Malware Sandbox Analysis

Why manual, when you can automated?

Introduction to Sandbox

- Execute malware in a controlled/monitored environment
- Most importantly, safe!
  - without fear of harming “real” systems
- Monitors file system, registry, process and network activity
- The result is impresive
- Examples
  - Cuckoo Sandbox
  - Falcon Sandbox
  - Any.run Sandbox

Why sandbox analysis?

- Automated and speed up analysis
- Sandboxes provide easy-to-understand output
- Complete command execution
- Ease of Use
- To determine
  - The nature and purpose of the malware
  - Interaction with the file system
  - Interaction with the registry
  - Interaction with the network
  - To determine identifiable patterns

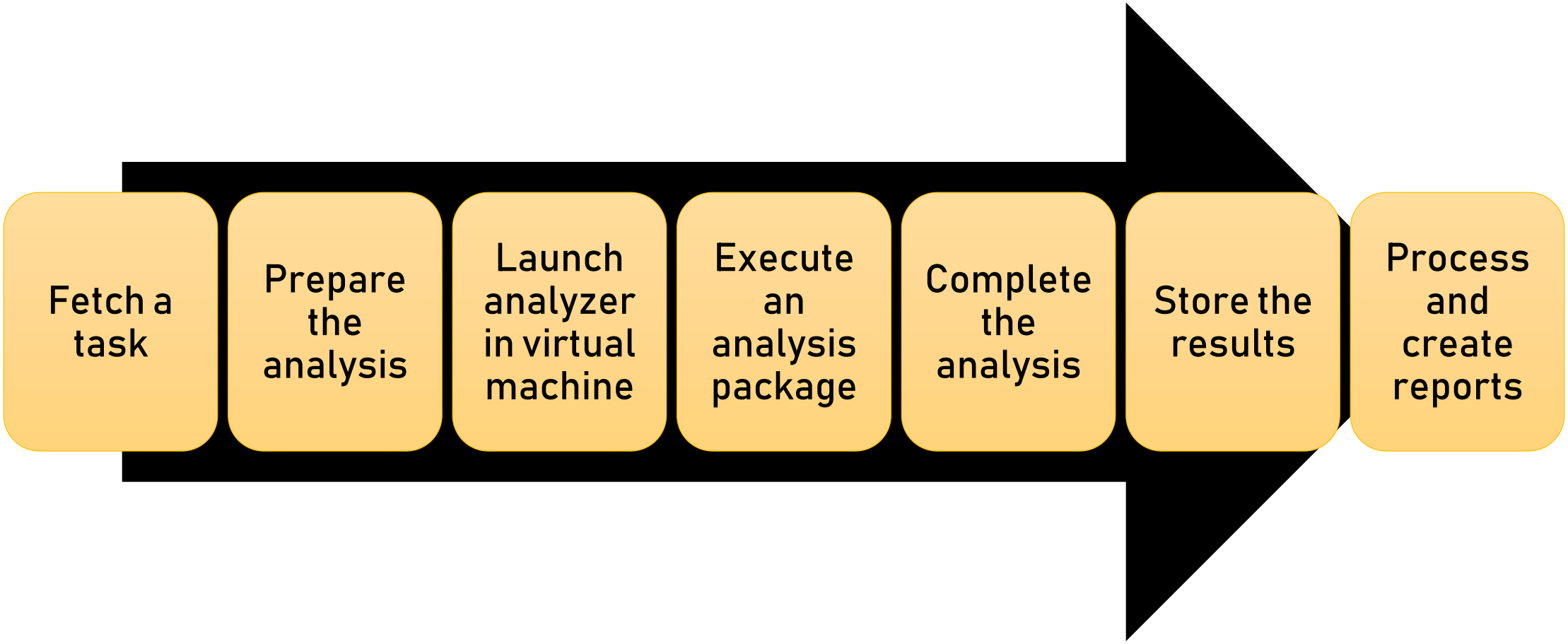
Disadvantage in Sandboxing

- Commercial tool were costing
- No guarantee the malware will work the same as in the real world
- Sandbox can be detected
- Results can be confusing or overwhelming
- Automation of exploit analysis is not trivial

Cuckoo Sandbox

- Open source automated malware analysis system
- Uses virtualization (VirtualBox, KVM, VMWare)
- Python based, easy to customize
- Multiple report types (JSON, HTML, MAEC)

Execution flow in Cuckoo



Support packages

- EXE
  - Default – Windows executables
- DLL
  - You can specify a function to use otherwise DllMain
- PDF
  - Launches Acrobat Reader
- DOC or XLS
  - Office, Need to verify path in package is the same as host OS
- IE
  - HTML/JS Browser testing
- BIN
  - Shell code or other generic binary data

Cuckoo working

- Takes sample as input
- Performs static analysis
- Reverts VM to clean snapshot
- Starts the VM
- Transfers the malware to VM
- Runs the monitoring tools (to monitor process, registry, file system, network activity)
- Executes the malware for the specified time

Cuckoo working (cont)

- Stops the monitoring tools
- Suspends the VM
- Acquires the memory image
- Performs memory analysis using Volatility framework
- Stores the results (Final reports, destkop screenshot, pcaps and malicious artifacts for later analysis)

Cuckoo Report

- Static Analysis results
  - File type (uses magic python module)
  - Cryptographic hash (md5sum – uses hashlib python module)
  - VirusTotal results (python script using VirusTotal's public api)
  - Determines packers used by malware (uses yara-python)
  - Determines the capabilities of the malware like IRC, P2P etc etc (uses yara-python module)

Cuckoo Report (cont)

- Dynamic Analysis results
  - Determines File system activity
  - Determines Process activity
  - Determines Registry activity
  - Monitor Network activity
  - Displays DNS summary
  - Shows TCP conversations
  - Displays HTTP requests & HTTP request tree

Cuckoo Report (cont)

- Memory Analysis results
  - uses Volatility advanced memory forensics framework
  - displays process, hidden process in memory
  - displays network connections, terminated network connections
  - displays listening sockets
  - determines api hooks, code injection and embedded executable in memory
  - displays DLL's loaded by the process memory
  - displays services in memory
  - displays the registry keys (like run registry key)

Cuckoo Time!

Setup offline Cuckoo?

Online Cuckoo

- https://www.malwar.ee/
- https://cuckoo.cert.ee/
- https://sandbox.pikker.ee/

cuckoo Dashboard Recent Pending Search Submit Import

Insights

Cuckoo Installation

Version	2.0.6

You are up to date.

Usage statistics

reported	1181941
completed	6
total	1195616
running	10
pending	0

From the press:

Click here for more

Cuckoo

SUBMIT A FILE FOR ANALYSIS

SUBMIT URLS/HASHES

Submit URLs/hashes

Submit

Drag your file into the left field or click the icon to select a file.

System info

free used total

FREE DISK SPACE | CPU LOAD | MEMORY USAGE

Analysing

cuckoo Dashboard Recent Pending Search Submit Import

~~submit file~~ » ~~configure~~ » ~~analyze~~ » Summary

✔ Your submission has been received and the tasks are being processed!

Next: View pending tasks Submit again

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	
1196492	26/08/2019 08:31	hxxp://amazon.co.uk.security-check.ga	ie	running
		Done		

Very first page after analyzing

cuckoo | Dashboard | Recent | Pending | Search | Submit | Import

Summary

Basic fingerprinting and static analysis

Malware scoring

Wannacry.exe

File *Wannacry.exe*

Summary | Download | Resubmit sample

Size	3.4MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA512	Show SHA512
CRC32	4022FCAA
ssdeep	98304:QqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3x:QqPe1Cxcxk3ZAEUadzR8yc4gB
Yara	None matched

Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs
FILE	July 24, 2019, 10:11 a.m.	July 24, 2019, 10:14 a.m.	192 seconds	none	Show Analyzer Log Show Cuckoo Log

Score

This file is **very suspicious**, with a score of **17.8 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

