ID: 694554
Sample Name:
THN6clTA6P.exe
Cookbook: default.jbs
Time: 23:45:45
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

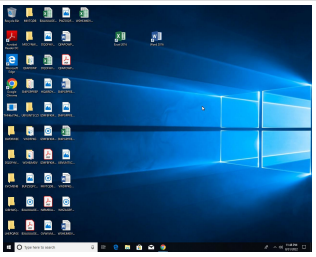
Windows Analysis Report

THN6clTA6P.exe

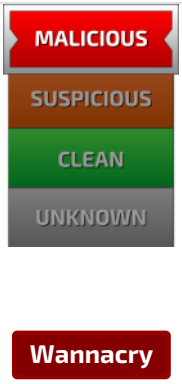
Overview

General Information

Sample Name:	THN6clTA6P.exe
Analysis ID:	694554
MD5:	3983f0ebeec88b..
SHA1:	9f34d48eae30b6..
SHA256:	ed492db95034ca..
Infos:	



Detection



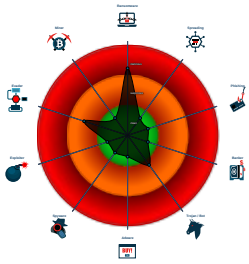
Wannacry

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Tries to download HTTP data from a…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Yara detected Wannacry ransomware
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Machine Learning detection for sam…
- Uses 32bit PE files
- Found decision node followed by no…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- THN6clTA6P.exe (PID: 2996 cmdline: "C:\Users\user\Desktop\THN6clTA6P.exe" MD5: 3983F0EBEEC88B8005724A203AE27180)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
THN6clTA6P.exe	WannaCry_Ransomware	Detects WannaCry Ransomware	Florian Roth (with the help of binar.ly)	0x415a0:$x1: icacls . /grant Everyone:F /T /C /Q 0x374de5:$x2: taskdl.exe 0x38b6d1:$x2: taskdl.exe 0x3136c:$x3: tasksche.exe 0x4157c:$x3: tasksche.exe 0x41558:$x4: Global\MsWinZonesCacheCounterMutexA 0x415d0:$x5: WNcry@2ol7 0xe048:$x7: mssecsvc.exe 0x17350:$x7: mssecsvc.exe 0x31344:$x8: C:\%s\qeriuwjhrf 0x415a0:$x9: icacls . /grant Everyone:F /T /C /Q 0xe034:$s1: C:\%s\%s 0x17338:$s1: C:\%s\%s 0x31358:$s1: C:\%s\%s 0x38be35:$s2: Windows 10 --> 0x414d0:$s3: cmd.exe /c "%s" 0x73a24:$s4: msg/m_portuguese.wnry 0x38b2a3:$s4: msg/m_portuguese.wnry 0x2e68c:$s5: \\192.168.56.20\IPC$ 0x1ba81:$s6: \\172.16.99.5\IPC$ 0x9131:$op1: 10 AC 72 0D 3D FF FF 1F AC 77 06 B8 01 00 00 00
THN6clTA6P.exe	WannaCry_Ransomware_Gen	Detects WannaCry Ransomware	Florian Roth (based on rule by US CERT)	0x1bacc:$s1: __TREEID__PLACEHOLDER__ 0x1bb68:$s1: __TREEID__PLACEHOLDER__ 0x1c3d4:$s1: __TREEID__PLACEHOLDER__ 0x1d439:$s1: __TREEID__PLACEHOLDER__ 0x1e4a0:$s1: __TREEID__PLACEHOLDER__ 0x1f508:$s1: __TREEID__PLACEHOLDER__ 0x20570:$s1: __TREEID__PLACEHOLDER__ 0x215d8:$s1: __TREEID__PLACEHOLDER__ 0x22640:$s1: __TREEID__PLACEHOLDER__ 0x236a8:$s1: __TREEID__PLACEHOLDER__ 0x24710:$s1: __TREEID__PLACEHOLDER__ 0x25778:$s1: __TREEID__PLACEHOLDER__ 0x267e0:$s1: __TREEID__PLACEHOLDER__ 0x27848:$s1: __TREEID__PLACEHOLDER__ 0x288b0:$s1: __TREEID__PLACEHOLDER__ 0x29918:$s1: __TREEID__PLACEHOLDER__ 0x2a980:$s1: __TREEID__PLACEHOLDER__ 0x2ab94:$s1: __TREEID__PLACEHOLDER__ 0x2abf4:$s1: __TREEID__PLACEHOLDER__ 0x2e2c4:$s1: __TREEID__PLACEHOLDER__ 0x2e340:$s1: __TREEID__PLACEHOLDER__
THN6clTA6P.exe	JoeSecurity_Wannacry	Yara detected Wannacry ransomware	Joe Security	
THN6clTA6P.exe	wanna_cry_ransomware_generic	detects wannacry ransomware on disk and in virtual page	us-cert code analysis team	0x4157c:$s11: 74 61 73 6B 73 63 68 65 2E 65 78 65 00 00 00 00 54 61 73 6B 53 74 61 72 74 00 00 00 74 2E 77 6E 72 79 00 00 69 63 61 63 0x415a4:$s12: 6C 73 20 2E 20 2F 67 72 61 6E 74 20 45 76 65 72 79 6F 6E 65 3A 46 20 2F 54 20 2F 43 20 2F 51 00 61 74 74 72 69 62 20 2B 68
THN6clTA6P.exe	Win32_Ransomware_WannaCry	unknown	ReversingLabs	0x340ba:$main_2: 68 08 02 00 00 33 DB 50 53 FF 15 8C 80 40 00 68 AC F8 40 00 E8 F6 F1 FF FF 59 FF 15 6C 81 40 00 83 38 02 75 53 68 38 F5 40 00 FF 15 68 81 40 00 8B 00 FF 70 04 E8 F0 56 00 00 59 85 C0 59 75 38 ... 0x8140:$main_3: 83 EC 50 56 57 B9 0E 00 00 00 BE D0 13 43 00 8D 7C 24 08 33 C0 F3 A5 A4 89 44 24 41 89 44 24 45 89 44 24 49 89 44 24 4D 89 44 24 51 66 89 44 24 55 50 50 50 6A 01 50 88 44 24 6B FF 15 34 A1 40 ... 0x8090:$start_service_3: 83 EC 10 68 04 01 00 00 68 60 F7 70 00 6A 00 FF 15 6C A0 40 00 FF 15 2C A1 40 00 83 38 02 7D 09 E8 6B FE FF FF 83 C4 10 C3 57 68 3F 00 0F 00 6A 00 6A 00 FF 15 10 A0 40 00 8B F8 85 FF 74 32 53 ... 0x9a16:$entrypoint_all: 55 8B EC 6A FF 68 A0 A1 40 00 68 A2 9B 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68 53 56 57 89 65 E8 33 DB 89 5D FC 6A 02 FF 15 C0 A0 40 00 59 83 0D 94 F8 70 00 FF 83 0D 98 F8 70 ... 0x3985e:$entrypoint_all: 55 8B EC 6A FF 68 88 D4 40 00 68 F4 76 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68 53 56 57 89 65 E8 33 DB 89 5D FC 6A 02 FF 15 C4 81 40 00 59 83 0D 4C F9 40 00 FF 83 0D 50 F9 40 ...

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.265600976.000000000040F000.00000008.00000001.01000000.00000005.sdmp	JoeSecurity_Wannacry	Yara detected Wannacry ransomware	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.262463921.000000000040F000.00000008.00000001.01000000.00000005.sdmp	JoeSecurity_Wannacry	Yara detected Wannacry ransomware	Joe Security	
00000001.00000000.262558061.0000000000710000.00000002.00000001.01000000.00000005.sdmp	wanna_cry_ransomware_generic	detects wannacry ransomware on disk and in virtual page	us-cert code analysis team	• 0xf57c:$s11: 74 61 73 6B 73 63 68 65 2E 65 78 65 00 00 00 00 54 61 73 6B 53 74 61 72 74 00 00 00 74 2E 77 6E 72 79 00 00 69 63 61 63 • 0xf5a4:$s12: 6C 73 20 2E 20 2F 67 72 61 6E 74 20 45 76 65 72 79 6F 6E 65 3A 46 20 2F 54 20 2F 43 20 2F 51 00 61 74 74 72 69 62 20 2B 68
00000001.00000002.265724046.0000000000710000.00000002.00000001.01000000.00000005.sdmp	wanna_cry_ransomware_generic	detects wannacry ransomware on disk and in virtual page	us-cert code analysis team	• 0xf57c:$s11: 74 61 73 6B 73 63 68 65 2E 65 78 65 00 00 00 00 54 61 73 6B 53 74 61 72 74 00 00 00 74 2E 77 6E 72 79 00 00 69 63 61 63 • 0xf5a4:$s12: 6C 73 20 2E 20 2F 67 72 61 6E 74 20 45 76 65 72 79 6F 6E 65 3A 46 20 2F 54 20 2F 43 20 2F 51 00 61 74 74 72 69 62 20 2B 68
Process Memory Space: THN6clTA6P.exe PID: 2996	JoeSecurity_Wannacry	Yara detected Wannacry ransomware	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.THN6clTA6P.exe.7100a4.1.raw.unpack	WannaCry_Ransomware	Detects WannaCry Ransomware	Florian Roth (with the help of binar.ly)	• 0xf4fc:$x1: icacls . /grant Everyone:F /T /C /Q • 0x342d41:$x2: taskdl.exe • 0x35962d:$x2: taskdl.exe • 0xf4d8:$x3: tasksche.exe • 0xf4b4:$x4: Global\MsWinZonesCacheCounterMutexA • 0xf52c:$x5: WNcry@2ol7 • 0xf4fc:$x9: icacls . /grant Everyone:F /T /C /Q • 0x359d91:$s2: Windows 10 --> • 0xf42c:$s3: cmd.exe /c "%s" • 0x41980:$s4: msg/m_portuguese.wnry • 0x3591ff:$s4: msg/m_portuguese.wnry • 0x2a02:$op4: 09 FF 76 30 50 FF 56 2C 59 59 47 3B 7E 0C 7C • 0x26dc:$op5: C1 EA 1D C1 EE 1E 83 E2 01 83 E6 01 8D 14 56 • 0x22c8:$op6: 8D 48 FF F7 D1 8D 44 10 FF 23 F1 23 C1
1.2.THN6clTA6P.exe.7100a4.1.raw.unpack	wanna_cry_ransomware_generic	detects wannacry ransomware on disk and in virtual page	us-cert code analysis team	• 0xf4d8:$s11: 74 61 73 6B 73 63 68 65 2E 65 78 65 00 00 00 00 54 61 73 6B 53 74 61 72 74 00 00 00 74 2E 77 6E 72 79 00 00 69 63 61 63 • 0xf500:$s12: 6C 73 20 2E 20 2F 67 72 61 6E 74 20 45 76 65 72 79 6F 6E 65 3A 46 20 2F 54 20 2F 43 20 2F 51 00 61 74 74 72 69 62 20 2B 68
1.2.THN6clTA6P.exe.7100a4.1.raw.unpack	Win32_Ransomware_WannaCry	unknown	ReversingLabs	• 0x2016:$main_2: 68 08 02 00 00 33 DB 50 53 FF 15 8C 80 40 00 68 AC F8 40 00 E8 F6 F1 FF FF 59 FF 15 6C 81 40 00 83 38 02 75 53 68 38 F5 40 00 FF 15 68 81 40 00 8B 00 FF 70 04 E8 F0 56 00 00 59 85 C0 59 75 38 ... • 0x77ba:$entrypoint_all: 55 8B EC 6A FF 68 88 D4 40 00 68 F4 76 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68 53 56 57 89 65 E8 33 DB 89 5D FC 6A 02 FF 15 C4 81 40 00 59 83 0D 4C F9 40 00 FF 83 0D 50 F9 40 ...
1.0.THN6clTA6P.exe.400000.0.unpack	WannaCry_Ransomware	Detects WannaCry Ransomware	Florian Roth (with the help of binar.ly)	• 0x415a0:$x1: icacls . /grant Everyone:F /T /C /Q • 0x374de5:$x2: taskdl.exe • 0x38b6d1:$x2: taskdl.exe • 0x3136c:$x3: tasksche.exe • 0x4157c:$x3: tasksche.exe • 0x41558:$x4: Global\MsWinZonesCacheCounterMutexA • 0x415d0:$x5: WNcry@2ol7 • 0x17350:$x7: mssecsvc.exe • 0x31344:$x8: C:\%s\qeriuwjhrf • 0x415a0:$x9: icacls . /grant Everyone:F /T /C /Q • 0x17338:$s1: C:\%s\%s • 0x31358:$s1: C:\%s\%s • 0x38be35:$s2: Windows 10 --> • 0x414d0:$s3: cmd.exe /c "%s" • 0x73a24:$s4: msg/m_portuguese.wnry • 0x38b2a3:$s4: msg/m_portuguese.wnry • 0x2e68c:$s5: \\192.168.56.20\IPC$ • 0x1ba81:$s6: \\172.16.99.5\IPC$ • 0x9131:$op1: 10 AC 72 0D 3D FF FF 1F AC 77 06 B8 01 00 00 00 • 0x3876:$op2: 44 24 64 8A C6 44 24 65 0E C6 44 24 66 80 C6 44 • 0x13e5:$op3: 18 DF 6C 24 14 DC 64 24 2C DC 6C 24 5C DC 15 88

