

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439...

malicious

This report is generated from a file or URL submitted to this webservice on June 28th 2021 15:07:21 (UTC) Threat Score: 100/100
AV Detection: 98%
Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
Labeled as: Trojan.Ransom.WannaCryptor
Report generated by Falcon Sandbox © Hybrid Analysis

Overview

Sample unavailable

Downloads

External Reports

Re-analyze

Hash Seen Before

Show Similar Samples

Report False-Positive

Request Report Deletion

Post

Link

E-Mail

Incident Response

- Incident Response
- Related Sandbox Artifacts
- Indicators
- File Details
- Screenshots (4)
- Hybrid Analysis (30)
- Network Analysis
- Extracted Strings
- Extracted Files (1905)
- Notifications
- Community (80)

Back to top

Risk Assessment

Remote Access	Reads terminal service related keys (often RDP related)
Ransomware	Deletes volume snapshots (often used by ransomware) Detected indicator that file is ransomware
Spyware	Deletes volume snapshots (often used by ransomware)
Persistence	Disables startup repair Grants permissions using icaccls (DACL modification) Spawns a lot of processes Tries to suppress failures during boot (often used to hide system changes) Writes data to a remote process
Fingerprint	Queries kernel debugger information Queries process information Reads system information using Windows Management Instrumentation Commandline (WMIC) Reads the active computer name Reads the cryptographic machine GUID
Evasive	Marks file for deletion Possibly checks for the presence of an Antivirus engine
Network Behavior	Contacts 9 hosts. View all details

MITRE ATT&CK™ Techniques Detection

This report has 34 indicators that were mapped to 26 attack techniques and 10 tactics.

[View all details](#)

Additional Context

OSINT

External References	https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168 https://www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/ https://misp.local/events/453.json
---------------------	---









À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Paramètres des cookies

Tout refuser

Autoriser tous les cookies

<div><div>HYBRID ANALYSIS</div><div><div> ▾</div><div> ▾</div><div></div><div> ▾</div><div><div> Request Info</div><div> ▾</div></div></div></div> <div><div></div><div><div></div><div> ▾</div></div></div>	
Associated SHA25...	c99c0d11167064f60f231993b753d4966ac1f3a3d70c3dd73a5e9f3300382e33
Associated URLs	<div>hxxps://github.com/ytisf/theZoo/raw/master/malware/Binaries/Ransomware.WannaCry/Ransomware.WannaCry.zip</div> <div>hxxps://raw.githubusercontent.com/Explodingstuff/WannaCry/master/WannaCry.EXE</div> <div>hxxps://github.com/Explodingstuff/WannaCry/blob/master/WannaCry.EXE?raw=true</div> <div>hxxps://github.com/limiteci/WannaCry/blob/main/WannaCry.EXE?raw=true</div>










Indicators

 Not all malicious and suspicious indicators are displayed. [Get your own cloud service](#) or the [full version](#) to view all details.

Malicious Indicators	17
Anti-Detection/Stealthyness	
Tries to suppress failures during boot (often used to hide system changes)	▾
External Systems	
Sample was identified as malicious by a large number of Antivirus engines	▾
Sample was identified as malicious by at least one Antivirus engine	▾
General	
The analysis extracted a file that was identified as malicious	▾
The analysis spawned a process that was identified as malicious	▾
Installation/Persistence	
Allocates virtual memory in a remote process	▾
Writes data to a remote process	▾
Network Related	
Uses network protocols on unusual ports	▾
Pattern Matching	
YARA signature match	▾
Ransomware/Banking	
Deletes backup catalog	▾
Deletes volume snapshots (often used by ransomware)	▾