Feedback

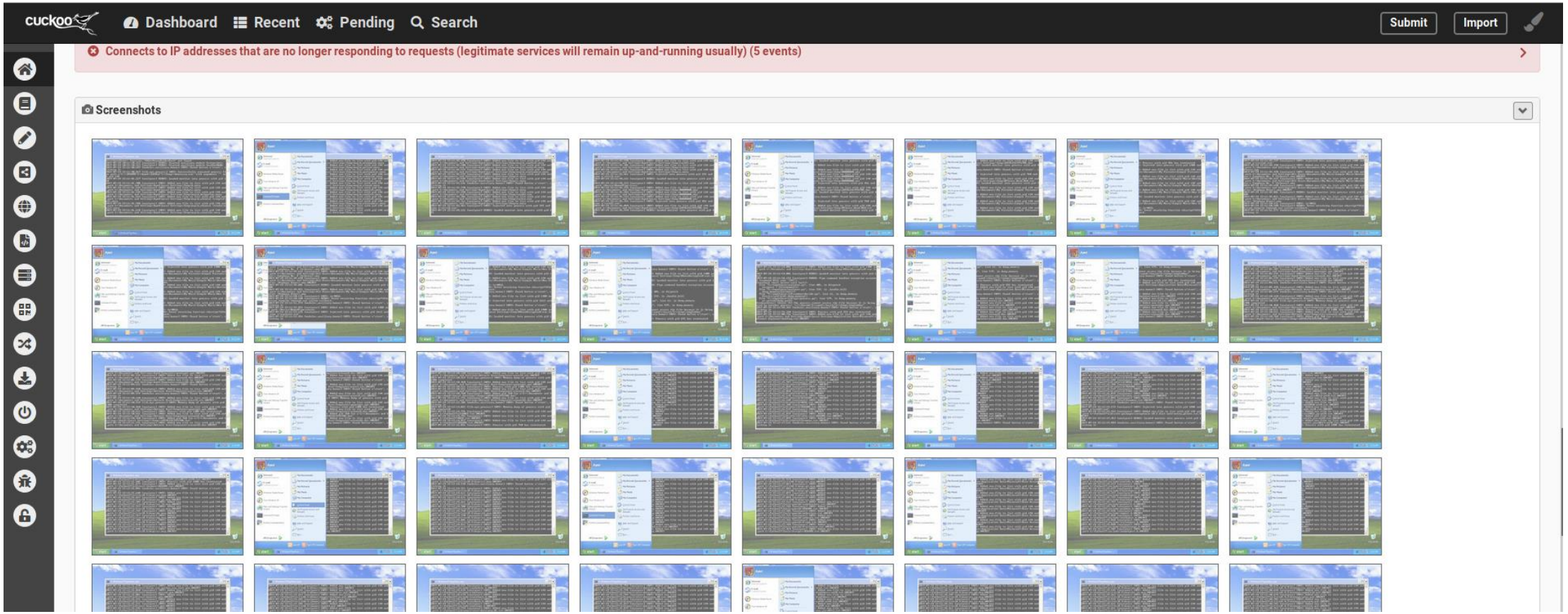
Expecting different results? Send us this analysis and we will inspect it. Click here