Source	Rule	Description	Author	Strings
1.0.THN6clTA6P.exe.400000.0.unpack	WannaCry_Ransomware_Gen	Detects WannaCry Ransomware	Florian Roth (based on rule by US CERT)	• 0x1bacc:$s1: __TREEID__PLACEHOLDER__ • 0x1bb68:$s1: __TREEID__PLACEHOLDER__ • 0x1c3d4:$s1: __TREEID__PLACEHOLDER__ • 0x1d439:$s1: __TREEID__PLACEHOLDER__ • 0x1e4a0:$s1: __TREEID__PLACEHOLDER__ • 0x1f508:$s1: __TREEID__PLACEHOLDER__ • 0x20570:$s1: __TREEID__PLACEHOLDER__ • 0x215d8:$s1: __TREEID__PLACEHOLDER__ • 0x22640:$s1: __TREEID__PLACEHOLDER__ • 0x236a8:$s1: __TREEID__PLACEHOLDER__ • 0x24710:$s1: __TREEID__PLACEHOLDER__ • 0x25778:$s1: __TREEID__PLACEHOLDER__ • 0x267e0:$s1: __TREEID__PLACEHOLDER__ • 0x27848:$s1: __TREEID__PLACEHOLDER__ • 0x288b0:$s1: __TREEID__PLACEHOLDER__ • 0x29918:$s1: __TREEID__PLACEHOLDER__ • 0x2a980:$s1: __TREEID__PLACEHOLDER__ • 0x2ab94:$s1: __TREEID__PLACEHOLDER__ • 0x2abf4:$s1: __TREEID__PLACEHOLDER__ • 0x2e2c4:$s1: __TREEID__PLACEHOLDER__ • 0x2e340:$s1: __TREEID__PLACEHOLDER__
Click to see the 17 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Possible WannaCry DNS Lookup 2 - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.860625532024293 08/31/22-23:46:48.979040
SID:	2024293
Source Port:	60625
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Known Sinkhole Response Header - Source IP: 104.21.68.165 - Destination IP: 192.168.2.3

Timestamp:	104.21.68.165192.168.2.380497462016803 08/31/22-23:46:49.148342
SID:	2016803
Source Port:	80
Destination Port:	49746
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

Tries to download HTTP data from a sinkholed server

Snort IDS alert for network traffic

Spam, unwanted Advertisements and Ransom Demands

Yara detected Wannacry ransomware

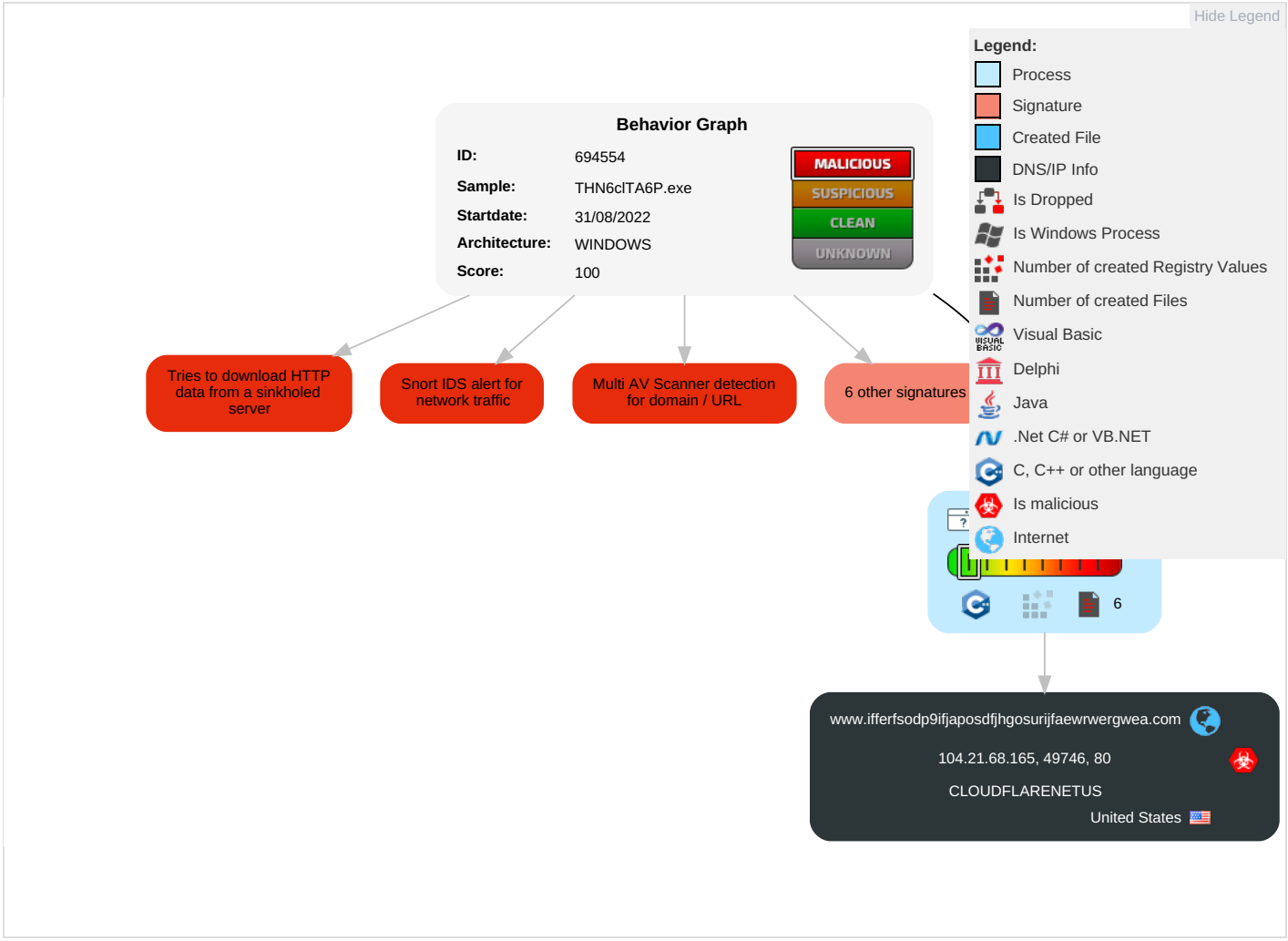
System Summary

Malicious sample detected (through community Yara rule)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Service Execution	4 Windows Service	4 Windows Service	1 Software Packing	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
THN6clTA6P.exe	89%	Virustotal		Browse
THN6clTA6P.exe	89%	Metadefender		Browse
THN6clTA6P.exe	100%	ReversingLabs	Win32.Ransomware.WannaCry	
THN6clTA6P.exe	100%	Avira	TR/Ransom.IZ	
THN6clTA6P.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.THN6clTA6P.exe.7100a4.1.unpack	100%	Avira	TR/Ransom.JB		Download File
1.2.THN6clTA6P.exe.400000.0.unpack	100%	Avira	TR/Ransom.JB		Download File
1.0.THN6clTA6P.exe.7100a4.1.unpack	100%	Avira	TR/Ransom.JB		Download File
1.0.THN6clTA6P.exe.400000.0.unpack	100%	Avira	TR/Ransom.JB		Download File

Domains

Source	Detection	Scanner	Label	Link
www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com/	6%	Virustotal		Browse
http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com/	100%	Avira URL Cloud	malware	
http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com	6%	Virustotal		Browse
http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com	104.21.68.165	true	true	• 6%, Virustotal, Browse	unknown

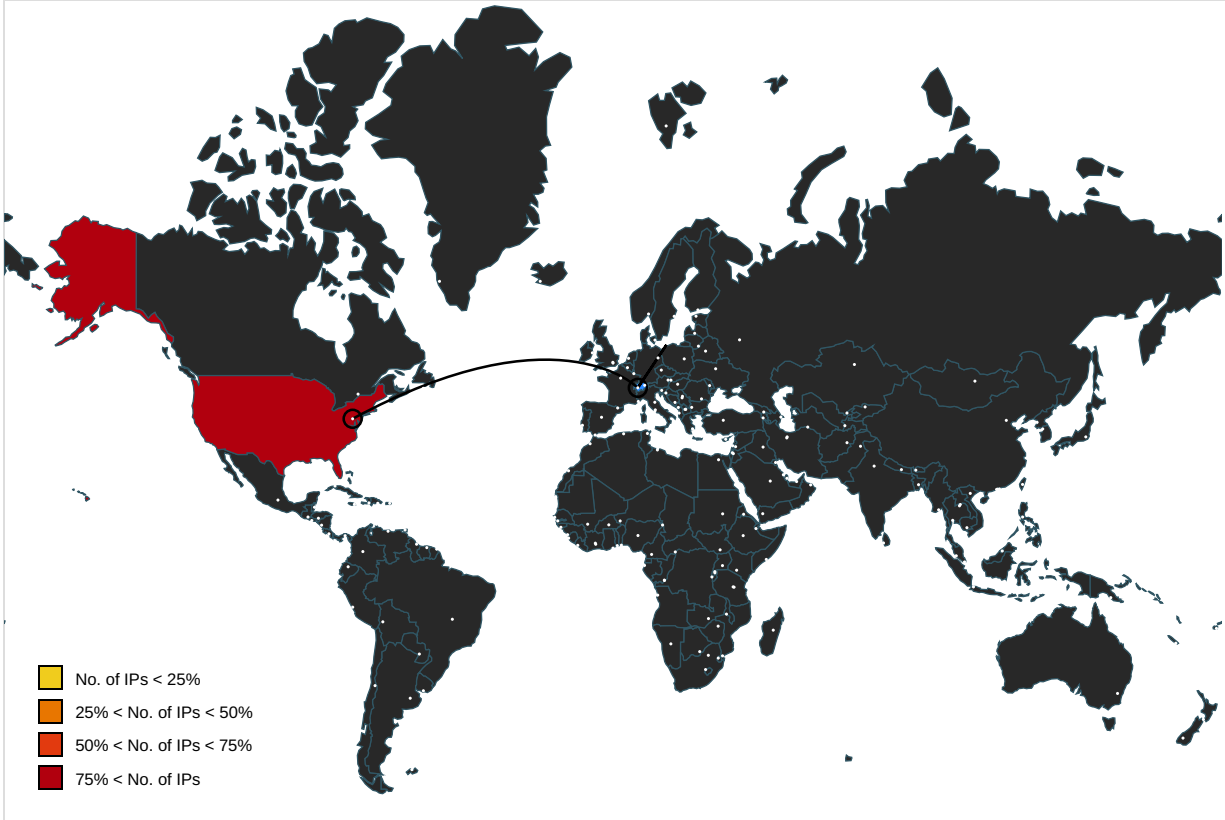
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com/	true	• 6%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com	THN6clTA6P.exe	true	• 6%, Virustotal, Browse • Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.68.165	www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694554
Start date and time:	2022-08-31 23:45:45 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	THN6clTA6P.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.winEXE@1/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 93.3%) • Quality average: 78.1% • Quality standard deviation: 28.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.964259281750754
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	THN6clTA6P.exe
File size:	3723293
MD5:	3983f0ebeec88b8005724a203ae27180
SHA1:	9f34d48eae30b6da0a5c5297a873f989a49e10e8
SHA256:	ed492db95034ca288dd52df88e3ce3ec7b146ffd854a394ac187f0553ef966d9
SHA512:	8e9956ad6ec1ef73a3555eaebc1efd2bf51a1794af2ee06d6fce2aace5e197d949fc27a2c8a89d224655db486f91c494e11235021a5238e81da3495f0b17d320
SSDEEP:	98304:whqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g30:whqPe1Cxcxk3ZAEUadzR8yc4gk
TLSH:	7B0633A8962DA1BCF0050DB044928557EBFB3C57B7BA5A2FCF4045660E43B6F9BC0E61
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U<S..]=..]=..]=.jA1..]=..A3..]=.~B7..]=.~B6..]=.~B9..]=..R`..]=..]<.J]='{6..]=..[;..]=.Rich.]=.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x409a16
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x4CE78ECC [Sat Nov 20 09:03:08 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	9ecee117164e0b870a53dd187cdd7174

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 0040A1A0h
push 00409BA2h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 68h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
xor ebx, ebx
mov dword ptr [ebp-04h], ebx
push 00000002h
call dword ptr [0040A0C0h]
pop ecx
or dword ptr [0070F894h], FFFFFFFFh
or dword ptr [0070F898h], FFFFFFFFh
call dword ptr [0040A0C8h]
mov ecx, dword ptr [0070F88Ch]
mov dword ptr [eax], ecx
call dword ptr [0040A0CCh]
mov ecx, dword ptr [0070F888h]
mov dword ptr [eax], ecx
mov eax, dword ptr [0040A0E4h]
mov eax, dword ptr [eax]
mov dword ptr [0070F890h], eax
call 00007F77E0708F21h
cmp dword ptr [00431410h], ebx
jne 00007F77E0708E0Eh
push 00409B9Eh
call dword ptr [0040A0D4h]
pop ecx
call 00007F77E0708EF3h
push 0040B010h
push 0040B00Ch
call 00007F77E0708EDEh
mov eax, dword ptr [0070F884h]
mov dword ptr [ebp-6Ch], eax
lea eax, dword ptr [ebp-6Ch]
push eax
push dword ptr [0070F880h]
lea eax, dword ptr [ebp-64h]

Instruction
push eax
lea eax, dword ptr [ebp-70h]
push eax
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [0040A0DCh]
push 0040B008h
push 0040B000h
call 00007F77E0708EABh

Rich Headers

Programming Language:	• [C++] VS98 (6.0) SP6 build 8804 • [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa1e0	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x310000	0x35a454	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xa000	0x188	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8bca	0x9000	False	0.5344509548611112	data	6.134590828123831	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xa000	0x998	0x1000	False	0.29345703125	data	3.503615586181224	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xb000	0x30489c	0x27000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x310000	0x35a454	0x35b000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
R	0x3100a4	0x35a000	PE32 executable (GUI) Intel 80386, for MS Windows	English	United States
RT_VERSION	0x66a0a4	0x3b0	data	English	United States

Imports

DLL	Import
KERNEL32.dll	WaitForSingleObject, InterlockedIncrement, GetCurrentThreadId, GetCurrentThread, ReadFile, GetFileSize, CreateFileA, MoveFileExA, SizeofResource, TerminateThread, LoadResource, FindResourceA, GetProcAddress, GetModuleHandleW, ExitProcess, GetModuleFileNameA, LocalFree, LocalAlloc, CloseHandle, InterlockedDecrement, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSection, GlobalAlloc, GlobalFree, QueryPerformanceFrequency, QueryPerformanceCounter, GetTickCount, LockResource, Sleep, GetStartupInfoA, GetModuleHandleA

DLL	Import
ADVAPI32.dll	StartServiceCtrlDispatcherA, RegisterServiceCtrlHandlerA, ChangeServiceConfig2A, SetServiceStatus, OpenSCManagerA, CreateServiceA, CloseServiceHandle, StartServiceA, CryptGenRandom, CryptAcquireContextA, OpenServiceA
WS2_32.dll	closesocket, recv, send, htonl, ntohl, WSAStartup, inet_ntoa, ioctlsocket, select, htons, socket, connect, inet_addr
MSVCP60.dll	??1_Lockit@std@@QAE@XZ, ??0_Lockit@std@@QAE@XZ
iphlpapi.dll	GetAdaptersInfo, GetPerAdapterInfo
WININET.dll	InternetOpenA, InternetOpenUrlA, InternetCloseHandle
MSVCRT.dll	__set_app_type, _stricmp, __p__fmode, __p__commode, _except_handler3, __setusermatherr, _initterm, __getmainargs, _acmdln, _adjust_fdiv, _controlfp, exit, _XcptFilter, _exit, _onexit, __dllonexit, free, ??2@YAPAXI@Z, _ftol, sprintf, _endthreadex, strncpy, rand, _beginthreadex, __CxxFrameHandler, srand, time, __p___argc

Possible Origin

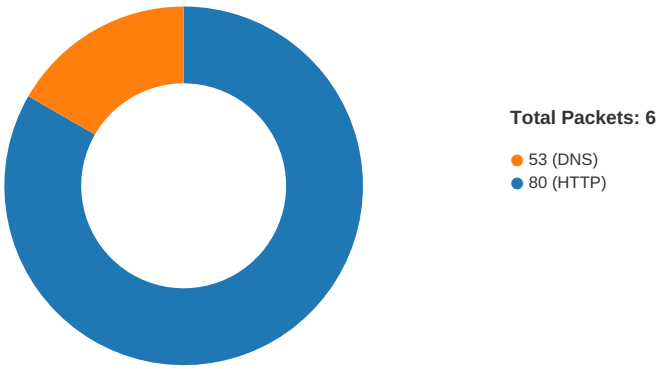
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8606255 32024293 08/31/22-23:46:48.979040	UDP	2024293	ET TROJAN Possible WannaCry DNS Lookup 2	60625	53	192.168.2.3	8.8.8.8
104.21.68.165192.168.2.380497462016803 08/31/22-23:46:49.148342	TCP	2016803	ET TROJAN Known Sinkhole Response Header	80	49746	104.21.68.165	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:46:49.046582937 CEST	49746	80	192.168.2.3	104.21.68.165
Aug 31, 2022 23:46:49.079365015 CEST	80	49746	104.21.68.165	192.168.2.3
Aug 31, 2022 23:46:49.079502106 CEST	49746	80	192.168.2.3	104.21.68.165
Aug 31, 2022 23:46:49.084465981 CEST	49746	80	192.168.2.3	104.21.68.165
Aug 31, 2022 23:46:49.117137909 CEST	80	49746	104.21.68.165	192.168.2.3
Aug 31, 2022 23:46:49.148341894 CEST	80	49746	104.21.68.165	192.168.2.3
Aug 31, 2022 23:46:49.149030924 CEST	49746	80	192.168.2.3	104.21.68.165

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:46:49.856214046 CEST	49746	80	192.168.2.3	104.21.68.165

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:46:48.979039907 CEST	60625	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:46:49.004631042 CEST	53	60625	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:46:48.979039907 CEST	192.168.2.3	8.8.8.8	0xb27c	Standard query (0)	www.ifferf sodp9ifjap osdfjhgosu rijfaewrwe rgwea.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:46:49.004631042 CEST	8.8.8.8	192.168.2.3	0xb27c	No error (0)	www.ifferf sodp9ifjap osdfjhgosu rijfaewrwe rgwea.com		104.21.68.165	A (IP address)	IN (0x0001)
Aug 31, 2022 23:46:49.004631042 CEST	8.8.8.8	192.168.2.3	0xb27c	No error (0)	www.ifferf sodp9ifjap osdfjhgosu rijfaewrwe rgwea.com		172.67.196.228	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49746	104.21.68.165	80	C:\Users\user\Desktop\THN6clTA6P.exe

Timestamp	kBytes transferred	Direction	Data
Aug 31, 2022 23:46:49.084465981 CEST	902	OUT	GET / HTTP/1.1 Host: www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com Cache-Control: no-cache
Aug 31, 2022 23:46:49.148341894 CEST	903	IN	HTTP/1.1 200 OK Date: Wed, 31 Aug 2022 21:46:49 GMT Content-Type: text/html;charset=UTF-8 Content-Length: 113 Connection: keep-alive x-sinkhole: sinkhole@blacklistthisdomain.com Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=BwAJjUBV7QoBfDcQC5xHuwWf6HaSer5urPutgRH%2BIhWdxjAnZxQhv3Lj7wdnu2PPlKacdGr9jV%2FTSwi3vI%2BYOhYgTU0rv1q0jFccnc7tRao14EgvdRHCOJyooOZRF5g5vft43xf7R9Y9%2BZ3RRpCsAmuUjh5Fhtj03GcJjYsFDcilY2Vk"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7438f608df147765-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 62 6f 64 79 3e 0a 20 20 3c 68 31 3e 42 6c 61 63 6b 4c 69 73 74 54 68 69 73 44 6f 6d 61 69 6e 20 2d 20 53 69 6e 6b 68 6f 6c 65 3c 2f 68 31 3e 0a 20 20 3c 70 3e 54 68 69 73 20 64 6f 6d 61 69 6e 20 68 61 73 20 62 65 65 6e 20 73 69 6e 6b 68 6f 6c 65 64 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e Data Ascii: <!DOCTYPE html><body> BlackListThisDomain - Sinkhole This domain has been sinkholed. </body>

Statistics

No statistics

System Behavior

Analysis Process: THN6clTA6P.exe PID: 2996, Parent PID: 5424

General

Target ID:	1
Start time:	23:46:47
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\THN6clTA6P.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\THN6clTA6P.exe"
Imagebase:	0x400000
File size:	3723293 bytes
MD5 hash:	3983F0EBEEC88B8005724A203AE27180
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Wannacry, Description: Yara detected Wannacry ransomware, Source: 00000001.00000002.265600976.000000000040F000.00000008.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Wannacry, Description: Yara detected Wannacry ransomware, Source: 00000001.00000000.262463921.000000000040F000.00000008.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: wanna_cry_ransomware_generic, Description: detects wannacry ransomware on disk and in virtual page, Source: 00000001.00000000.262558061.0000000000710000.00000002.00000001.01000000.00000005.sdmp, Author: us-cert code analysis team • Rule: wanna_cry_ransomware_generic, Description: detects wannacry ransomware on disk and in virtual page, Source: 00000001.00000002.265724046.0000000000710000.00000002.00000001.01000000.00000005.sdmp, Author: us-cert code analysis team
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly