ID: 533988
Sample Name: Everything.exe
Cookbook: default.jbs
Time: 22:10:38
Date: 04/12/2021
Version: 34.0.0 Boulder Opal

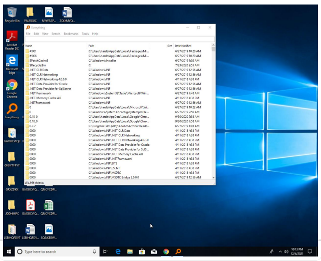
Table of Contents

Windows Analysis Report Everything.exe

Overview

General Information

Sample Name:	Everything.exe
Analysis ID:	533988
MD5:	b2e26b3562562d..
SHA1:	52aacfe08a0d514.
SHA256:	66b9610e94d003..
Infos:	
Most interesting Screenshot:	



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

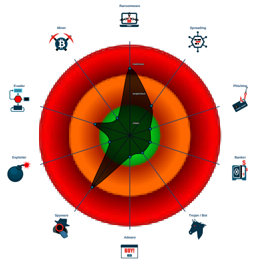
Thanos

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Thanos ransomware
- Tries to harvest and steal browser in…
- AV process strings found (often use…
- Queries the volume information (nam…
- Installs a raw input device (often for …
- PE file contains strange resources
- Checks for available system drives …

Classification



Process Tree

- **System is w10x64**
- Everything.exe (PID: 5704 cmdline: "C:\Users\user\Desktop\Everything.exe" MD5: B2E26B3562562D5C2647EB466FD17EB6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Everything.exe PID: 5704	JoeSecurity_Thanos	Yara detected Thanos ransomware	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Thanos ransomware

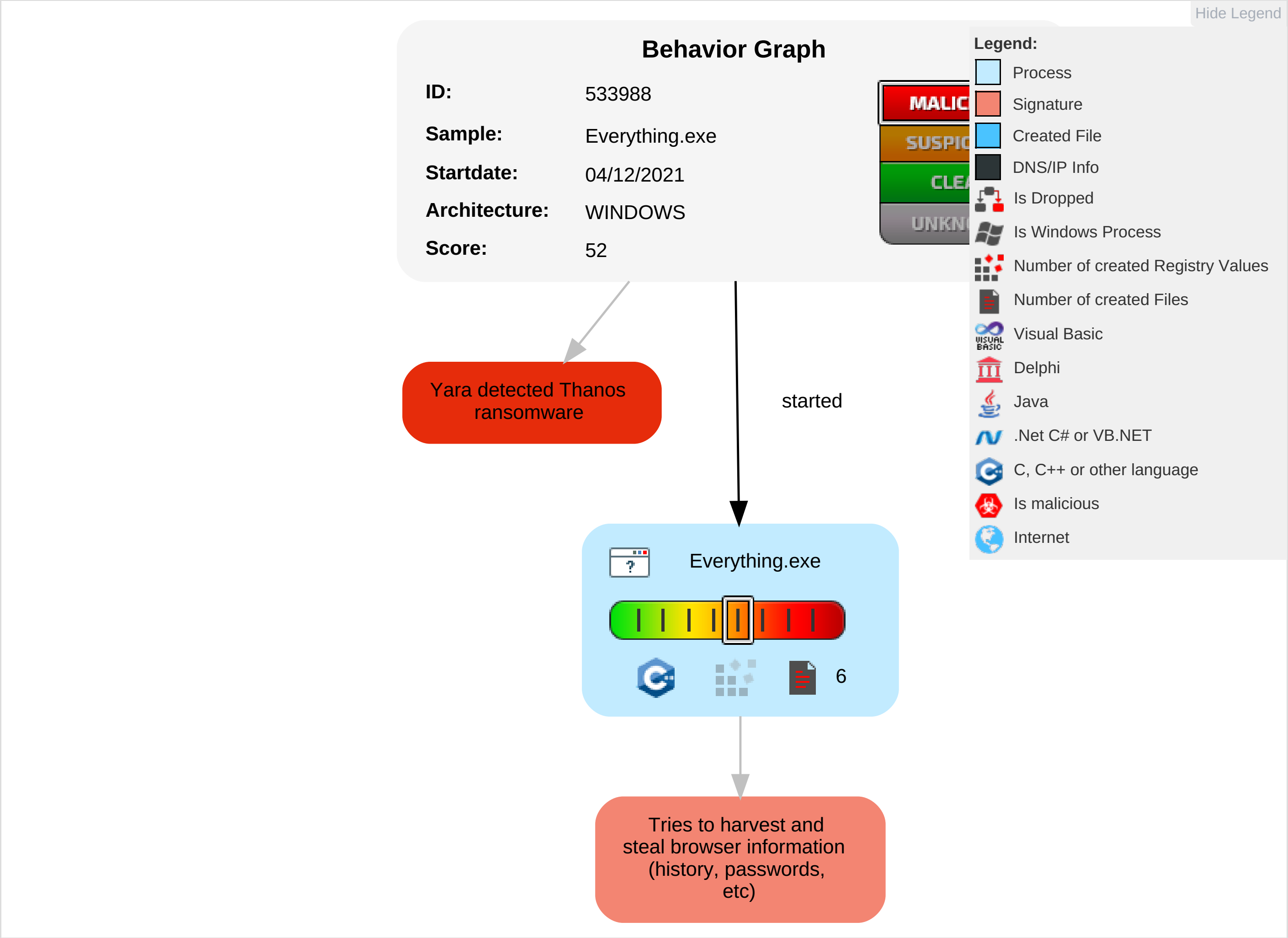
Stealing of Sensitive Information:

Tries to harvest and steal browser information (history, passwords, etc)

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
Replication Through Removable Media 1	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping 1	Security Software Discovery 1 1	Replication Through Removable Media 1	Input Capture 1 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Devi Without Authorizati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	Input Capture 1 1	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



Hide Legend

Behavior Graph

ID: 533988

Sample: Everything.exe

Startdate: 04/12/2021

Architecture: WINDOWS

Score: 52

MALIC
SUSPIC
CLEA
UNKN
Yara detected Thanos ransomware
started
Everything.exe
6
Tries to harvest and steal browser information (history, passwords, etc)

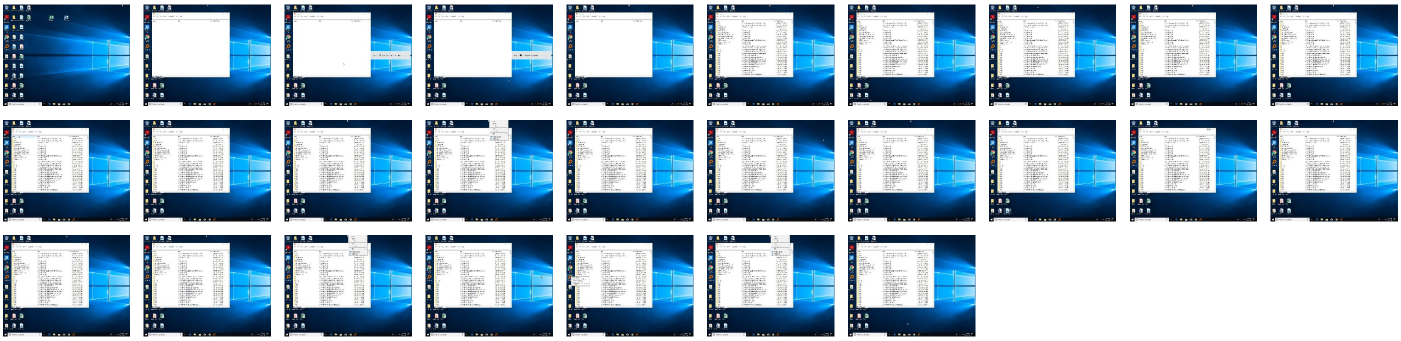
Legend:

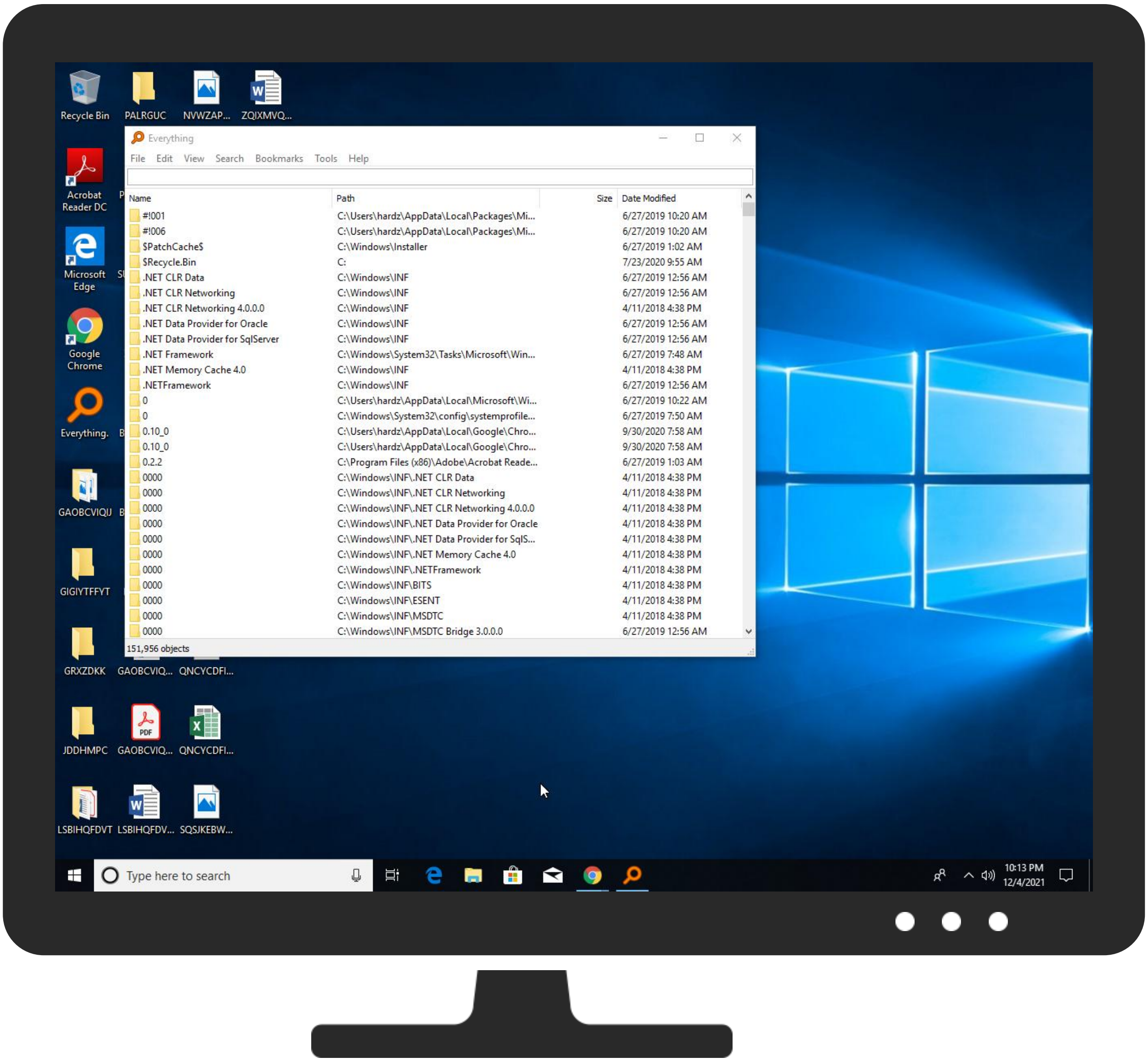
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Screenshots

Thumbnails

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





Name	Path	Size	Date Modified
#!001	C:\Users\hardz\AppData\Local\Packages\Mi...		6/27/2019 10:20 AM
#!006	C:\Users\hardz\AppData\Local\Packages\Mi...		6/27/2019 10:20 AM
$PatchCache$	C:\Windows\Installer		6/27/2019 1:02 AM
$Recycle.Bin	C:		7/23/2020 9:55 AM
.NET CLR Data	C:\Windows\INF		6/27/2019 12:56 AM
.NET CLR Networking	C:\Windows\INF		6/27/2019 12:56 AM
.NET CLR Networking 4.0.0.0	C:\Windows\INF		4/11/2018 4:38 PM
.NET Data Provider for Oracle	C:\Windows\INF		6/27/2019 12:56 AM
.NET Data Provider for SqlServer	C:\Windows\INF		6/27/2019 12:56 AM
.NET Framework	C:\Windows\System32\Tasks\Microsoft\Win...		6/27/2019 7:48 AM
.NET Memory Cache 4.0	C:\Windows\INF		4/11/2018 4:38 PM
.NETFramework	C:\Windows\INF		6/27/2019 12:56 AM
0	C:\Users\hardz\AppData\Local\Microsoft\Wi...		6/27/2019 10:22 AM
0	C:\Windows\System32\config\systemprofile...		6/27/2019 7:50 AM
0.10_0	C:\Users\hardz\AppData\Local\Google\Chro...		9/30/2020 7:58 AM
0.10_0	C:\Users\hardz\AppData\Local\Google\Chro...		9/30/2020 7:58 AM
0.2.2	C:\Program Files (x86)\Adobe\Acrobat Reade...		6/27/2019 1:03 AM
0000	C:\Windows\INF\.NET CLR Data		4/11/2018 4:38 PM
0000	C:\Windows\INF\.NET CLR Networking		4/11/2018 4:38 PM
0000	C:\Windows\INF\.NET CLR Networking 4.0.0.0		4/11/2018 4:38 PM
0000	C:\Windows\INF\.NET Data Provider for Oracle		4/11/2018 4:38 PM
0000	C:\Windows\INF\.NET Data Provider for SqlS...		4/11/2018 4:38 PM
0000	C:\Windows\INF\.NET Memory Cache 4.0		4/11/2018 4:38 PM
0000	C:\Windows\INF\.NETFramework		4/11/2018 4:38 PM
0000	C:\Windows\INF\BITS		4/11/2018 4:38 PM
0000	C:\Windows\INF\ESENT		4/11/2018 4:38 PM
0000	C:\Windows\INF\MSDTC		4/11/2018 4:38 PM
0000	C:\Windows\INF\MSDTC Bridge 3.0.0.0		6/27/2019 12:56 AM

