing of documents, which provides an analyst with insights on how the software operates even if no source code is available



3 occurrences of "Agomo" found in 1 files.

▼ ccsetup533-infection.csv 3 occurrences found

- File ccsetup533-infection.csv; Line 18642: "29/9/2017 9:58:13.641","registry","SetValueKey","C:\Program Files\CCleaner\CCleaner.exe","HKLM\SOFTWARE\Piriform\Agomo\TCID"
- File ccsetup533-infection.csv; Line 18643: "29/9/2017 9:58:20.156","registry","SetValueKey","C:\Program Files\CCleaner\CCleaner.exe","HKLM\SOFTWARE\Piriform\Agomo\TCID"

⌚ /Volumes/Untitled/CCleaner/malwr/logs/ccsetup533-infection.csv

| 18642 | "29/9/2017 9:58:13.641","registry","SetValueKey","C:\Program Files\CCleaner\CCleaner.exe","HKLM\SOFTWARE\Piriform\Agomo\TCID" |
|-------|---|
| 18643 | "29/9/2017 9:58:20.156","registry","SetValueKey","C:\Program Files\CCleaner\CCleaner.exe","HKLM\SOFTWARE\Piriform\Agomo\TCID" |

Regshot & Fake DNS

```
File Edit Tabs Help  
remnux@rem... remnux@rem... remnux@rem...  
  
remnux@remnux:~$ fakedns  
pyminifakeDNS:: dom.query. 60 IN A 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128  
Respuesta: www.piriform.com. -> 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128  
Respuesta: clients5.google.com. -> 192.168.157.128  
Respuesta: www.google.com. -> 192.168.157.128  
Respuesta: go.microsoft.com. -> 192.168.157.128  
Respuesta: google.com. -> 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128  
Respuesta: watson.telemetry.microsoft.com. -> 192.168.157.128  
Respuesta: ctld1.windowsupdate.com. -> 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128  
Respuesta: sqm telemetry microsoft com -> 192.168.157.128  
Respuesta: ab1145b758c30.com. -> 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128  
Respuesta: win8.ipv6.microsoft.com. -> 192.168.157.128
```

Fake DNS

Keys added: 118

HKLM\SOFTWARE\Microsoft\.NETFramework\SQM
HKLM\SOFTWARE\Microsoft\.NETFramework\SQM\CommonDatapoints
HKLM\SOFTWARE\Microsoft\.NETFramework\SQM\Rare
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\Volatile
HKLM\SOFTWARE\Piriform
HKLM\SOFTWARE\Piriform\Agomo
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(_?_Volume{46da0021-4f42-11e3-97
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd6
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher
HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag\Lovelace

Apps ACL Android The CFReDS Project PublicMemoryImage CNIT 123 P

Values added: 684

HKLM\SOFTWARE\Microsoft\.NETFramework\SQM>LastNextSampleTime: 93 E7 5D 21 C8 B7 5C 21
HKLM\SOFTWARE\Microsoft\.NETFramework\SQM\CommonDatapoints\1008: 0x00025F57
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\RacLastCEIP: 9E D3 A3 DC 9A 36 D3 01
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\RacLastCrimDataTime: C4 07 2C E2 9A 36 D3 01
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\RacLastTime: 6D 4E A8 E7 9A 36 D3 01
HKLM\SOFTWARE\Microsoft\SQMClient\Windows\Uploader>LastUploadTime: 75 FA 2A AC 97 36 D3 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\AIT\LastHeartbeatTime: C9 39 BC 0F
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\AIT\RunsSinceLastShimClear: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Superfetch\DecompressRateKB: E4 E0 05 00 DE AB 0E
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\LastIndex: 0x0000000C
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\Volatile\NestingLevel: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\Volatile\StartNesting: 00 00 00 00 00 00
HKLM\SOFTWARE\Piriform\Agomo\MUID: 0x07038893
HKLM\SOFTWARE\Piriform\Agomo\: 0xB5CF9686
HKLM\SOFTWARE\Piriform\Agomo\TCID: 0x59CC9E82

Infected Machine

Simple Network Analysis on Fake CCleaner

ICMP Echo start at 0.000 Dest IP 224.0.0.0

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|---------------------------|-----------------|----------|--------|---|
| 1 | 0.000000 | 192.168.113.136 | 224.0.0.0 | ICMP | 58 | Echo (ping) request id=0x0001, seq=4/1024, ttl=255 (no response) |
| 2 | 0.343982 | 192.168.113.136 | 192.168.113.2 | DNS | 76 | Standard query 0x7342 A www.piriform.com |
| 3 | 0.509582 | 192.168.113.2 | 192.168.113.136 | DNS | 129 | Standard query response 0x7342 CNAME f.global-ssl.fastly.net A 1 |
| 4 | 0.513557 | 192.168.113.136 | 151.101.8.64 | TCP | 66 | 49181-443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 149 | 577.448862 | 192.168.113.136 | 192.168.113.2 | NBNS | 110 | Refresh NB <01><02>_MSBROWSE__<02><01> |
| 150 | 580.902102 | fe80::8d94:deb5:78fc:e8d4 | ff02::1:2 | DHCPv6 | 156 | Solicit XID: 0x2348a0 CID: 0001000121570119000c29467e52 |
| 151 | 588.917905 | fe80::8d94:deb5:78fc:e8d4 | ff02::1:2 | DHCPv6 | 156 | Solicit XID: 0x2348a0 CID: 0001000121570119000c29467e52 |
| 152 | 598.339543 | fe80::8d94:deb5:78fc:e8d4 | ff02::1 | TCPv6 | 86 | Router Advertisement from 00:0c:29:46:7e:52 |
| 153 | 600.875837 | 192.168.113.136 | 216.126.225.148 | TCP | 66 | 49185-443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 154 | 601.158775 | 216.126.225.148 | 192.168.113.136 | TCP | 60 | 443-49185 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 155 | 601.158813 | 192.168.113.136 | 216.126.225.148 | TCP | 54 | 49185-443 [ACK] Seq=1 Ack=1 Win=65535 Len=0 |
| 156 | 601.159155 | 192.168.113.136 | 216.126.225.148 | SSL | 196 | Client Hello |
| 157 | 601.159368 | 216.126.225.148 | 192.168.113.136 | TCP | 60 | 443-49185 [ACK] Seq=1 Ack=143 Win=64240 Len=0 |
| 158 | 604.918598 | fe80::8d94:deb5:78fc:e8d4 | ff02::1:2 | DHCPv6 | 156 | Solicit XID: 0x2348a0 CID: 0001000121570119000c29467e52 |
| 159 | 630.874310 | 192.168.113.136 | 216.126.225.148 | TCP | 54 | 49185-443 [RST, ACK] Seq=143 Ack=1 Win=0 Len=0 |
| 160 | 630.876410 | 192.168.113.136 | 192.168.113.2 | DNS | 77 | Standard query 0x0188 A ab1145b758c30.com |
| 161 | 631.375839 | 192.168.113.2 | 192.168.113.136 | DNS | 109 | Standard query response 0x0188 A 127.100.183.225 A 10.158.168.17 |

Frame 153: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Vmware_46:7e:52 (00:0c:29:46:7e:52), Dst: Vmware_f8:cd:a8 (00:50:56:f8:cd:a8)
Internet Protocol Version 4, Src: 192.168.113.136 (192.168.113.136), Dst: 216.126.225.148 (216.126.225.148)
Transmission Control Protocol, Src Port: 49185 (49185), Dst Port: 443 (443), Seq: 0, Len: 0

Contact IP 216.126.225.148 at 600.875037

September (2017-09)

Contact Domain ab1145b758c30.com at 630.876410

Random Domain Name - DGA

ab6d54340c1a[.]com, aba9a949bc1d[.]com, ab2da3d400c20[.]com
ab3520430c23[.]com, ab1c403220c27[.]com, ab1abad1d0c2a[.]com
ab8cee60c2d[.]com, **ab1145b758c30[.]com**, **ab890e964c34[.]com**
ab3d685a0c37[.]com, ab70a139cc3a[.]com



52.213.122.236
52.50.107.236



IP Whois

Amazon Data Services Ireland Limited AMAZON-DUB (NET-52-208-0-0-1) 52.208.0.0 – 52.215.255.255
Amazon Technologies Inc. AT-88-Z (NET-52-192-0-0-1) 52.192.0.0 – 52.223.255.255

How Cuckoo Calculate the Rating

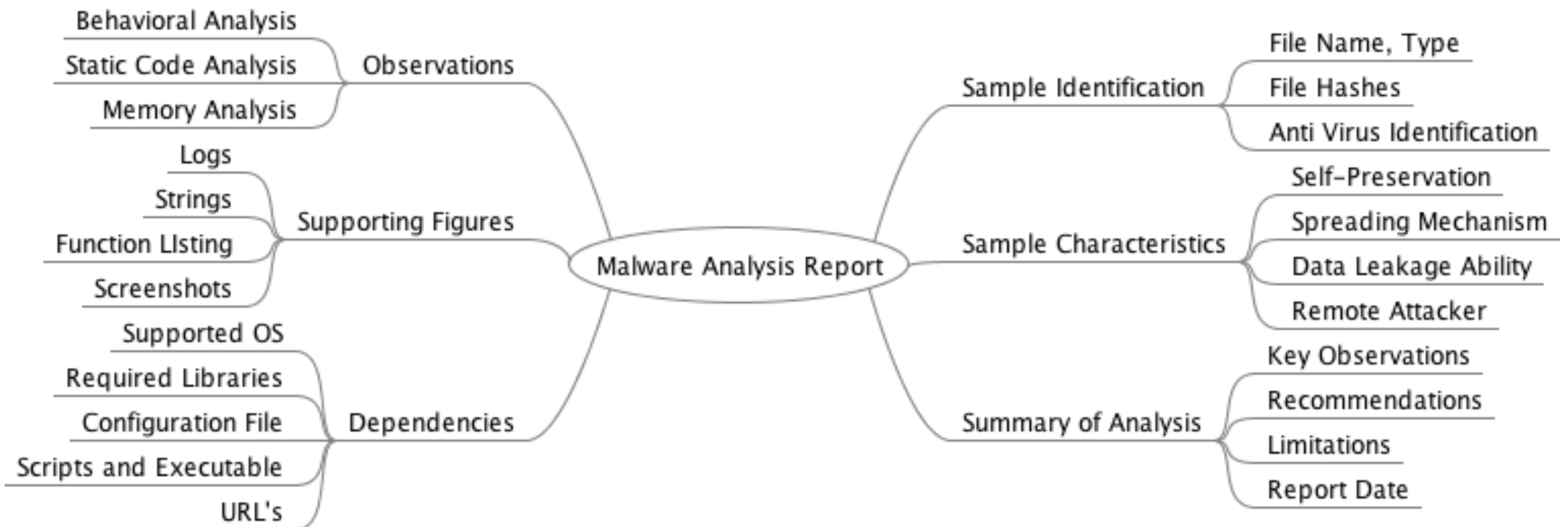
- ▶ in the file “lib/cuckoo/core/plugins.py”

```
score = 0
for signature in self.signatures:
    if signature.matched:
        self.matched.append(signature.results())
        score += signature.severity
self.results["info"]["score"] = score / 5.0
```

- ▶ And the second magic number appears in web/templates/analysis/overview/index.html:

```
<strong>{{ analysis.info.score }} out of 10.</strong>
```

- ▶ Don't get confused if your result more than 10 points, this is not Cuckoo bugs but your file is really bad file



Report Summary - Stage 1 (1/2)

| Sample Identification | | | | | | | | | | | | | | | | | |
|-----------------------|--|----------|-----------------|----------------------|----------------------|-----------|---------------------------------|-------------|---------------------------|----------|----------------|----------------------|---------------|-----------|------------------------------|-------------|-----------------|
| File Name, Type | CCleaner 5.33.6162 Portable, Setup, Extract | | | | | | | | | | | | | | | | |
| File Hashes | Portable - 6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9 Setup - 1a4a5123d7b2c534cb3e3168f7032cf9ebf38b9a2a97226d0fdb7933cf6030ff Extract - 8f56fd14133ccd84b6395913536f5823d74737c410b829f729baaf2fe645a0a9 | | | | | | | | | | | | | | | | |
| AV Identification | Extract Malware <table><tbody><tr><td>Symantec</td><td>Backdoor.Trojan</td></tr><tr><td>TrendMicro-HouseCall</td><td>TROJ_GEN.R011C0DIK17</td></tr><tr><td>Kaspersky</td><td>HEUR:Trojan.Win32.Axiombase.gen</td></tr><tr><td>BitDefender</td><td>Trojan.GenericKD.12388319</td></tr></tbody></table> Portable <table><tbody><tr><td>Symantec</td><td>Trojan.Sibakdi</td></tr><tr><td>TrendMicro-HouseCall</td><td>BKDR_CCHACK.A</td></tr><tr><td>Kaspersky</td><td>Backdoor.Win32.InfeCleaner.a</td></tr><tr><td>BitDefender</td><td>Trojan.PRForm.A</td></tr></tbody></table> | Symantec | Backdoor.Trojan | TrendMicro-HouseCall | TROJ_GEN.R011C0DIK17 | Kaspersky | HEUR:Trojan.Win32.Axiombase.gen | BitDefender | Trojan.GenericKD.12388319 | Symantec | Trojan.Sibakdi | TrendMicro-HouseCall | BKDR_CCHACK.A | Kaspersky | Backdoor.Win32.InfeCleaner.a | BitDefender | Trojan.PRForm.A |
| Symantec | Backdoor.Trojan | | | | | | | | | | | | | | | | |
| TrendMicro-HouseCall | TROJ_GEN.R011C0DIK17 | | | | | | | | | | | | | | | | |
| Kaspersky | HEUR:Trojan.Win32.Axiombase.gen | | | | | | | | | | | | | | | | |
| BitDefender | Trojan.GenericKD.12388319 | | | | | | | | | | | | | | | | |
| Symantec | Trojan.Sibakdi | | | | | | | | | | | | | | | | |
| TrendMicro-HouseCall | BKDR_CCHACK.A | | | | | | | | | | | | | | | | |
| Kaspersky | Backdoor.Win32.InfeCleaner.a | | | | | | | | | | | | | | | | |
| BitDefender | Trojan.PRForm.A | | | | | | | | | | | | | | | | |
| Supported OS | Windows OS (32 and 64-bit) | | | | | | | | | | | | | | | | |
| Required Libraries | advapi32.dll, kernel32.dll, msrvct.dll, psapi.dll, ws2_32.dll, wininet.dll, iphlpapi.dll, shlwapi.dll, shell32.dll, wtsapi32.dll | | | | | | | | | | | | | | | | |
| Configuration File | s:\workspace\ccleaner\branches\v5.33\bin\CCleaner\Release\CCleaner.pdb | | | | | | | | | | | | | | | | |
| Dependencies | | | | | | | | | | | | | | | | | |
| URL / IP | ab6d54340c1a[.]com, aba9a949bc1d[.]com, ab2da3d400c20[.]com, ab3520430c23[.]com, ab1c403220c27[.]com, ab1abad1d0c2a[.]com ab8cee60c2d[.]com, ab1145b758c30[.]com , ab890e964c34[.]com , ab3d685a0c37[.]com, ab70a139cc3a[.]com | | | | | | | | | | | | | | | | |

Report Summary - Stage 1 (2/2)

| | | |
|-------------------------------|---------------------|---|
| Supporting Figures | Strings | - |
| | Function Listing | IsUserAnAdmin, GetComputerNameExA, etc [Ref. Extracted String] |
| | Screenshots | - |
| Observations | Behavioral Analysis | Generate ICMP Traffic \x00os\x00\xb4\xfc\x9e\x01X\xc9\x93\xd0\x12M\x00 |
| | | Connected to specific IP and Random Domain |
| | Key Observations | Agomo Registry Value, PDB Path, ICMP Traffic, DGA |
| Summary of Analysis | Recommendations | Backup data, restore computer to clean point, update your Cleaner |
| | Limitation | Guest VM Not Fully Harden |
| | Report Date | 20 Oct 2017 |
| Sample Characteristics | Spreading Mechanism | CCleaner download site |
| | Data Leak Ability | Detect userIsAdmin, GetComputerName |
| | Remote Attacker | 216.126.225.148 |

Conclusion

- **Are we really sure rely only on automatic analysis [using default configuration] ?**
 - ▶ More faster, but devil always in details
 - ▶ CCleaner malware try to evade its existence by removing the PE header information
 - ▶ Don't forget to run some cases to understand more details (Don't forget to tuning your weapon)
- **There is no trace or evidence the existence of malware in hard drive**
 - ▶ CCleaner malware try to evade its existence by removing the PE header information, and run in the memory
- **Attacker invasion to supply chain**
 - ▶ “Trust but verify” before using it. Security testing become a mandatory before deploy a new release of software
 - ▶ Source code audit before releasing the application
 - ▶ Regularly screening employee or contractor
- **There is still much more room in Cuckoo to improve**
 - ▶ Comparison feature only to do a comparison for the same hash file, it would be nice if we can compare two different result analysis of two different files
 - ▶ Comparison feature only highlight in “general” view

Referensi

- ▶ Evidence Aurora Operation Still Active Part 2: More Ties Uncovered Between CCleaner Hack & Chinese Hackers, <http://www.intezer.com/evidence-aurora-operation-still-active-part-2-more-ties-uncovered-between-ccleaner-hack-chinese-hackers/>
- ▶ CCleanup: A Vast Number of Machines at Risk, <http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>
- ▶ Moloch, <https://molo.ch/>
- ▶ Cuckoo Sandbox Documentation, <http://docs.cuckoosandbox.org/>



**“Kechilafan satu orang sahaja tjukup sudah
menjebabkan keruntuhan negara”**

Dr. Roebiono Kertopati