Playing around with Fake CCleaner and Cuckoo

Jakarta, 20 Oktober 2017

Today’s Agenda

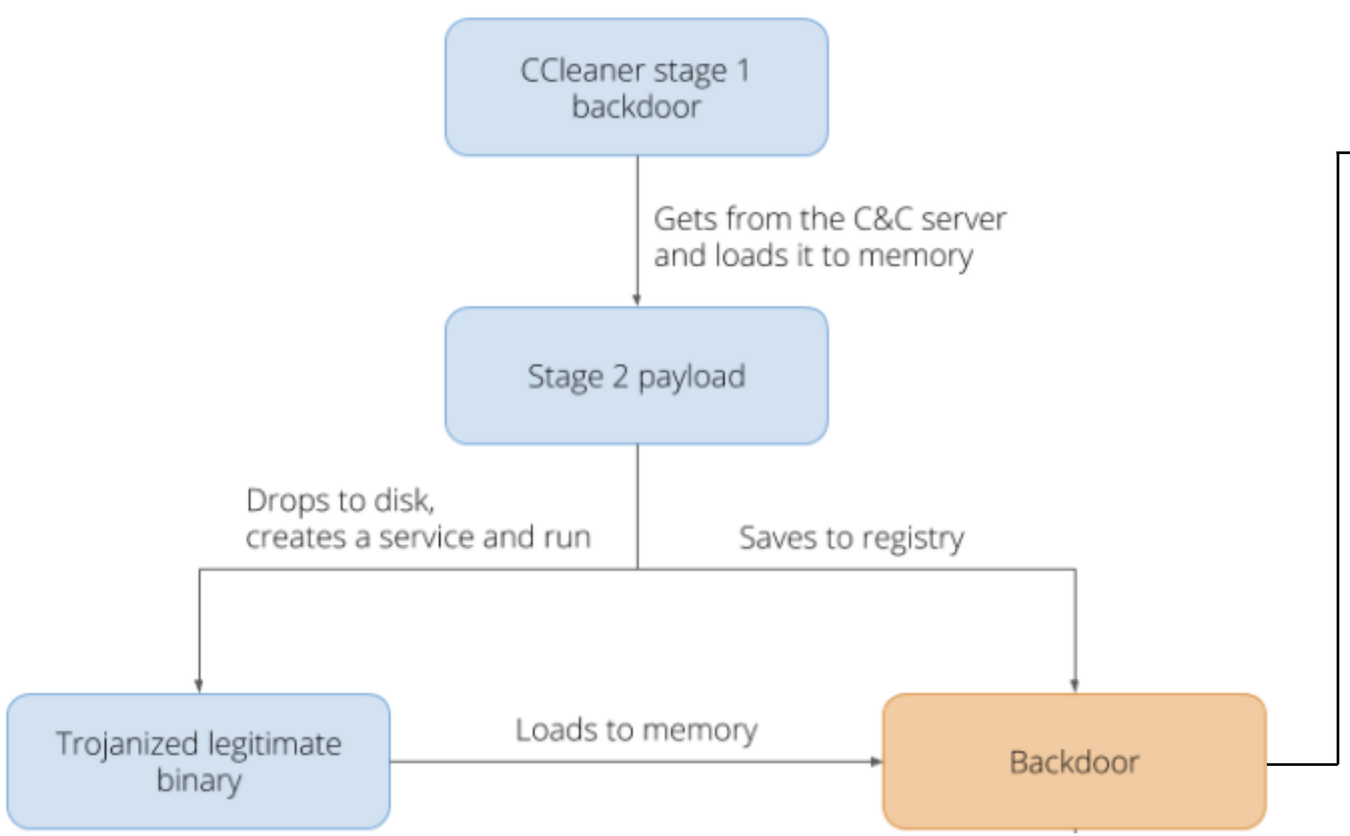
- Fake CCleaner Overview
- Clean CCleaner vs Malware CCleaner Comparison
- More on CCleaner Analysis
- CCleaner Malware Analysis Report
- Conclusions

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)



Backdoor Process

1. Sends HTTP request to https://microsoft.com and https://update.microsoft.com
2. Checks if HTTP response contains strings "Microsoft" and "Internet Explorer"
3. Sends HTTP request to https://en.search.wordpress.com/?src=organic&q=keepost or https://github.com/search?q=joinlur&type=Users&utf8=%E2%9C%93
4. Sends HTTP request to https://en.search.wordpress.com/?src=organic&q=keepost or https://github.com/search?q=joinlur&type=Users&utf8=%E2%9C%93
5. Retrieves a response that uses steganography to store an IP address in a field called "ptoken"
6. ptoken field is xor'ed to get the decrypted address of C&C
7. Connects to C&C IP address, sends machine information, and waits for next payload

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.sepm	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