Signatures

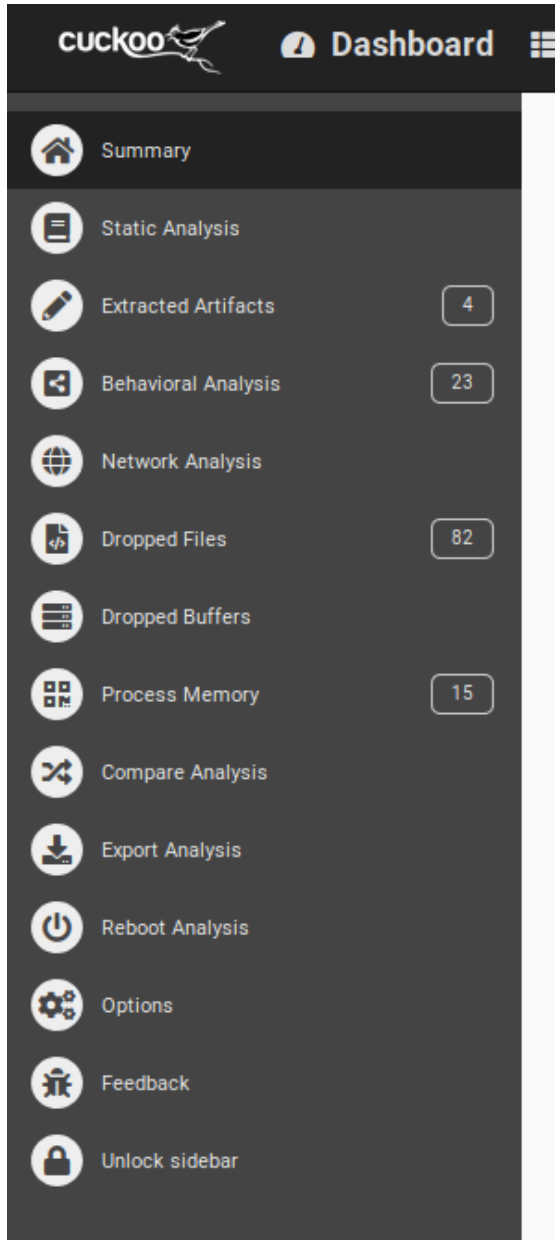
Signatures

- Queries for the computername (12 events)
- Checks if process is being debugged by a debugger (4 events)
- Command line console output was observed (18 events)
- Uses Windows APIs to generate a cryptographic key (4 events)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- The executable uses a known packer (1 event)
- The file contains an unknown PE resource name possibly indicative of a packer (1 event)
- Starts servers listening (10 events)
- Allocates read-write-execute memory (usually to unpack itself) (1 event)
- A process attempted to delay the analysis task. (1 event)
- Queries the disk size which could be used to detect virtual machine with small fixed size or dynamic allocation (5 events)

Screenshots on every Desktop behavior



Side bar


cuckoo
Dashboard
Summary
Static Analysis
Extracted Artifacts
4
Behavioral Analysis
23
Network Analysis
Dropped Files
82
Dropped Buffers
Process Memory
15
Compare Analysis
Export Analysis
Reboot Analysis
Options
Feedback
Unlock sidebar

Static analysis with Cuckoo!

Static Analysis | Strings | Antivirus | IRMA

PE Compile Time

2010-11-20 11:05:05

PE Imphash

68f013d7437aa653a8a98a05807afeb1

Version Infos

LegalCopyright	\xa9 Microsoft Corporation. All rights reserved.
InternalName	diskpart.exe
FileVersion	6.1.7601.17514 (win7sp1_rtm.101119-1850)
CompanyName	Microsoft Corporation
ProductName	Microsoft\xae Windows\xae Operating System
ProductVersion	6.1.7601.17514
FileDescription	DiskPart
OriginalFilename	diskpart.exe
Translation	0x0409 0x04b0

PEiD Signatures

Portable Executable analysis

PEiD Signatures

Armadillo v1.71

Sections

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
.text	0x00001000	0x000069b0	0x00007000	6.4042351061
.rdata	0x00008000	0x00005f70	0x00006000	6.66357096841
.data	0x0000e000	0x00001958	0x00002000	4.45574950787
.rsrc	0x00010000	0x00349fa0	0x0034a000	7.9998679751

Resources

Name	Offset	Size	Language	Sub-language	File type
XIA	0x000100f0	0x00349635	LANG_ENGLISH	SUBLANG_ENGLISH_US	Zip archive data, at least v2.0 to extract
RT_VERSION	0x00359728	0x00000388	LANG_ENGLISH	SUBLANG_ENGLISH_US	data
RT_MANIFEST	0x00359ab0	0x000004ef	LANG_ENGLISH	SUBLANG_ENGLISH_US	exported SGML document, ASCII text, with CRLF line terminators

Imports

Imports

Library KERNEL32.dll:

- 0x40802c GetFileAttributesW
- 0x408030 GetFileSizeEx
- 0x408034 CreateFileA
- 0x408038 InitializeCriticalSection
- 0x40803c DeleteCriticalSection
- 0x408040 ReadFile
- 0x408044 GetFileSize
- 0x408048 WriteFile
- 0x40804c LeaveCriticalSection
- 0x408050 EnterCriticalSection
- 0x408054 SetFileAttributesW
- 0x408058 SetCurrentDirectoryW
- 0x40805c CreateDirectoryW
- 0x408060 GetTempPathW
- 0x408064 GetWindowsDirectoryW

Library USER32.dll:

- 0x4081d0 wsprintfA

Library ADVAPI32.dll:

- 0x408000 CreateServiceA
- 0x408004 OpenServiceA
- 0x408008 StartServiceA
- 0x40800c CloseServiceHandle
- 0x408010 CryptReleaseContext
- 0x408014 RegCreateKeyW
- 0x408018 RegSetValueExA
- 0x40801c RegQueryValueExA
- 0x408020 RegCloseKey
- 0x408024 OpenSCManagerA

Library MSVCRT.dll:

- 0x408108 realloc
- 0x40810c fclose
- 0x408110 fwrite
- 0x408114 fread
- 0x408118 fopen
- 0x40811c sprintf
- 0x408120 rand
- 0x408124 srand
- 0x408128 strcpy
- 0x40812c memset
- 0x408130 strlen
- 0x408134 wcscat
- 0x408138 wcslen
- 0x40813c __CxxFrameHar
- 0x408140 ??3@YAXPAX@Z

Strings

Static Analysis

Static Analysis | Strings | Antivirus | IRMA

```
!This program cannot be run in DOS mode.
`.rdata
@.data
SVWjcf
WWWWWPj
@4+G4t
q89p8t
V,YYG;~
tlHt Ht
~(9~$u
FP;FTt
k|_^][Y
=j&&LZ66lA??~
}{))R>
f""D~**T
V22dN::t
o%%Jr..\$
&&Lj66lZ??~A
99rKJJ
```

AV signature

Static Analysis | Strings | Antivirus | IRMA

Antivirus	Signature
Bkav	W32.RansomwareTBE.Trojan
MicroWorld-eScan	Trojan.Ransom.WannaCryptor.A
FireEye	Generic.mg.84c82835a5d21bbc
CAT-QuickHeal	Ransom.WannaCrypt.A4
McAfee	Ransom-O
Malwarebytes	Ransom.WannaCrypt
VIPRE	Trojan.Win32.Generic!BT
AegisLab	Trojan.Win32.Wanna.u!c
K7AntiVirus	Trojan (0050d7171)
BitDefender	Trojan.Ransom.WannaCryptor.A

Extracted artifacts

Extracted Artifacts

#1 script / cmd	#2 script / cmd	#3 script / cmd	#4 script /

Extracted

Category:	script
Yara:	None matched
Program:	cmd
First seen:	Aug. 26, 2019, 10:36 a.m.

Script

48331566839929.bat

Behavioral Analysis

- Process tree
- Process contents

Process tree

Process tree

WannaCry.exe "C:\Users\Administrator\AppData\Local\Temp\WannaCry.exe"	2344	
attrib.exe attrib +h .	2604	
icacls.exe icacls . /grant Everyone:F /T /C /Q	2564	
taskdl.exe taskdl.exe	2620	
cmd.exe cmd /c 48331566839929.bat	3040	
cscript.exe cscript.exe //nologo m.vbs	1792	
taskdl.exe taskdl.exe	2264	
@WanaDecryptor@.exe @WanaDecryptor@.exe co	2244	
taskhsvc.exe TaskData\Tor\taskhsvc.exe	2668	
cmd.exe	2896	

Process contents

Process contents

attrib.exe

PID 2604

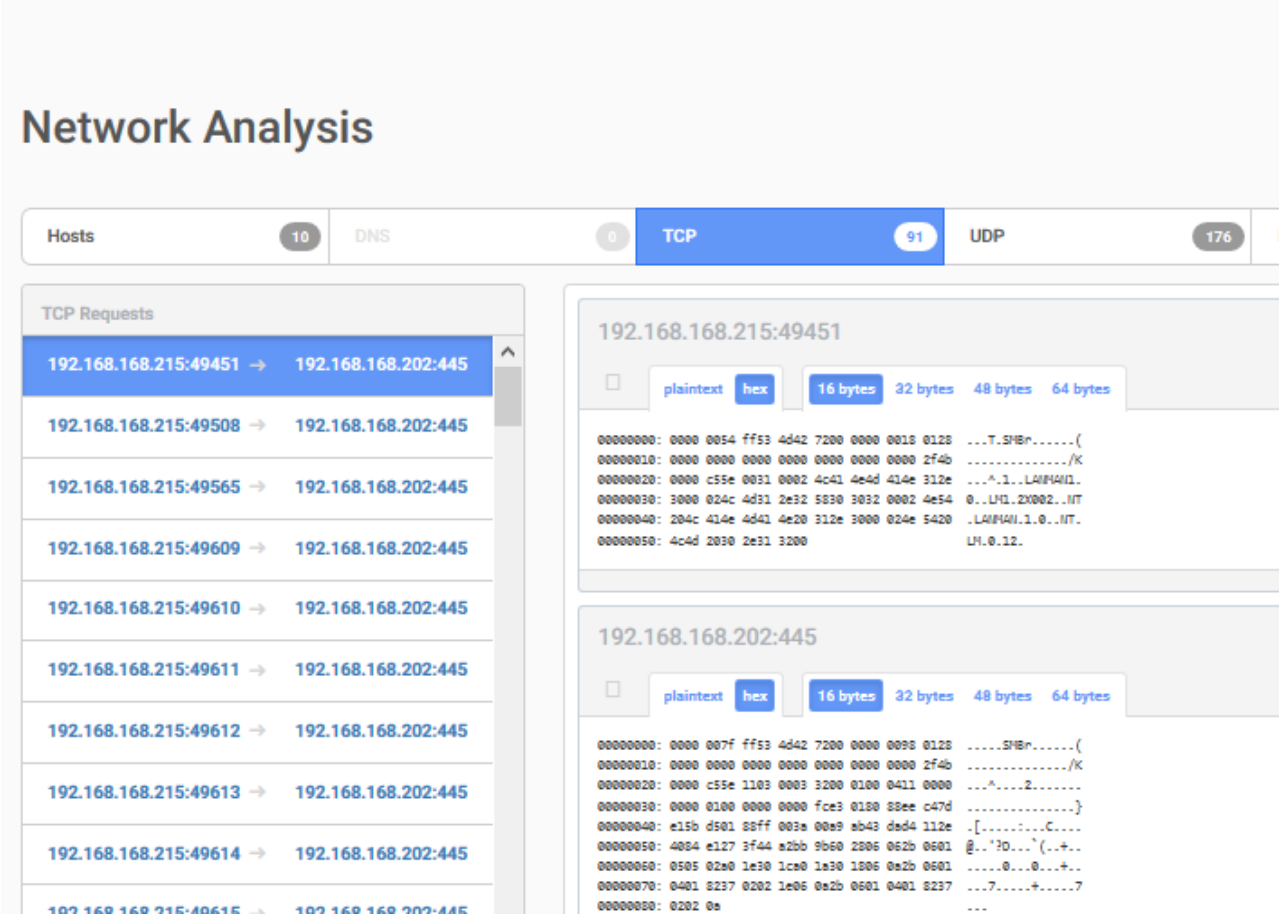
Parent PID 2344

1

default | registry | file | network | process | services | synchronisation | iexplore | office | pdf

Time & API	Arguments	Status	Return	Repeated
GetSystemTimeAsFileTime Aug. 26, 2019, 10:36 a.m.		1	0	0
SetUnhandledExceptionFilter Aug. 26, 2019, 10:36 a.m.			0	0
FindFirstFileExW Aug. 26, 2019, 10:36 a.m.	filepath_r: C:\Users\Administrator\AppData\Local filepath: C:\Users\Administrator\AppData\Local	1	6749080	0
NtClose Aug. 26, 2019, 10:36 a.m.	handle: 0x0000007c	1	0	0
FindFirstFileExW	filepath_r: C:\Users\Administrator\AppData\Local\Temp			

Network Analysis



Process memory

- Dump the executables to dig more

Process Memory

Process memory dump for **taskse.exe** (PID 1036, dump 1)

Extracted/injected images (may contain unpacked executables)

Download #1
Download #2
Download #3
Download #4
Download #5
Download #6
Download #7
Download #8
Download #9
Download #10

Process memory dump for **reg.exe** (PID 1636, dump 1)

Extracted/injected images (may contain unpacked executables)

Download #1
Download #2
Download #3
Download #4
Download #5
Download #6

Let’s analysis by your own!

- Find any malware on the internet
- Present to us what's your finding