À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

 <div><div> ▾</div><div> ▾</div><div> ▾</div><div> ▾</div><div><div> Request Info</div><div>▾</div></div></div> <div><div></div><div><div></div><div></div></div></div>	<div>Modifies the access control lists of files</div> <div>▼</div>	
Unusual Characteristics		
<div>Spawns a lot of processes</div> <div>▼</div>		
Hiding 2 Malicious Indicators		
<div>All indicators are available only in the private webservice or standalone version</div>		
Suspicious Indicators	<div>36</div>	
Anti-Reverse Engineering		
<div>PE file has unusual entropy sections</div> <div>▼</div>		
Environment Awareness		
<div>Reads the active computer name</div> <div>▼</div>		
<div>Reads the cryptographic machine GUID</div> <div>▼</div>		
General		
<div>Reads configuration files</div> <div>▼</div>		
Installation/Persistence		
<div>Drops executable files</div> <div>▼</div>		
Network Related		
<div>Found potential IP address in binary/memory</div> <div>▼</div>		
<div>Sends traffic on typical HTTP outbound port, but without HTTP header</div> <div>▼</div>		
Ransomware/Banking		
<div>Detected indicator that file is ransomware</div> <div>▼</div>		
<div>Detected text artifact in screenshot that indicate file could be ransomware</div> <div>▼</div>		
<div>The input sample dropped very many files</div> <div>▼</div>		
Remote Access Related		
<div>Reads terminal service related keys (often RDP related)</div> <div>▼</div>		
Spyware/Information Retrieval		
<div>Reads system information using Windows Management Instrumentation Commandline (WMIC)</div> <div>▼</div>		
System Destruction		
<div>Marks file for deletion</div> <div>▼</div>		
<div>Opens file with deletion access rights</div> <div>▼</div>		
System Security		

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

<div><div>HYBRID ANALYSIS</div><div><div>▼</div><div>▼</div><div></div><div>▼</div><div> Request Info ▼</div></div></div> <div><div></div><div></div><div>▼</div></div>	
CRC value set in PE header does not match actual value	▼
Imports suspicious APIs	▼
Installs hooks/patches the running process	▼
Reads information about supported languages	▼
Timestamp in PE header is very old or in the future	▼
Hiding 15 Suspicious Indicators	
All indicators are available only in the private webservice or standalone version	
Informative25	
Anti-Reverse Engineering	
PE file contains zero-size sections	▼
Environment Awareness	
Executes WMI queries	▼
External Systems	
Detected Suricata Alert	▼
General	
Contacts server	▼
Creates mutants	▼
Drops files marked as clean	▼
Launches a VBS file	▼
Loads rich edit control libraries	▼
Logged script engine calls	▼
Overview of unique CLSIDs touched in registry	▼
Process launched with changed environment	▼
Runs shell commands	▼
Scanning for window names	▼
Spawns new processes	▼
Spawns new processes that are not known child processes	▼
The input sample possibly contains the RDTSCP instruction	▼
Installation/Persistence	
Connects to IP ports	▼

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

File Sections

Name	Entropy	Virtual Address	Virtual Size	Raw Size	MD5	Characteristics
.text	6.4042351061	0x1000	0x69b0	0x7000	920e964050a1a5dd60dd00083fd541a2	-
.rdata	6.66357096841	0x8000	0x5f70	0x6000	2c42611802d585e6eed68595876d1a15	-
.data	4.45574950787	0xe000	0x1958	0x2000	83506e37bd8b50cacabd480f8eb3849b	-
.rsrc	7.9998679751	0x10000	0x349fa0	0x34a000	f99ce7dc94308f0a149a19e022e4c316	-

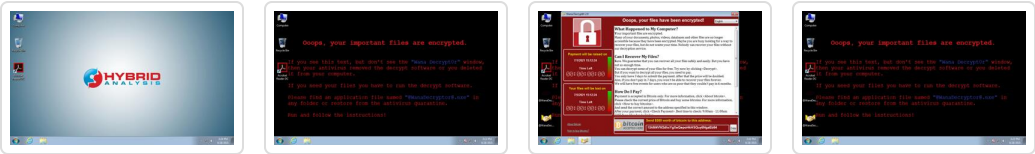
File Resources

Name	RVA	Size	Type	Language
XIA	0x100f0	0x349635	Zip archive data, at least v2.0 to extract	English
RT_VERSION	0x359728	0x388	data	English
RT_MANIFEST	0x359ab0	0x4ef	exported SGML document, ASCII text, with CRLF line terminators	English


File Imports

ADVAPI32.dll	KERNEL32.dll	MSVCRT.dll	USER32.dll
CloseServiceHandle			
CreateServiceA			
CryptReleaseContext			
OpenSCManagerA			
OpenServiceA			
RegCloseKey			

Screenshots




Hybrid Analysis




Tip: Click an analysed process below to view more details.