151,956 objects

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Everything.exe	0%	Virustotal		Browse
Everything.exe	0%	Metadefender		Browse
Everything.exe	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	533988
Start date:	04.12.2021
Start time:	22:10:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Everything.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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:	mal52.rans.spyw.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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) x86-64, for MS Windows
Entropy (8bit):	6.5538245305677245
TrID:	• Win64 Executable GUI (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Everything.exe
File size:	2260560
MD5:	b2e26b3562562d5c2647eb466fd17eb6
SHA1:	52aacfe08a0d514ebcc1a6340659145145cfa400
SHA256:	66b9610e94d003a2b44abe976524c0181d808b8b8e663a 26378204a71165aecd
SHA512:	040c9fecd0c97904943fb24371c9c8a3f0962b5917c9782 b2441778dc002b0112e937a2c83995ab9ec95a1ec802aa 41a08ef782ca7b0a96f648145621cb9fbf7
SSDEEP:	49152:GoJjoQNXnzFDyh07AVWFOl2B3Pqv1tFqOay6Ji 4OOV4ckrx:GoZzYhErBo9D/Urk9
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$........E.u.$.&. $.&.$.&...&.$.&...&.$.&...&.$.&...&.$.&.$.&.%.&...&u$.&... &.$.&...&.$.&Rich.$.&........................PE..d....e.`...

File Icon

🔍	
Icon Hash:	e1d89c8c98e46683

Static PE Info

General

Entrypoint:	0x1401a9d10
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x600E6583 [Mon Jan 25 06:30:27 2021 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:	e396317e0c41e0f27509668e8b94edb7

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=DigiCert SHA2 Assured ID Code Signing CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 11/15/2020 4:00:00 PM 3/17/2022 4:59:59 PM
Subject Chain	• CN=voidtools, O=voidtools, L=Wilmington, S=South Australia, C=AU
Version:	3
Thumbprint MD5:	3A87B1969EBF5AE3902466A24594F034
Thumbprint SHA-1:	B5B6468C781744765A590C0FE13AA418FC3335D1
Thumbprint SHA-256:	4305C18985398C70E97EBC77CA324F10285782FD81577BA047B3BB55301C4F54
Serial:	0EAE3BA49CF8C17C1257CDDF597DA847

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1aeb5e	0x1aec00	False	0.411908734765	data	6.46175691631	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1b0000	0x4b686	0x4b800	False	0.290957419288	data	5.78852274837	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1fc000	0x135e8	0x11e00	False	0.358623798077	data	5.73557878982	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x210000	0xc9cc	0xca00	False	0.48497447401	data	6.18084382443	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x21d000	0xa1e4	0xa200	False	0.332296489198	data	4.58887803299	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x228000	0x31ae	0x3200	False	0.161796875	GLS_BINARY_LSB_FIRST	3.93155021834	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Everything.exe PID: 5704 Parent PID: 5820

General

Start time:	22:11:27
Start date:	04/12/2021
Path:	C:\Users\user\Desktop\Everything.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Everything.exe"
Imagebase:	0x7ff6f89c0000
File size:	2260560 bytes
MD5 hash:	B2E26B3562562D5C2647EB466FD17EB6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal