

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c...

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

Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1

AV Detection: 98%

Report generated by Falcon Sandbox © Hybrid Analysis

Labeled as: Trojan.Ransom.WannaCryptor

 Overview  Sample unavailable  Downloads ▼

 External Reports ▼  Re-analyze

 Looking for file context ...  Show Similar Samples  Report False-Positive

 Request Report Deletion

#tag #wannacry #Worm #ransomware #gozi
#isfb #papas #ursnif #wanacrypt0r #wcry

 Post  Link  E-Mail

Incident Response

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 Com

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



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-l/989428fa5504f378b993ee6efbc0b168
	https://www.bleepingcomputer.com/news/security/telefonica-tells-employee-s-to-shut-down-computers-amid-massive-ransomware-outbreak/
	https://misp.local/events/453.json
	https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa?environmentId=100
External User Tags	#adfind #cobaltstrike #dominionvotingmachines.com #egregor #malware #maze #qbot #sekhmet #sha256 #sharphound #trafficmanager.net #ursnif #wannacry

Related Sandbox Artifacts

Associated SHA25...	c99c0d11167064f60f231993b753d4966ac1f3a3d70c3dd73a5e9f3300382e33
Associated URLs	https://github.com/ytisf/theZoo/raw/master/malware/Binaries/Ransomware.WannaCry/Ransomware.WannaCry.zip
	https://raw.githubusercontent.com/Explodingstuff/WannaCry/master/WannaCry.EXE

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](#)

 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



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](#)



Deletes backup catalog	▼
Deletes volume snapshots (often used by ransomware)	▼
System Destruction	
Deletes backup catalog	▼
Deletes volume snapshots (often used by ransomware)	▼
System Security	
Modifies the access control lists of files	▼
Unusual Characteristics	
Spawns a lot of processes	▼
Hiding 2 Malicious Indicators	
All indicators are available only in the private web-service or standalone version	
Suspicious Indicators	36
Anti-Reverse Engineering	
PE file has unusual entropy sections	▼
Environment Awareness	

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](#)



Drops executable files	▼
Network Related	
Found potential IP address in binary/memory	▼
Sends traffic on typical HTTP outbound port, but without HTTP header	▼
Ransomware/Banking	
Detected indicator that file is ransomware	▼
Detected text artifact in screenshot that indicate file could be ransomware	▼
The input sample dropped very many files	▼
Remote Access Related	
Reads terminal service related keys (often RDP related)	▼
Spyware/Information Retrieval	
Reads system information using Windows Management Instrumentation Commandline (WMIC)	▼
System Destruction	
Marks file for deletion	▼
Opens file with deletion access rights	▼
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](#)



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 webinterface or standalone version	

Informative	25
Anti-Reverse Engineering	
PE file contains zero-size sections	▼
Environment Awareness	
Executes WMI queries	▼
External Systems	
Detected Suricata Alert	▼
General	
Contacts server	▼

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](#)



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 LPC ports	▼
Dropped files	▼
Modifies auto-execute functionality by setting/creating a value in the registry	▼
Opens the MountPointManager (often used to detect additional infection locations)	▼
Touches files in the Windows directory	▼
Network Related	
Found potential URL in binary/memory	▼
Remote Access Related	

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 Details

All Details: ☐ Off

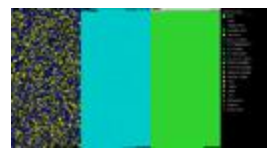
 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

Filename	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Size	3.4MiB (3514368 bytes)
Type	peexe executable
Description	PE32 executable (GUI) Intel 80386, for MS Windows
Architecture	WINDOWS
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa 
Compiler/Packer	Microsoft visual C++ 5.0

Resources

Language	ENGLISH
Icon	

Visualization

Input File (PortEx) 

Version Info

LegalCopyright	Microsoft Corporation. All rights reserved.
InternalName	diskpart.exe
FileVersion	6.1.7601.17514 (win7sp1_rtm.

Classification (TrID)

- 41.0% (.EXE) Win32 Executable MS Visual C++ (generic)
- 36.3% (.EXE) Win64 Executable (generic)
- 8.6% (.DLL) Win32 Dynamic Link Library

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 Metadata

File Compositions

Imported Objects

File Analysis

- 1 .RES Files linked with CVTRES.EXE 5.00 (Visual Studio 5) (build: 1735)
- 7 .CPP Files compiled with CL.EXE 12.00 (Visual Studio 6) (build: 9782)

File Sections

Details

Name	.text
Entropy	6.4042351061
Virtual Address	0x1000
Virtual Size	0x69b0
Raw Size	0x7000
MD5	920e964050a1a5dd60dd00083fd541a2

Name	.rdata
Entropy	6.66357096841
Virtual Address	0x8000
Virtual Size	0x5f70
Raw Size	0x6000
MD5	2c42611802d585e6eed68595876d1a15

Name	.data
Entropy	4.45574950787
Virtual Address	0xe000
Virtual Size	0x1958
Raw Size	0x2000

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](#)



Virtual Address	0x10000
Virtual Size	0x349fa0
Raw Size	0x34a000
MD5	f99ce7dc94308f0a149a19e022e4c316

File Resources

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

File Imports

ADVAPI32.dll	KERNEL32.dll	MSVCRT.dll	USER32.dll
CloseServiceHandle			

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](#)



Screenshots

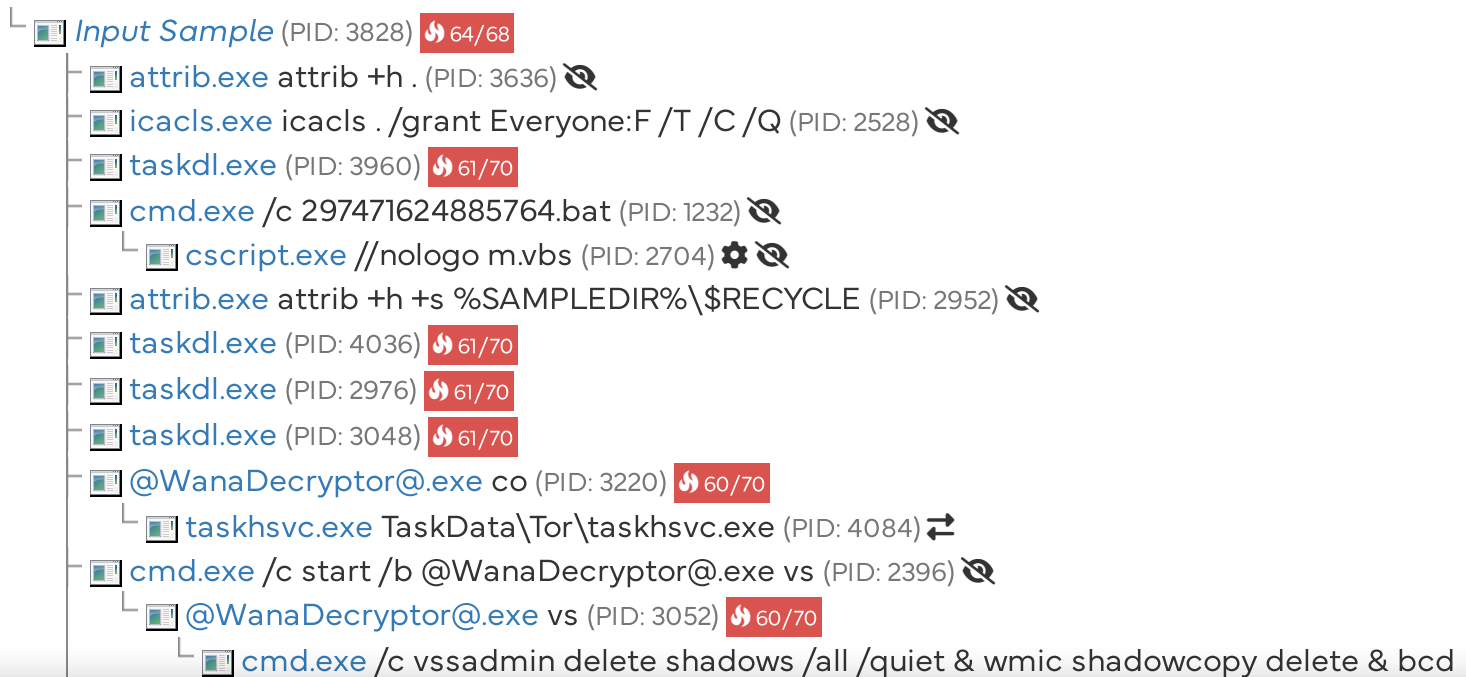
Loading content, please wait...

Hybrid Analysis



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

Analysed 30 processes in total ([System Resource Monitor](#)).



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](#)



- @WanaDecryptor@.exe (PID: 1028) 60/70
- taskdl.exe (PID: 4060) 61/70
- cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "cwvrycnp e891" /t REG_SZ /d "\"C:\tasksche.exe\""/f (PID: 1424)
- └─ reg.exe reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "cwvrycnp e891" /t REG_SZ /d "\"C:\tasksche.exe\""/f (PID: 1828)
- taskse.exe C:\@WanaDecryptor@.exe (PID: 1936) 59/69
- taskdl.exe (PID: 2476) 61/70
- @WanaDecryptor@.exe (PID: 3200) 60/70
- taskse.exe C:\@WanaDecryptor@.exe (PID: 3652) 59/69

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

Network Analysis

DNS Requests

No relevant DNS requests were made.

Contacted Hosts

Login to Download Contacted Hosts (CSV)

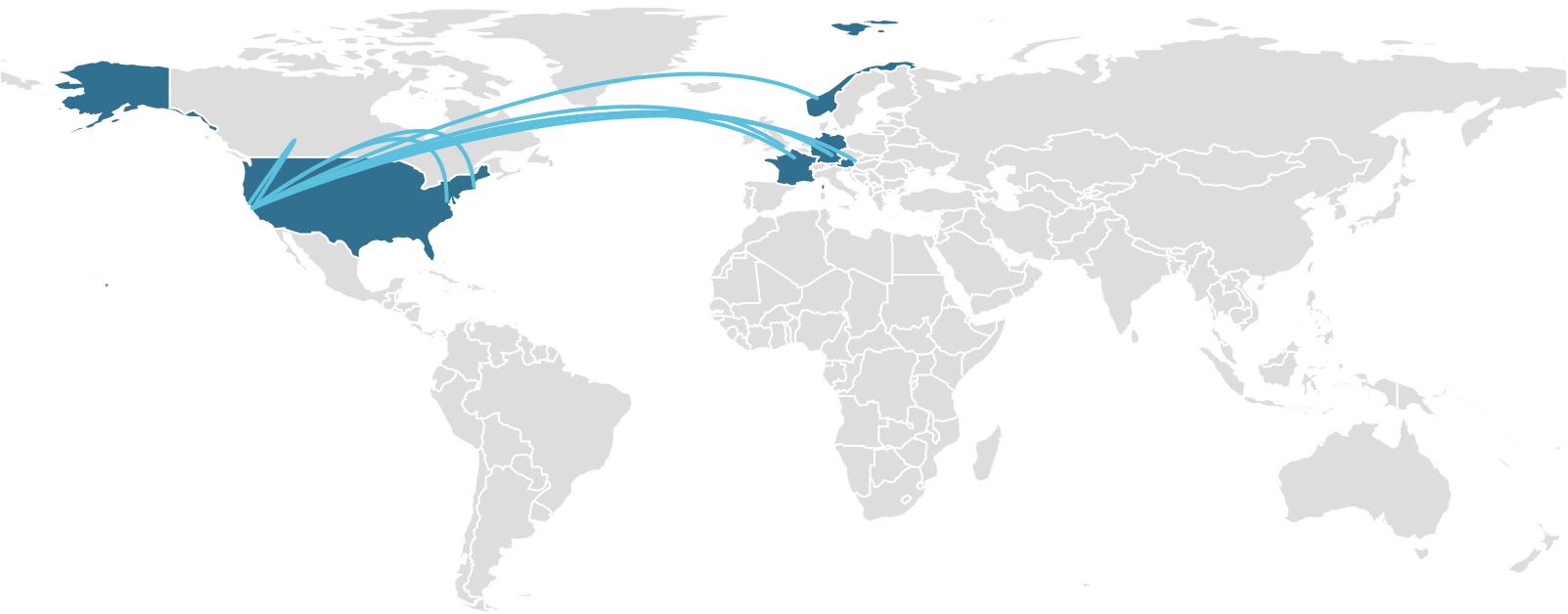
IP Address	Port/Protocol	Associated Process	Details
185.11.180.67 OSINT	9001 TCP	taskhsvc.exe PID: 4084	Norway
128.31.0.39 OSINT	9101 TCP	taskhsvc.exe PID: 4084	United States

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](#)



Contacted Countries



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

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](#)



local -> 78.46.217.214:443 (TCP)	UNKNOWN traffic	ET BAS Hash - Possible malware - malspam	2020377
local -> 20.54.64.202:80 (TCP)	Misc activity	ET INFO Windows OS Submitting USB Metadata to Microsoft	2025275

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

Extracted Strings

All Details:

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) | icacls.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) | vssadmin.exe (1)
- wbadmin.exe (1) | WMIC.exe (1)

```
!Zo)XWxH)'U5Gb(oM1XA"%  
  
"C:\tasksche.exe"  
  
# Tor state file last generated on 2021-06-28 15:16:02 local time# Other times below are in UTC# You *do not* need to edi  
t this file.TorVersion Tor 0.2.9.10 (git-1f6c8eda0073f464)LastWritten 2021-06-28 13:16:02  
  
%GUID:"Computer"%
```



Extracted Files

i Displaying 37 extracted file(s). The remaining **1868** file(s) are available in the full version and XML/JSON reports.

Malicious

6

297471624885764.bat

Overview

Download Disabled

VirusTotal Report

Looking for file context ...

Size

278B (278 bytes)

Type

script

javascript

Description

DOS batch file, ASCII text, with CRLF, CR line terminators

AV Scan Result

Labeled as "BAT_WCRY.BA" (24/60)

Runtime Process

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe (PID: 3828)

MD5

fefe6b30d0819f1a1775e14730a10e0e

SHA1

6d461ff1eddb21957383f8840e55c9674b81efc2

SHA256

f01b7f52e3cb64f01ddc248eb6ae871775ef7cb4297eba5d230d0345af9a5077

@WanaDecryptor@.exe

Overview

Download Disabled

VirusTotal Report

Looking for file context ...

Size

240KiB (245760 bytes)

Type

peexe

executable

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](#)



[Overview](#) [Download Disabled](#) [VirusTotal Report](#) [Looking for file context ...](#)

Size 157B (157 bytes)

Type [script](#) [javascript](#)

Description ASCII text, with CRLF line terminators

AV Scan Result Labeled as "Trojan.Generic" (22/56)

Runtime Process cscript.exe (PID: 2704)

MD5 800446ec5d8b6041f6b08693d8aa1d53 [📋](#)

SHA1 39b9e242af021ee4daa31956f5e786f5d8f9d62c [📋](#)

SHA256 51432d3196d9b78bdc9867a77d601caffd4adaa66dcac944a5ba0b3112bbea3b [📋](#)

taskdl.exe

[Overview](#) [Download Disabled](#) [Extended File Details](#) [VirusTotal Report](#) [Looking for file context ...](#)

Size 20KiB (20480 bytes)

Type [peexe](#) [executable](#)

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

AV Scan Result Labeled as "Trojan.Ransom.WannaCryptor" (61/70)

Runtime Process icacds.exe (PID: 2528)

MD5 4fef5e34143e646dbf9907c4374276f5 [📋](#)

SHA1 47a9ad4125b6bd7c55e4e7da251e23f089407b8f [📋](#)

SHA256 4a468603fdbcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79 [📋](#)

taskse.exe

[Overview](#) [Download Disabled](#) [Extended File Details](#) [VirusTotal Report](#) [Looking for file context ...](#)

Size 20KiB (20480 bytes)

Type [peexe](#) [executable](#)

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](#)



[Overview](#) [Download Disabled](#) [VirusTotal Report](#) [Looking for file context ...](#)

Size 240KiB (245760 bytes)
Type [peexe](#) [executable](#)
Description PE32 executable (GUI) Intel 80386, for MS Windows
AV Scan Result Labeled as "Trojan.Ransom.WannaCryptor" (60/70)
Runtime Process icaccls.exe (PID: 2528)
MD5 7bf2b57f2a205768755c07f238fb32cc [📋](#)
SHA1 45356a9dd616ed7161a3b9192e2f318d0ab5ad10 [📋](#)
SHA256 b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25 [📋](#)

Clean

10

libeay32.dll

[Overview](#) [Download Disabled](#) [Extended File Details](#) [VirusTotal Report](#) [Looking for file context ...](#)

Size 3MiB (3197106 bytes)
Type [pedll](#) [executable](#)
Description PE32 executable (DLL) (console) Intel 80386, for MS Windows
AV Scan Result 0/67
Runtime Process @WanaDecryptor@.exe (PID: 3220)
MD5 6ed47014c3bb259874d673fb3eaedc85 [📋](#)
SHA1 c9b29ba7e8a97729c46143cc59332d7a7e9c1ad8 [📋](#)
SHA256 58be53d5012b3f45c1ca6f4897bece4773efbe1ccbf0be460061c183ee14ca19 [📋](#)

libevent-2-0-5.dll

[Overview](#) [Download Disabled](#) [Extended File Details](#) [VirusTotal Report](#) [Looking for file context ...](#)

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](#)



libevent_core-2-0-5.dll

[Overview](#) [Download Disabled](#) [Extended File Details](#) [VirusTotal Report](#) [Looking for file context ...](#)

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](#) [Looking for file context ...](#)

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](#) [Looking for file context ...](#)

Size 511KiB (523262 bytes)

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](#)



[Overview](#) [Download Disabled](#) [Extended File Details](#) [VirusTotal Report](#) [Looking for file context ...](#)

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](#) [Looking for file context ...](#)

Size 695KiB (711459 bytes)

Type [peDll](#) [executable](#)

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

AV Scan Result 0/68

Runtime Process @WanaDecryptor@.exe (PID: 3220)

MD5 a12c2040f6fddd34e7acb42f18dd6bdc [📋](#)

SHA1 d7db49f1a9870a4f52e1f31812938fdea89e9444 [📋](#)

SHA256 bd70ba598316980833f78b05f7eeaef3e0f811a7c64196bf80901d155cb647c1 [📋](#)

taskhsvc.exe

[Overview](#) [Download Disabled](#) [Extended File Details](#) [VirusTotal Report](#) [Looking for file context ...](#)

Size 3MiB (3098624 bytes)

Type [peexe](#) [executable](#)

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](#)



[Overview](#) [Download Disabled](#) [VirusTotal Report](#) [Looking for file context ...](#)

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](#) [Looking for file context ...](#)

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



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](#)

~SD7D1D.tmp



Informative

15

@Please_Read_Me@.txt



cached-certs.tmp



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



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](#)



00000000.res



@WanaDecryptor@.exe.lnk



Notifications

Runtime



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.](#)

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](#)



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](#)