Analysed 30 processes in total (System Resource Monitor).


- 

Input Sample


(PID: 3828)

64/68
- 

attrib.exe

attrib +h . (PID: 3636)
- 


icaccls.exe

icaccls . /grant Everyone:F /T /C /Q (PID: 2528)
- 

taskdl.exe

(PID: 3960)

61/70


Hash Seen Before
- 

cmd.exe

/c 297471624885764.bat (PID: 1232)


À PROPOS DES COOKIES SUR CE SITE


En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)





HYBRID


ANALYSIS

 ▾


 ▾

 ▾

 ▾


 Request Info


▾





×


▾


 @WanaDecryptor@.exe vs (PID: 3052)


 60/70


 Hash Seen Before


 cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet (PID: 2136)





 vssadmin.exe vssadmin delete shadows /all /quiet (PID: 2688)





 WMIC.exe wmic shadowcopy delete (PID: 3548)





 bcdedit.exe bcdedit /set {default} bootstatuspolicy ignoreallfailures (PID: 3256)





 bcdedit.exe bcdedit /set {default} recoveryenabled no (PID: 3100)





 wbadmin.exe wbadmin delete catalog -quiet (PID: 3640)





 taskse.exe C:\@WanaDecryptor@.exe (PID: 748)


 59/69


 Hash Seen Before


 taskdl.exe (PID: 2144)


 61/70


 @WanaDecryptor@.exe (PID: 1028)


 60/70


 Hash Seen Before


 taskdl.exe (PID: 4060)


 61/70


 cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "cwvrycnpe891" /t REG_SZ /d "\"C:\tasksche.exe\""/f (PID: 1424)





 reg.exe reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "cwvrycnpe891" /t REG_SZ /d "\"C:\tasksche.exe\""/f (PID: 1828)





 taskse.exe C:\@WanaDecryptor@.exe (PID: 1936)


 59/69


 Hash Seen Before


 taskdl.exe (PID: 2476)





 61/70









 @WanaDecryptor@.exe (PID: 3200)

 60/70

 taskse.exe C:\@WanaDecryptor@.exe (PID: 3652)

 59/69

 Hash Seen Before

 Logged Script Calls	 Logged Stdout	 Extracted Streams	 Memory Dumps
 Reduced Monitoring	 Network Activityy	 Network Error	 Multiscan Match













Network Analysis

DNS Requests

No relevant DNS requests were made.

Contacted Hosts

Login to Download Contacted Hosts (CSV)

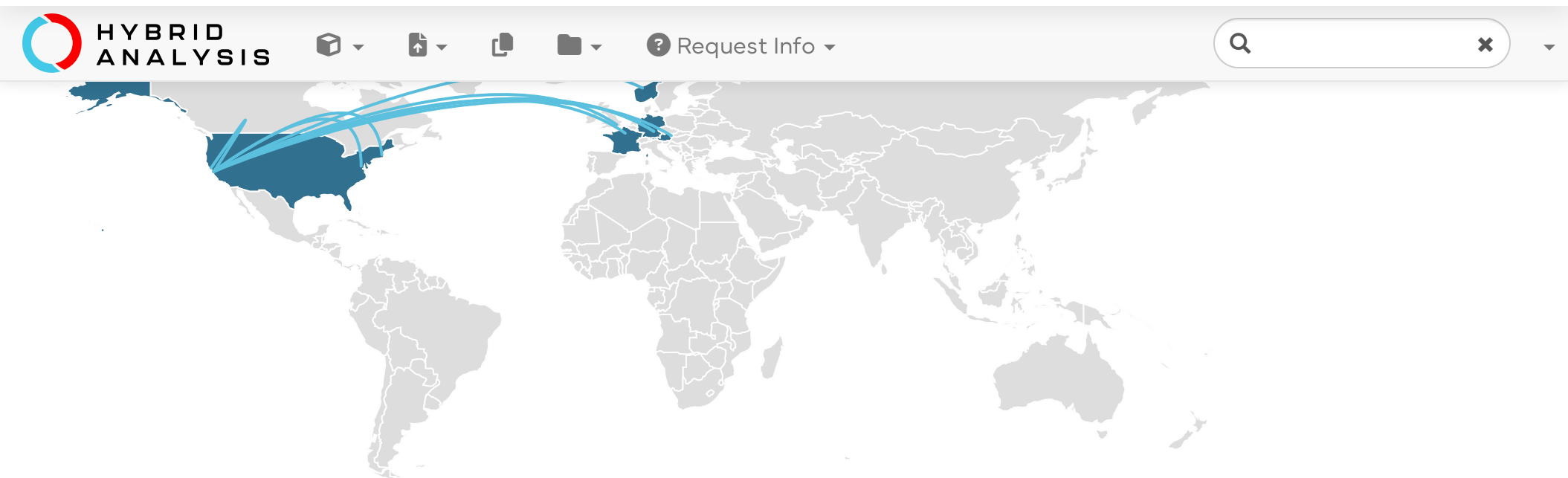
IP Address	Port/Protocol	Associated Process	Details
185.11.180.67 <div> OSINT</div>	9001 TCP	taskhsvc.exe PID: 4084	 Norway
128.31.0.39 <div> OSINT</div>	9101 TCP	taskhsvc.exe PID: 4084	 United States
178.33.183.251 <div> OSINT</div>	443 TCP	taskhsvc.exe PID: 4084	 France
108.197.232.51 <div> OSINT</div>	9001 TCP	taskhsvc.exe PID: 4084	 United States
86.59.21.38 <div> OSINT</div>	443 TCP	taskhsvc.exe PID: 4084	 Austria
172.107.96.70 <div> OSINT</div>	443 TCP	taskhsvc.exe PID: 4084	 United States
...

Contacted Countries

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Page 7 of 14



HTTP Traffic

No relevant HTTP requests were made.

Suricata Alerts

Event	Category	Description	SID
local -> 128.31.0.39:9101 (TCP)	Unknown Traffic	ET JA3 Hash - Possible Malware - Malspam	2028377
128.31.0.39 -> local:49165 (TCP)	Misc activity	ET POLICY TLS possible TOR SSL traffic	2018789
local -> 178.33.183.251:443 (TCP)	Unknown Traffic	ET JA3 Hash - Possible Malware - Malspam	2028377
local -> 86.59.21.38:443 (TCP)	Unknown Traffic	ET JA3 Hash - Possible Malware - Malspam	2028377
local -> 108.197.232.51:9001 (TCP)	Unknown Traffic	ET JA3 Hash - Possible Malware - Malspam	2028377
108.197.232.51 -> local:49171 (TCP)	Misc activity	ET POLICY TLS possible TOR SSL traffic	2018789
local ->	Unknown Traffic	ET JA3 Hash - Possible Malware - Malspam	2028377

i ET rules applied using Suricata. Find out more about proofpoint ET Intelligence [here](#).

Extracted Strings


Search

All Details:


























Off

Download All Memory Strings (92KiB)

- | | | | | |
|--------------------------|-------------------------|--------------------------|--------------------------|----------------------|
| All Strings (2049) | Interesting (1033) | ed01ebfbc9eb5bbea545a... | 00000000.pky (6) | reg.exe:1828 (3) |
| taskhsvc.exe:4084 (1053) | screen_2.png (48) | @WanaDecryptor@.exe:... | cscript.exe (1) | cmd.exe (4) |
| ed01ebfbc9eb5bbea545a... | screen_0.png (4) | vssadmin.exe:2688 (6) | taskdl.exe:3960 (1) | |
| WMIC.exe:3548 (24) | 297471624885764.bat (9) | screen_3.png (13) | icacds.exe:2528 (2) | |
| attrib.exe:3636 (1) | attrib.exe:2952 (1) | cscript.exe:2704 (3) | @WanaDecryptor@.exe:1... | attrib.exe (1) |
| bcdedit.exe (2) | taskse.exe (1) | m.vbs (4) | reg.exe (1) | bcdedit.exe:3256 (2) |
| | | | | taskhsvc.exe (1) |

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

<div><div>HYBRID ANALYSIS</div><div><div>▼</div><div>▼</div><div></div><div>▼</div><div> Request Info ▼</div></div></div> <div><div></div><div></div><div>▼</div></div>	
<div><div>taskse.exe</div><div><div><div>Overview</div><div>Download Disabled</div><div>Extended File Details</div><div>VirusTotal Report</div><div>Hash Seen Before</div></div></div></div> <div><div><div>Size</div><div>20KiB (20480 bytes)</div></div><div><div>Type</div><div>peexeexecutable</div></div><div><div>Description</div><div>PE32 executable (GUI) Intel 80386, for MS Windows</div></div><div><div>AV Scan Result</div><div>Labeled as "Trojan.Ransom.WannaCryptor" (61/70)</div></div><div><div>Runtime Process</div><div>icaccls.exe (PID: 2528)</div></div><div><div>MD5</div><div>4fef5e34143e646dbf9907c4374276f5</div><div></div></div><div><div>SHA1</div><div>47a9ad4125b6bd7c55e4e7da251e23f089407b8f</div><div></div></div><div><div>SHA256</div><div>4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79</div><div></div></div></div>	
<div><div>taskse.exe</div><div><div><div>Overview</div><div>Download Disabled</div><div>Extended File Details</div><div>VirusTotal Report</div><div>Hash Seen Before</div></div></div></div> <div><div><div>Size</div><div>20KiB (20480 bytes)</div></div><div><div>Type</div><div>peexeexecutable</div></div><div><div>Description</div><div>PE32 executable (GUI) Intel 80386, for MS Windows</div></div><div><div>AV Scan Result</div><div>Labeled as "Trojan.Ransom.WannaCryptor" (59/69)</div></div><div><div>Runtime Process</div><div>icaccls.exe (PID: 2528)</div></div><div><div>MD5</div><div>8495400f199ac77853c53b5a3f278f3e</div><div></div></div><div><div>SHA1</div><div>be5d6279874da315e3080b06083757aad9b32c23</div><div></div></div><div><div>SHA256</div><div>2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d</div><div></div></div></div>	
<div><div>u.wnry</div><div><div><div>Overview</div><div>Download Disabled</div><div>VirusTotal Report</div><div>Hash Seen Before</div></div></div></div> <div><div><div>Size</div><div>240KiB (245760 bytes)</div></div><div><div>Type</div><div>peexeexecutable</div></div><div><div>Description</div><div>PE32 executable (GUI) Intel 80386, for MS Windows</div></div><div><div>AV Scan Result</div><div>Labeled as "Trojan.Ransom.WannaCryptor" (60/70)</div></div><div><div>Runtime Process</div><div>icaccls.exe (PID: 2528)</div></div><div><div>MD5</div><div>7bf2b57f2a205768755c07f238fb32cc</div><div></div></div><div><div>SHA1</div><div>45356a9dd616ed7161a3b9192e2f318d0ab5ad10</div><div></div></div><div><div>SHA256</div><div>b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25</div><div></div></div></div>	
<div>Clean<div>10</div></div>	
<div><div>libeay32.dll</div><div><div><div>Overview</div><div>Download Disabled</div><div>Extended File Details</div><div>VirusTotal Report</div><div>Hash Seen Before</div></div></div></div> <div><div><div>Size</div><div>3MiB (3197106 bytes)</div></div><div><div>Type</div><div>pedllexecutable</div></div><div><div>Description</div><div>PE32 executable (DLL) (console) Intel 80386, for MS Windows</div></div><div><div>AV Scan Result</div><div>0/67</div></div><div><div>Runtime Process</div><div>@WanaDecryptor@.exe (PID: 3220)</div></div><div><div>MD5</div><div>6ed47014c3bb259874d673fb3eaedc85</div><div></div></div><div><div>SHA1</div><div>c9b29ba7e8a97729c46143cc59332d7a7e9clad8</div><div></div></div><div><div>SHA256</div><div>58be53d5012b3f45c1ca6f4897bece4773efbe1ccbf0be460061c183ee14ca19</div><div></div></div></div>	
<div><div>libevent-2-0-5.dll</div><div><div><div>Overview</div><div>Download Disabled</div><div>Extended File Details</div><div>VirusTotal Report</div><div>Hash Seen Before</div></div></div></div> <div><div><div>Size</div><div>702KiB (719217 bytes)</div></div><div><div>Type</div><div>pedllexecutable</div></div><div><div>Description</div><div>PE32 executable (DLL) (GUI) Intel 80386, for MS Windows</div></div><div><div>AV Scan Result</div><div>0/60</div></div></div>	