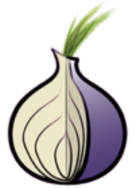
DLL, exe, .doc, HTML, PDF, PPT, etc

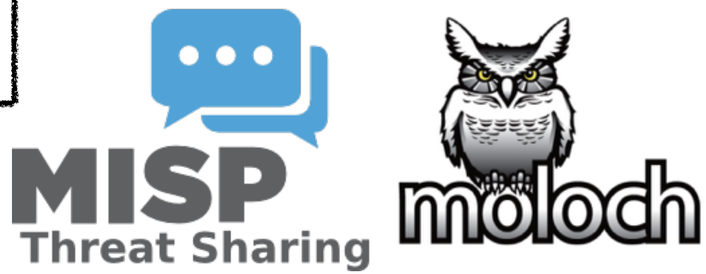
Integration

- Suricata/Snort
- MITM Proxy

Network Analysis Routing

VPN, Non Routing, Inetsim





Malware Analysis Platform

- **Windows**
- Linux
- Android

Sandbox Architecture

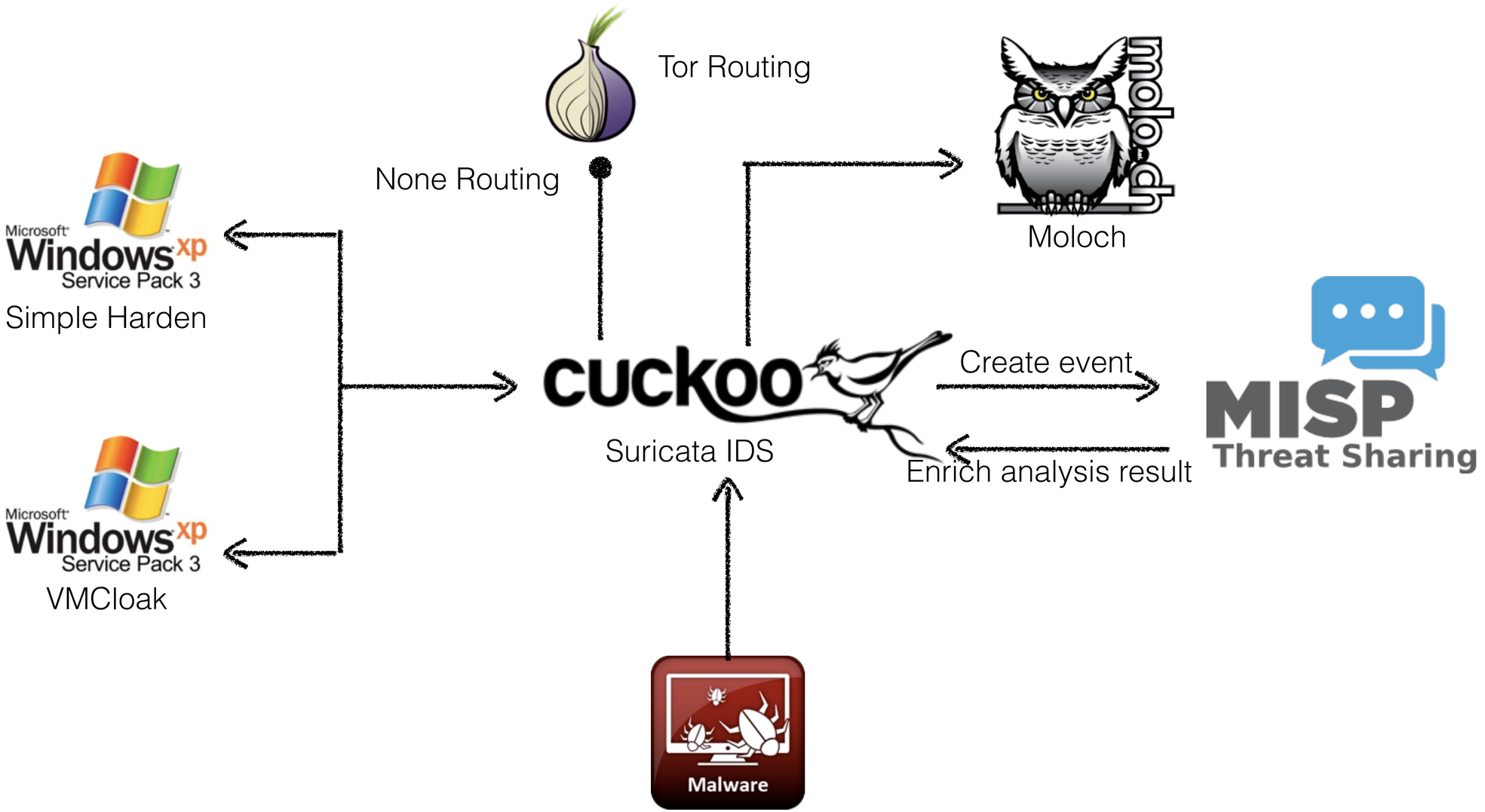
- **Virtualbox**
- VMWare Workstation
- KVM
- Xen Server, etc

Scoring System

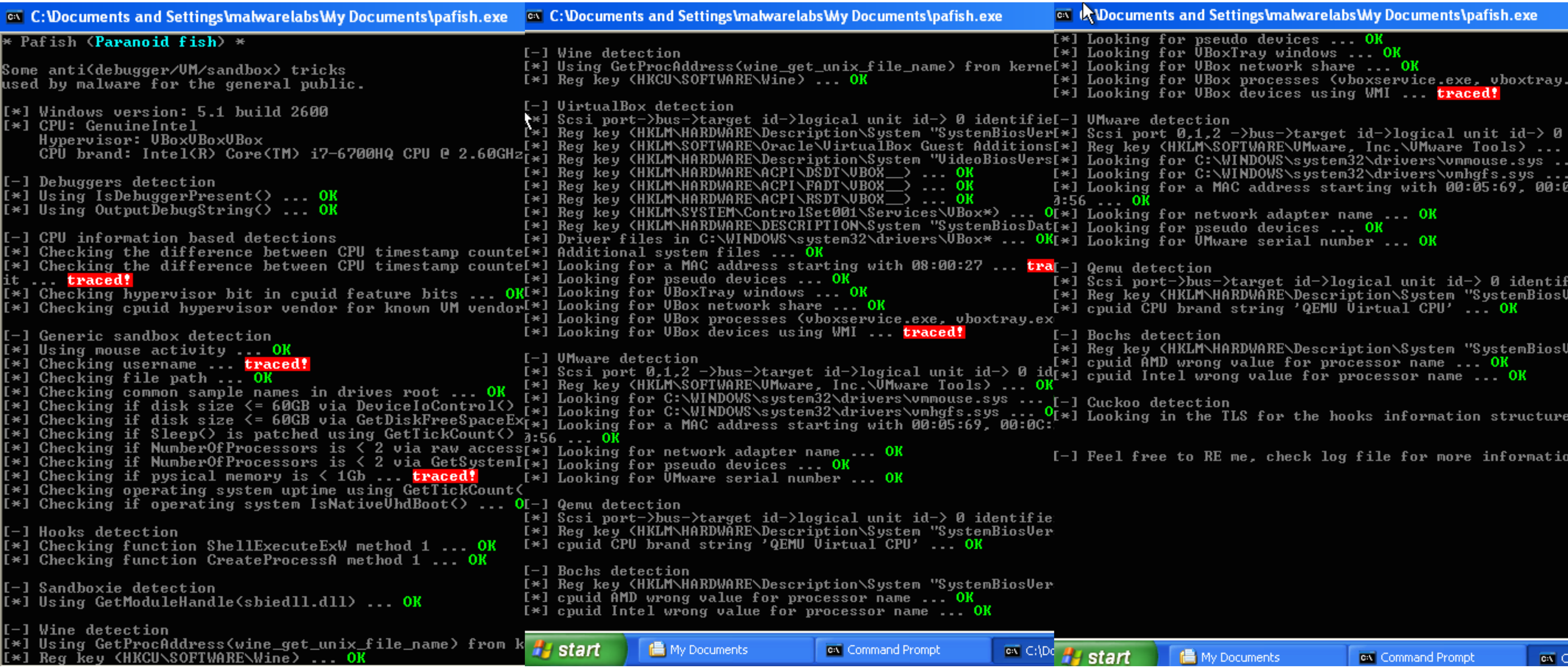
Playing Around Case

- **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)

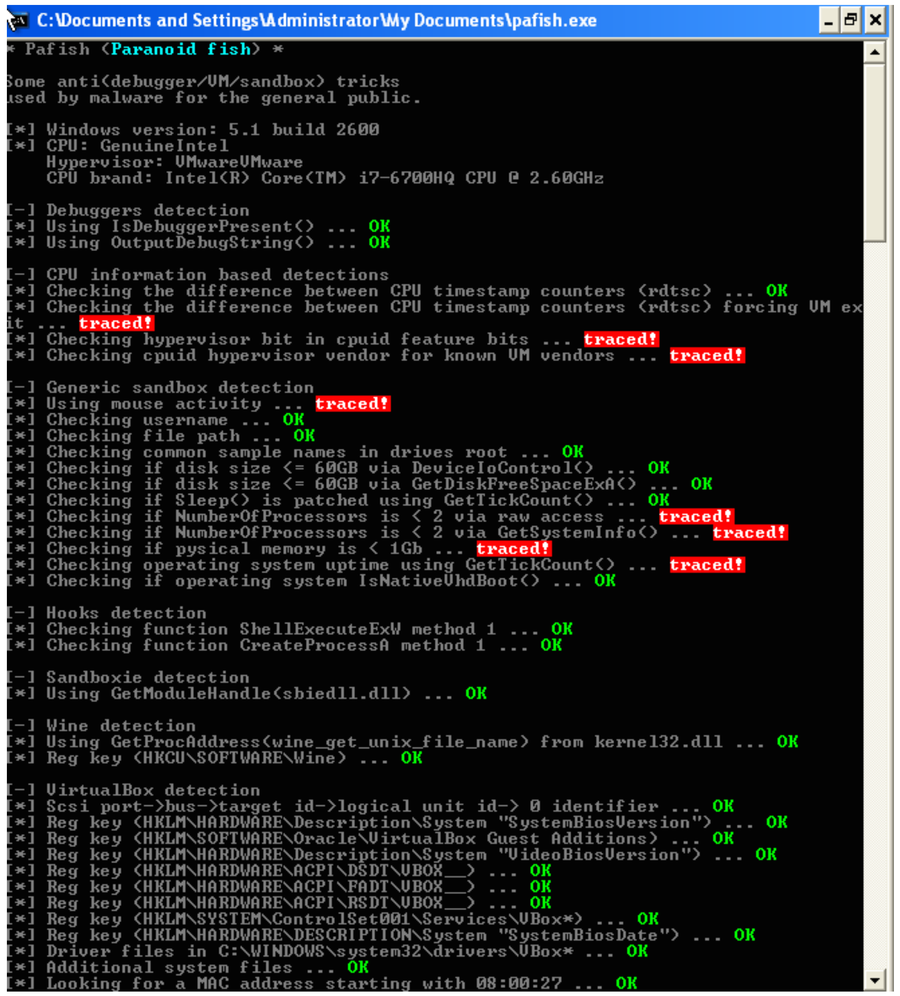
Cuckoo Sandbox Schema

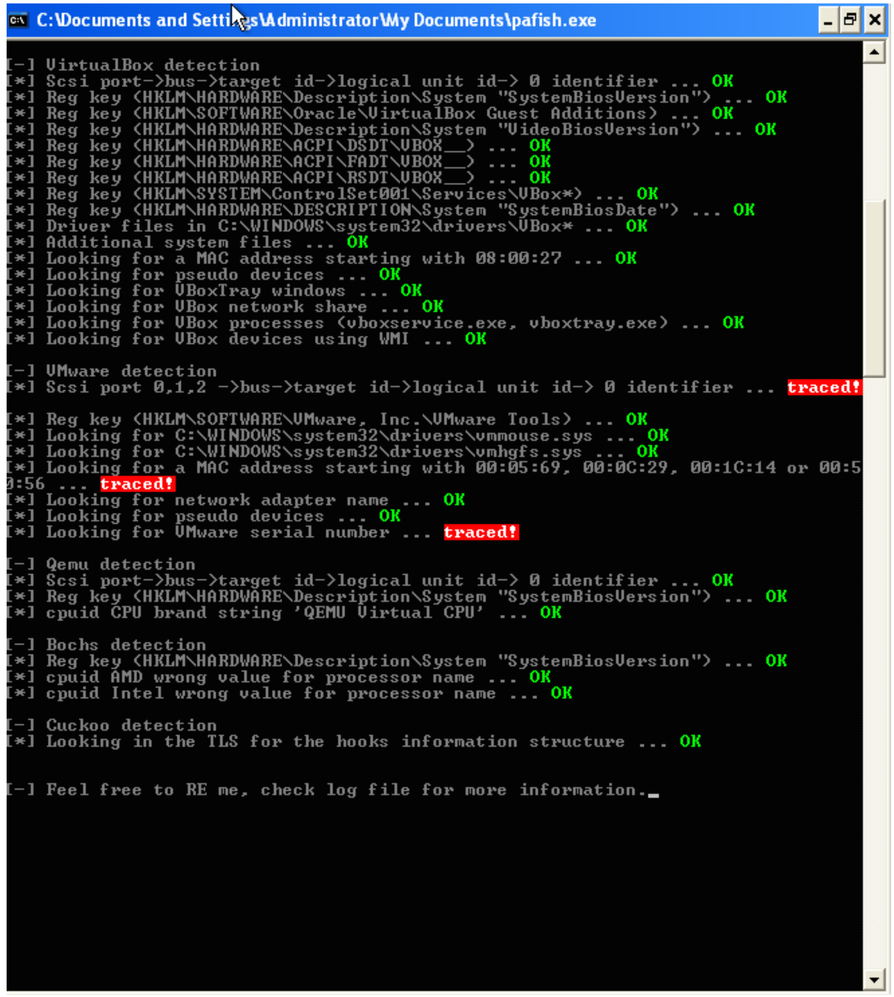


Guest OS [Windows XP SP3] in Virtual Box

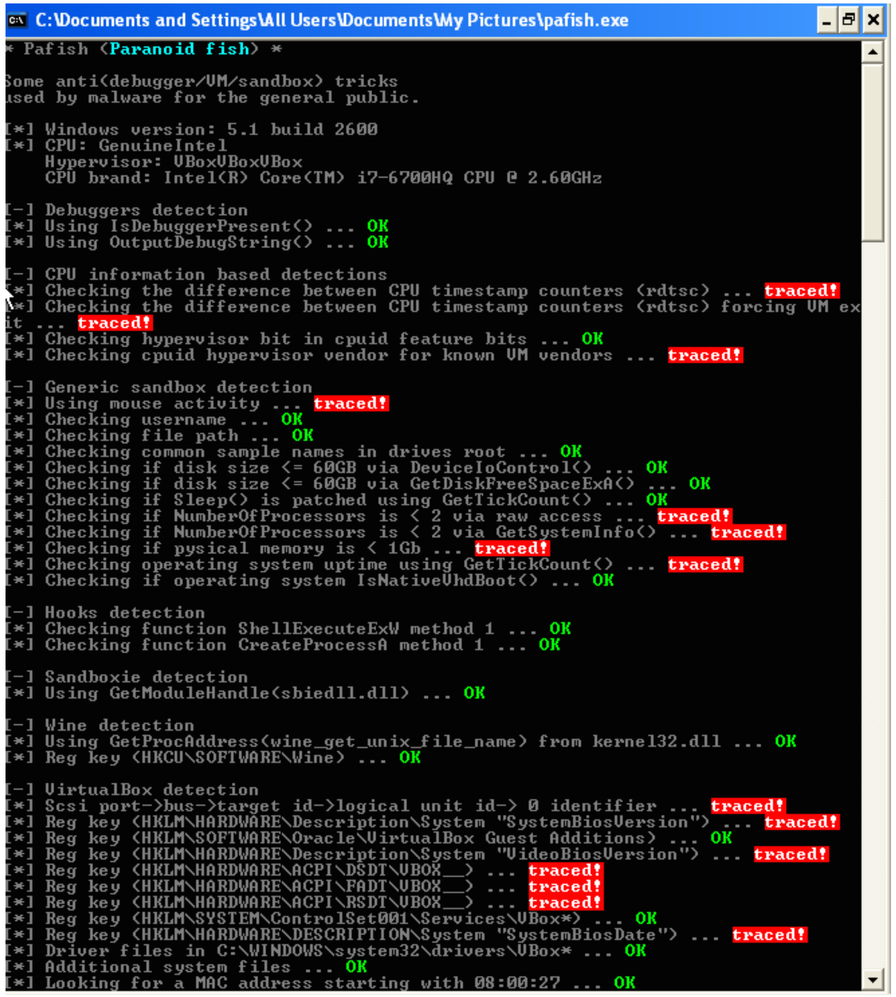


VMCloak WinXP Result in VMWare





VMCloak WinXP Result in Virtual Box



Summary VM Guest Comparison Results

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

CCleaner 5.35 Setup.exe

- Try to identified 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)	Info
2	Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)	
3	This executable is signed	
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)	**Warning**
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 sofware 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)	
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)	Alert
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)	
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**
Signatures Comparison	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)
	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
Signatures Comparison	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)
		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)	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	Destinatio	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

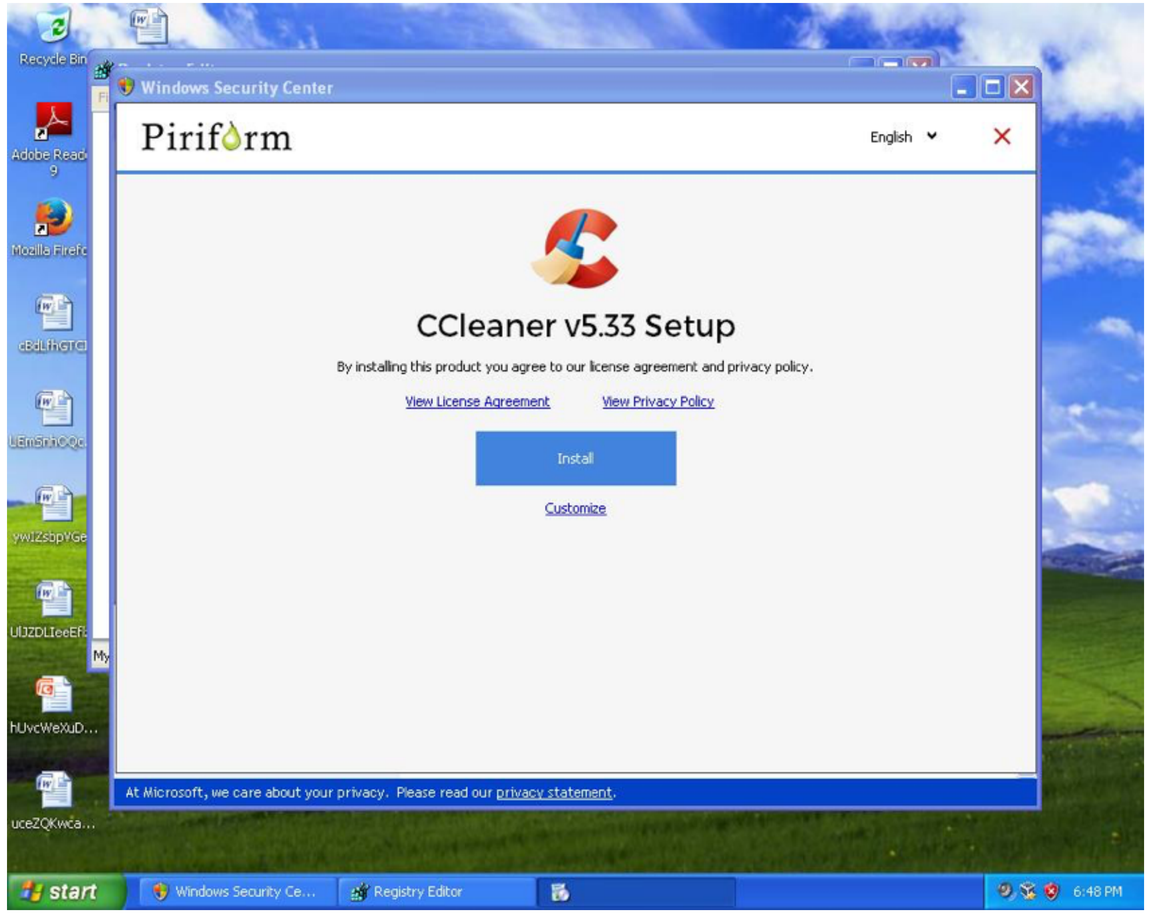
Name	Response	Post-Analysis Lookup
time.windows.com		
service.piriform.com		151.101.8.64
ab890e964c34.com		72.5.65.111
www.piriform.com		151.101.8.64

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**
Signatures Comparison	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)
	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'virtual_address': u'0x00691000', u'entropy': 6.800257473603851, u'name': u'.rsrc', u'virtual_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	

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'virtual_address': u'0x00691000', u'entropy': 6.800257473603851, u'name': u'.rsrc', u'virtual_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	success	0	0	
	region_size: 262144				
	protection: 64 (PAGE_EXECUTE_READWRITE)				
	base_address: 0x01840000				
	allocation_type: 8192 (MEM_RESERVE)				
	process_handle: 0xffffffff				
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	success	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	success	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'virtual_address': u'0x00691000', u'entropy': 6.800257473603851, u'name': u'.rsrc', u'virtual_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'virtual_address': u'0x00691000', u'entropy': 6.800257473603851, u'name': u'.rsrc', u'virtual_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

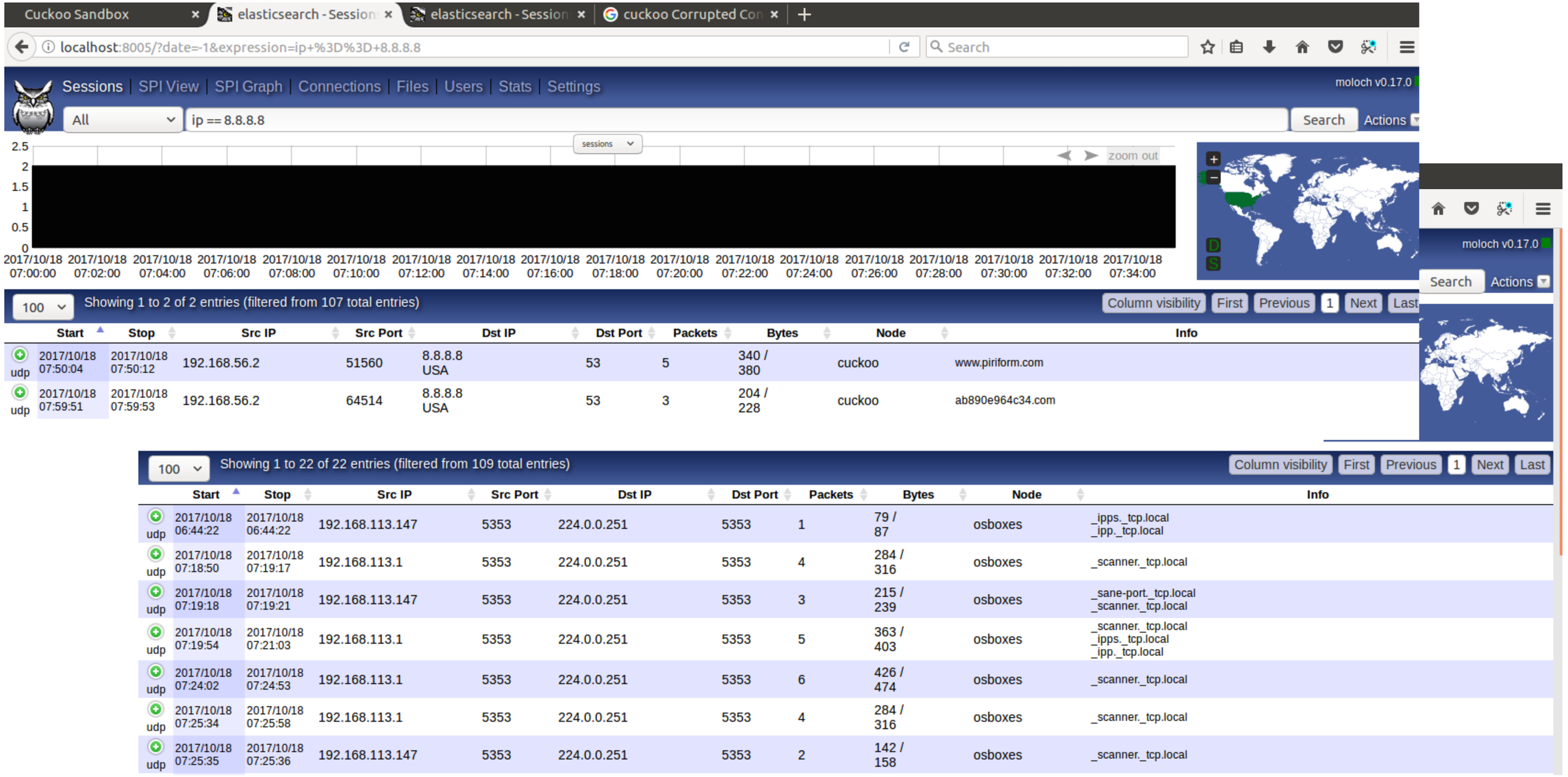
Suricata Alerts

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


Cuckoo Sandbox
elasticsearch - Session
elasticsearch - Session
cuckoo Corrupted Con
localhost:8005/?date=-1&expression=ip+%3D%3D+8.8.8.8
Search
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
1.5
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
100
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
udp 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
udp 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
moloch v0.17.0
Search
Actions
100
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
udp 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
udp 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
udp 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
udp 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
udp 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
udp 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
udp 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

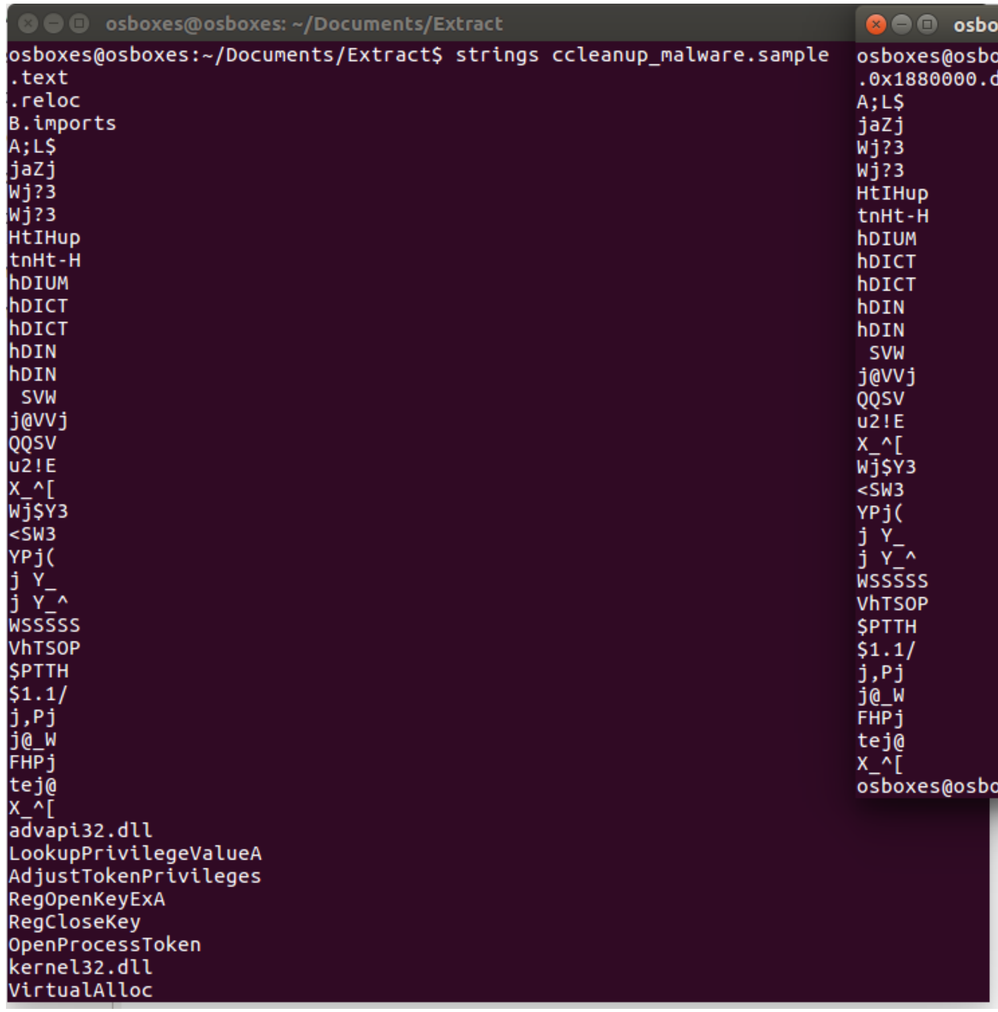
Little Bit Memory Analysis

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.”

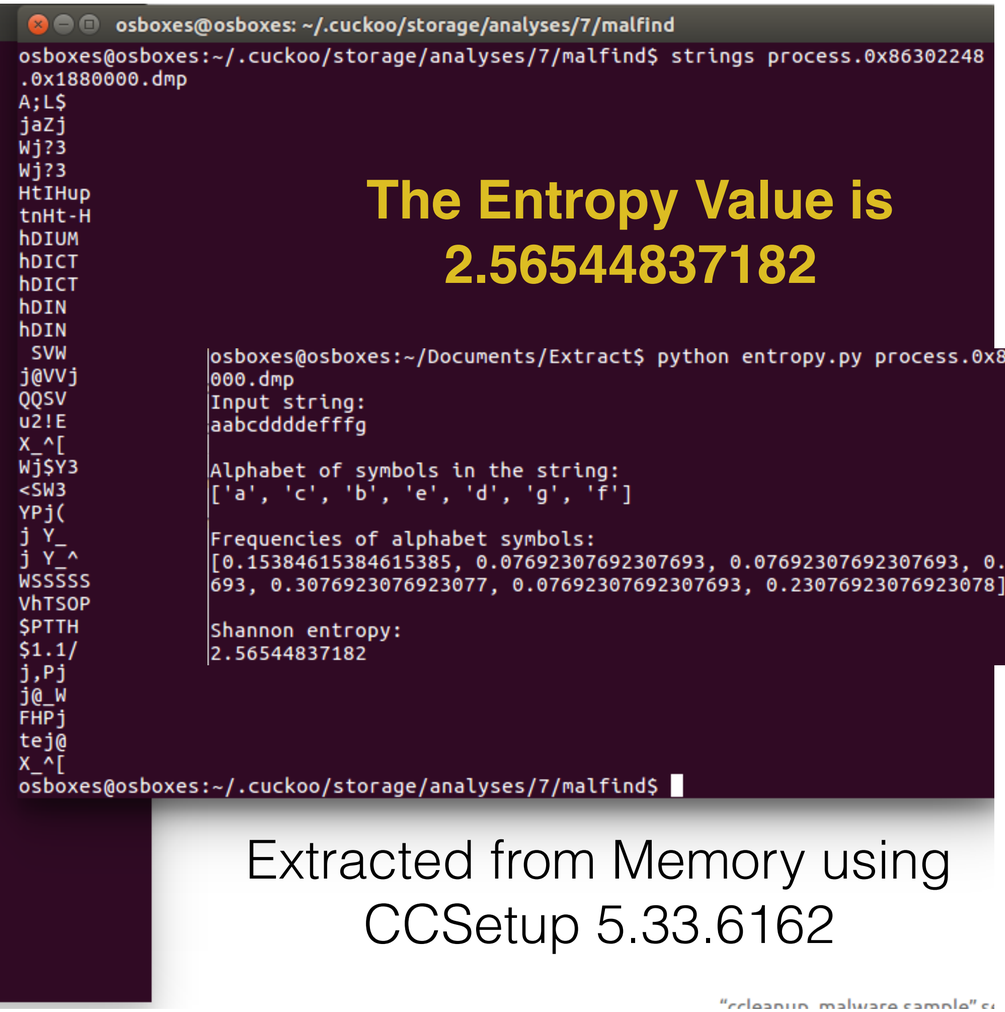
```
osboxes@osboxes:~/.cuckoo/storage/analyses/8$ vol.py -f memory.dmp --profile=WinXPSP3x86 malfind
Volatility Foundation Volatility Framework 2.6
Process: csrss.exe Pid: 584 Address: 0x7f6f0000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

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

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-0xffffff], 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



Sample from @jaytezer in VirusTotal

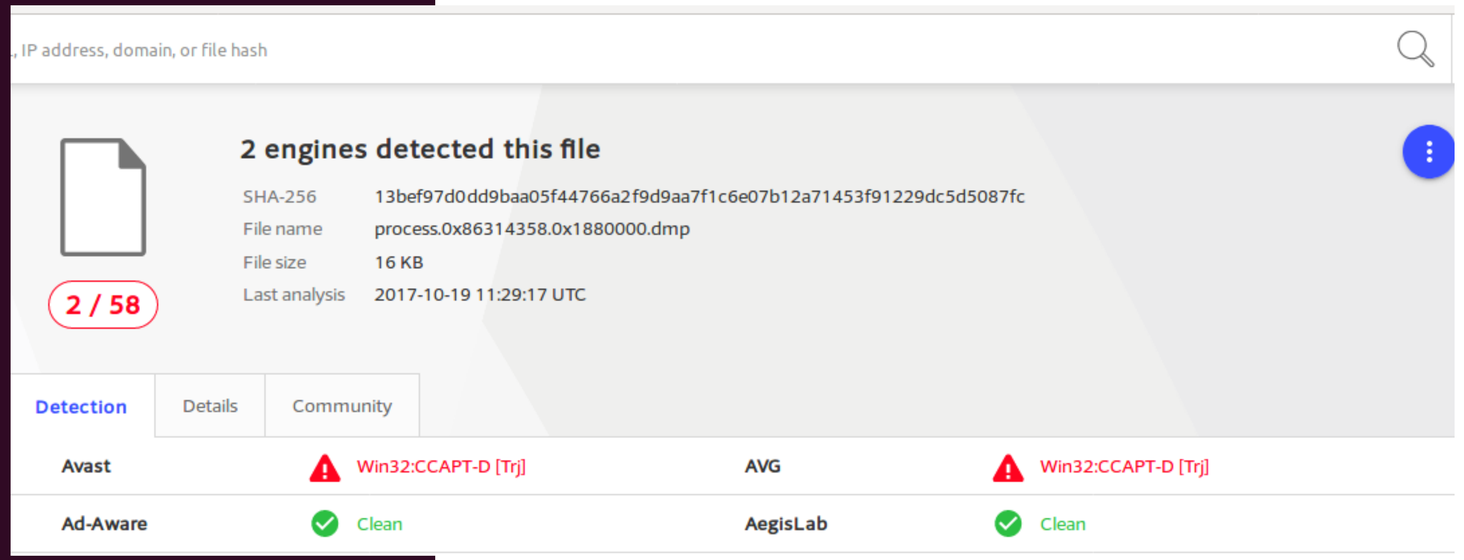


Extracted from Memory using CCSetup 5.33.6162

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      x77dfc238 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



CCleaner 5.33.6162 Extracted Malware

Guest Machine	Simple Harden	VMCloak
Timeout	120	120
Signature	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)	
	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

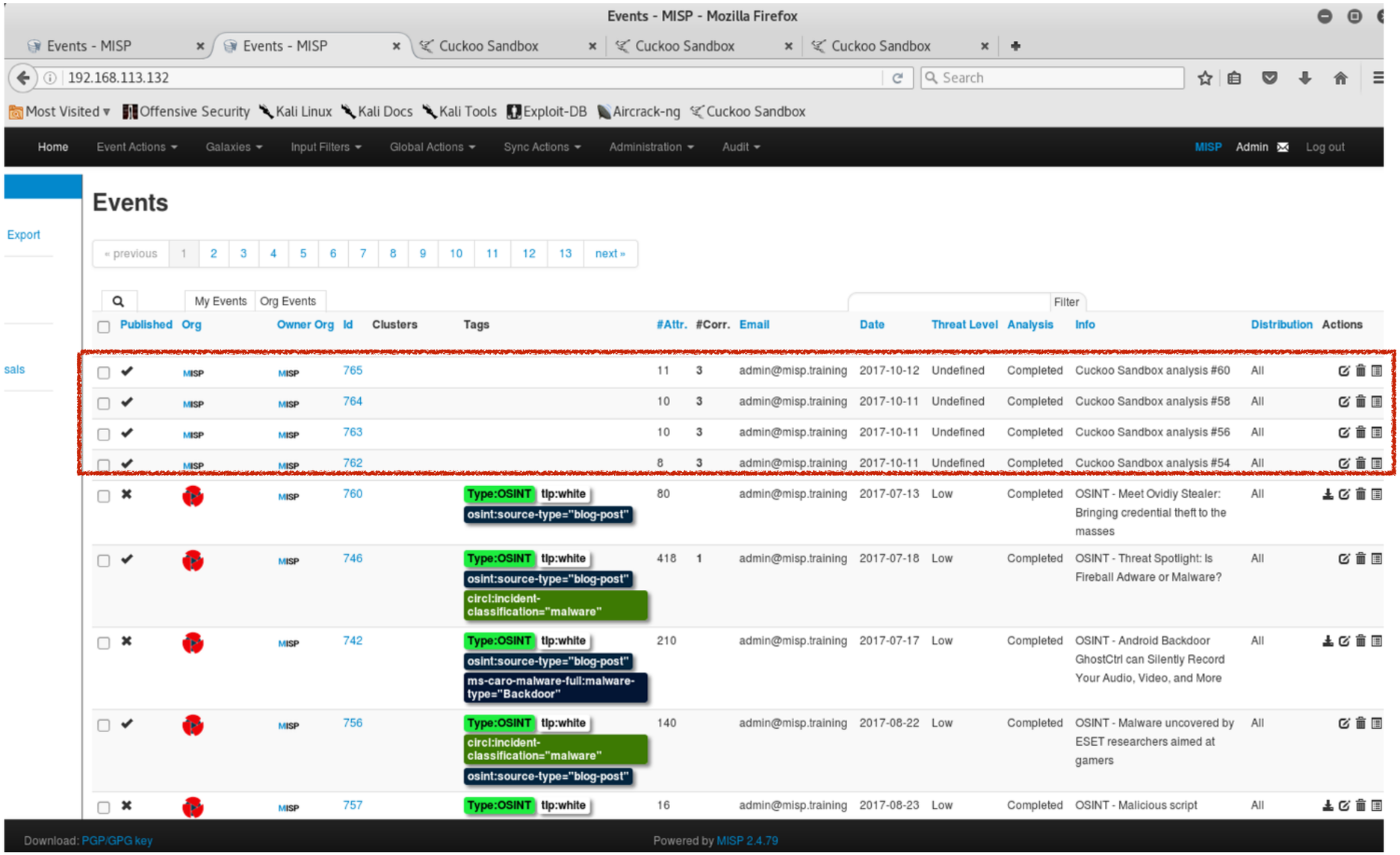
advapi32.dll	kernel32.dll	msvcrt.dll	psapi.dll	ws2_32.dll
LookupPrivilegeValueA	VirtualAlloc	sprintf	GetModuleFileNameExA	WSAStartup
AdjustTokenPrivileges	LocalFree	strlen		gethostbyname
RegOpenKeyExA	LocalAlloc	strncpy	**wininet.dll**	
RegCloseKey	lstrcmpiA	memcpy	InternetCloseHandle	**iphlpapi.dll**
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**	**120**	**1200**
CCleaner Setup 5.35 (Normal)	7.4	**7.8**	**7**	**16.8**
Portable CC 5.33.6162	12	14.2	12.4	14.8
CCleaner Setup 5.33.6162	**5.4**	**5.4**	5.6	21
Extracted Malware	3 **)	-	1.4 **)	-

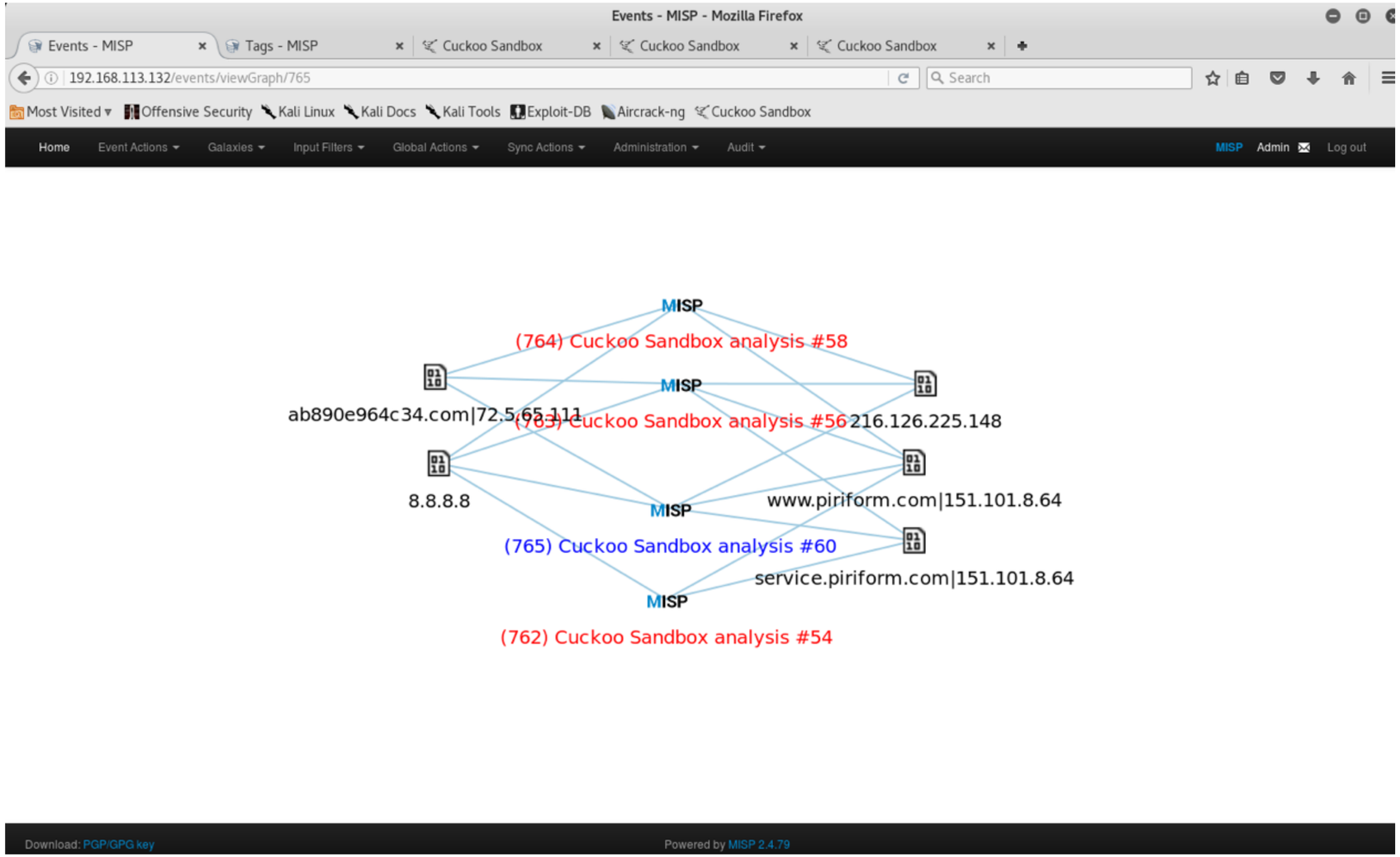
*) Test result using global routing options
**) as execute file

MISP Results



Cuckoo analysis result are fed into MISP events

MISP : Sharing is Caring

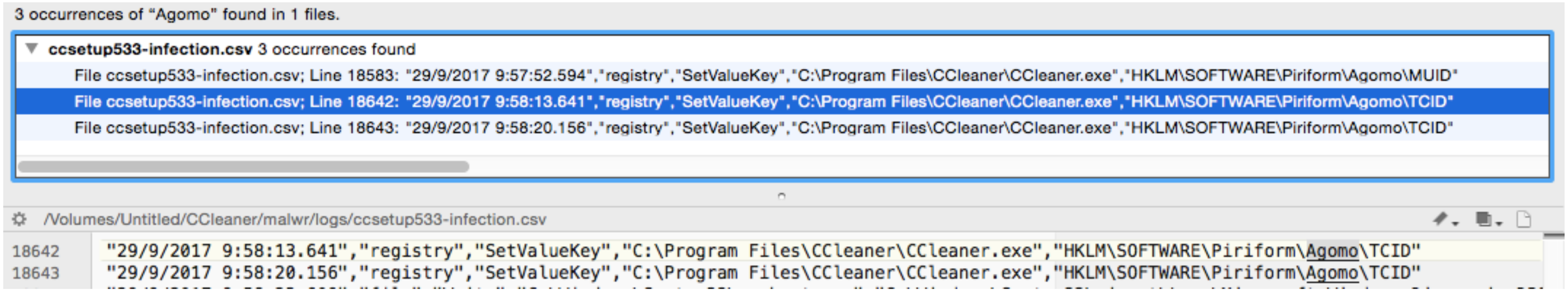


- MISP node represent an organisation
- The same colour in the text represent the similar input events (with different ID)
- Cuckoo results feeds into MISP, then MISP can make a correlation
- Imagine if we can integrated all the effort, there will be no more redundant analysis and we can easily aware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



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: ctldl.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 | PublicMemoryIma... | CNIT 123 F

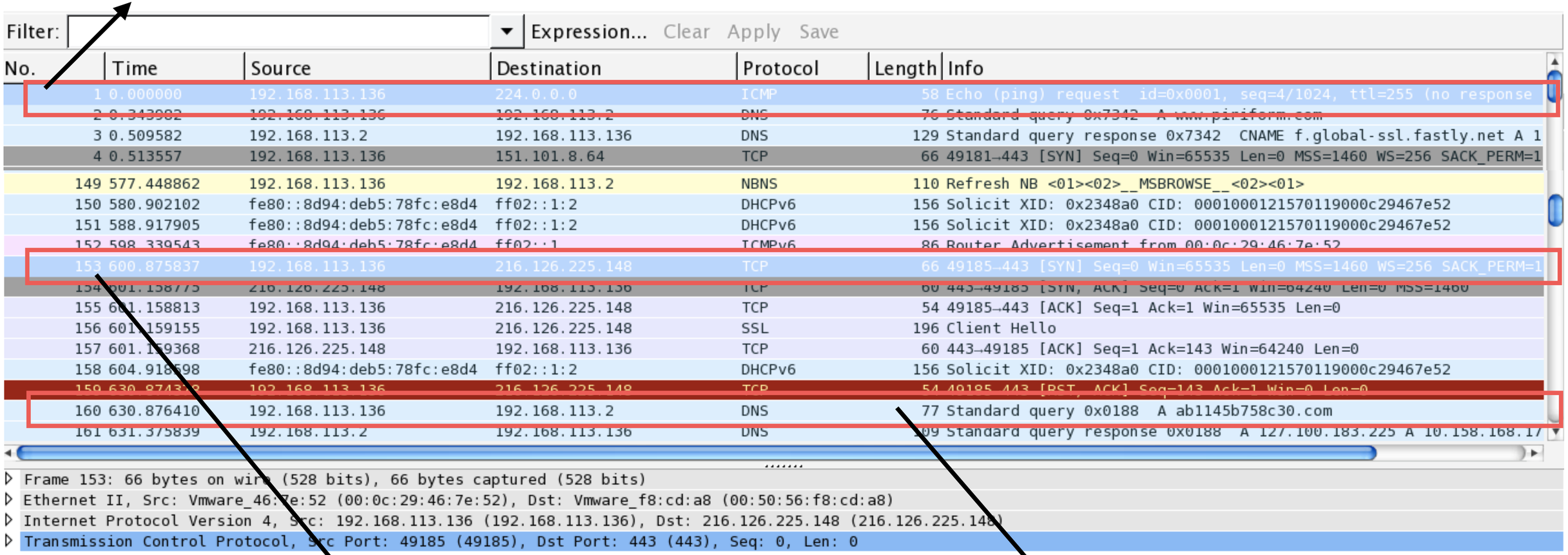
Values added: 684

```
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 0
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\AIT\RunsSinceLastShimClear: 0x000
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Superfetch\DecompressRateKB: E4 E0 05 00 DE AB 0
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
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



Contact IP 216.126.225.148 at 600.875037

September (2017-09)

Contact Domain ab1145b578c30.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

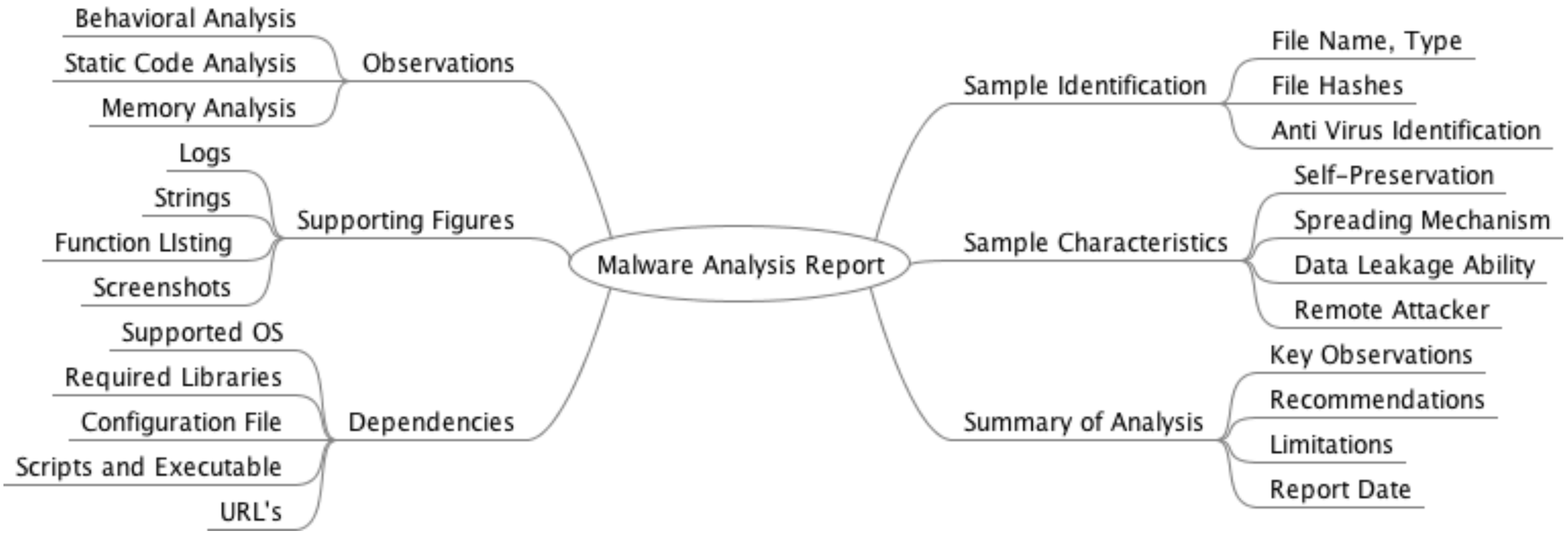
- in the file “lib/cuckoo/core/plugins.py”

```
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


Malware Analysis Report
Observations
Behavioral Analysis
Static Code Analysis
Memory Analysis
Supporting Figures
Logs
Strings
Function LIsting
Screenshots
Dependencies
Supported OS
Required Libraries
Configuration File
Scripts and Executable
URL's
Sample Identification
File Name, Type
File Hashes
Anti Virus Identification
Sample Characteristics
Self-Preservation
Spreading Mechanism
Data Leakage Ability
Remote Attacker
Summary of Analysis
Key Observations
Recommendations
Limitations
Report Date

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** Symantec — Backdoor.Trojan TrendMicro-HouseCall — TROJ_GEN.R011C0DIK17 Kaspersky — HEUR:Trojan.Win32.Axiombase.gen BitDefender — Trojan.GenericKD.12388319	**Portable** Symantec — Trojan.Sibakdi TrendMicro-HouseCall — BKDR_CCHACK.A Kaspersky — Backdoor.Win32.InfeCleaner.a BitDefender — Trojan.PRForm.A
Dependencies	Supported OS	Windows OS (32 and 64-bit)	
	Required Libraries	advapi32.dll, kernel32.dll, msvcrt.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	
	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
Summary of Analysis	Key Observations	Agomo Registry Value, PDB Path, ICMP Traffic, DGA
	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 Sanbox Documentation, http://docs.cuckoosandbox.org/

“Kechilafan satu orang sahaja tjukup sudah menjebabkan keruntuhan negara”

Dr. Roebiono Kertopati