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

HYBRID ANALYSIS

Request Info

Q

×

Overview

Download Disabled

Extended File Details

VirusTotal Report

Hash Seen Before

Size

408KiB (417759 bytes)

Type

pedll

executable

Description

PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

AV Scan Result

0/67

Runtime Process

@WanaDecryptor@.exe (PID: 3220)

MD5

e5df3824f2fcad0c75fd601fcf37ee70

SHA1

902418a4c5f3684dba5e3246de8c4e21c92d674e

SHA256

5cd126b4f8c77bdf0c5c980761a9c84411586951122131f13b0640db83f792d8

libevent_extra-2-0-5.dll

Overview

Download Disabled

Extended File Details

VirusTotal Report

Hash Seen Before

Size

402KiB (411369 bytes)

Type

pedll

executable

Description

PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

AV Scan Result

0/68

Runtime Process

@WanaDecryptor@.exe (PID: 3220)

MD5

6d6602388ab232ca9e8633462e683739

SHA1

41072cc983568d8feeb3e18c4b74440e9d44019a

SHA256

957d58061a42ca343064ec5fb0397950f52aedef0594a18867d1339d5fbb12e7e

libgcc_s_sjlj-1.dll

Overview

Download Disabled

Extended File Details

VirusTotal Report

Hash Seen Before

Size

511KiB (523262 bytes)

Type

pedll

executable

Description

PE32 executable (DLL) (console) Intel 80386, for MS Windows

AV Scan Result

0/68

Runtime Process

taskhsvc.exe (PID: 4084)

MD5

73d4823075762ee2837950726baa2af9

SHA1

ebce3532ed94ad1df43696632ab8cf8da8b9e221

SHA256

9aeccf88253d4557a90793e22414868053caaab325842c0d7acb0365e88cd53b

libssp-0.dll

Overview

Download Disabled

Extended File Details

VirusTotal Report

Hash Seen Before

Size

90KiB (92599 bytes)

Type

pedll

executable

Description

PE32 executable (DLL) (console) Intel 80386, for MS Windows

AV Scan Result

0/67

Runtime Process

taskhsvc.exe (PID: 4084)

MD5

78581e243e2b41b17452da8d0b5b2a48

SHA1

eaefb59c31cf07e60a98af48c5348759586a61bb

SHA256

f28caebe9bc6aa5a72635acb4f0e24500494e306d8e8b2279e7930981281683f

ssleay32.dll

Overview

Download Disabled

Extended File Details

VirusTotal Report

Hash Seen Before

Size

695KiB (711459 bytes)

Type

pedll

executable

Description

PE32 executable (DLL) (console) Intel 80386, for MS Windows

AV Scan Result

0/68

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

HYBRID ANALYSIS

📦

📄

📄

📁

🔍 Request Info

🔍

✕

▼

👤 Overview

⬇️ Download Disabled

👁 Extended File Details

📄 VirusTotal Report

📋 Hash Seen Before

📄 tor.exe

👤 Overview

⬇️ Download Disabled

📄 VirusTotal Report

📋 Hash Seen Before

Size

3MiB (3098624 bytes)

Type

peexe

executable

Description

PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows

AV Scan Result

0/69

Runtime Process

@WanaDecryptor@.exe (PID: 3220)

MD5

fe7eb54691ad6e6af77f8a9a0b6de26d

SHA1

53912d33bec3375153b7e4e68b78d66dab62671a

SHA256

e48673680746fbe027e8982f62a83c298d6fb46ad9243de8e79b7e5a24dcd4eb

📄 zlib1.dll

👤 Overview

⬇️ Download Disabled

👁 Extended File Details

📄 VirusTotal Report

📋 Hash Seen Before

Size

105KiB (107520 bytes)

Type

pedll

executable

Description

PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows

AV Scan Result

0/58

Runtime Process

taskhsvc.exe (PID: 4084)

MD5

fb072e9f69afdb57179f59b512f828a4

SHA1

fe71b70173e46ee4e3796db9139f77dc32d2f846

SHA256

66d653397cbb2dbb397eb8421218e2c126b359a3b0decc0f31e297df099e1383

Informative Selection

6

📄 @WanaDecryptor@.bmp

👤 Overview

⬇️ Download Disabled

📋 Hash Seen Before

Size

1.4MiB (1440054 bytes)

Type

unknown

Description

PC bitmap, Windows 3.x format, 800 x 600 x 24

Runtime Process

@WanaDecryptor@.exe (PID: 1028)

MD5

c17170262312f3be7027bc2ca825bf0c

SHA1

f19eceda82973239a1fdc5826bce7691e5dcb4fb

SHA256

d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa

📄 desktop.ini

▼

📄 ~SD7229.tmp

▼


📄 ~SD7229.tmp

▼

À PROPOS DES COOKIES SUR CE SITE


En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Page 12 of 14



HYBRID

ANALYSIS



Request Info

Q

×

▼

Informative15

 @Please_Read_Me@.txt

Overview

Download Disabled

Hash Seen Before

Size

933B (933 bytes)

Runtime Process

icaccls.exe (PID: 2528)

MD5

7e6b6da7c61fcb66f3f30166871def5b

📋

SHA1

00f699cf9bbc0308f6e101283eca15a7c566d4f9

📋

SHA256

4a25d98c121bb3bd5b54e0b6a5348f7b09966bffeec30776e5a731813f05d49e

📋

 cached-certs.tmp

Download Disabled

Hash Seen Before

Size

18KiB (18605 bytes)

Runtime Process

taskhsvc.exe (PID: 4084)

MD5

130f890c0f858bc031046eeda3cbd626

📋

SHA1

f787ea85dcfca43af9964c644c7c6dc6da6a3efa

📋

SHA256

74227d2600f58ba5d3542d4a344727c0e85536c3a00cfe3eeb8a08d1af0305bc

📋

 cached-microdesc-consensus.tmp

▼

 state.tmp

▼

 unverified-microdesc-consensus.tmp

▼

 Amazon_Downloader_Log_20171206-225712_1810e9e0-1a8d-457c-be3a-737de50dc6bb.txt

▼

 Amazon_Downloader_Log_20171206-225712_1810e9e0-1a8d-457c-be3a-737de50dc6bb.txt.WNCRYT

▼

 Database1.accdb

▼

 Database1.accdb.WNCRYT

▼

 Outlook.pst

▼

 Outlook.pst.WNCRYT

▼

 00000000.eky

▼

 00000000.pky

▼

 00000000.res

▼

 @WanaDecryptor@.exe.lnk

▼

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Community

Anonymous commented 6 years ago

WannaCry

Anonymous commented 6 years ago

AgentTesla@arkangel.live

78 comments are hidden. [Please click this link to display all.](#)

 You must be logged in to submit a comment.

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)