ID: 492525
Sample Name: yjOapKcgE1
Cookbook: default.jbs
Time: 19:35:45
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

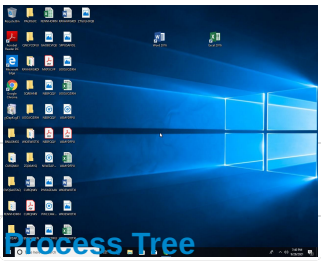
Windows Analysis Report yjOapKcgE1

Overview

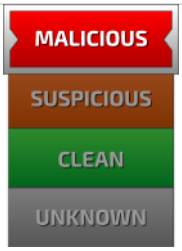
General Information

Sample Name:	yjOapKcgE1 (renamed file extension from none to exe)
Analysis ID:	492525
MD5:	1d46afb839b846e.
SHA1:	8cffc99cda16d5d…
SHA256:	d158534622b057..
Tags:	exe Troldesh
Infos:	

Most interesting Screenshot:



Detection



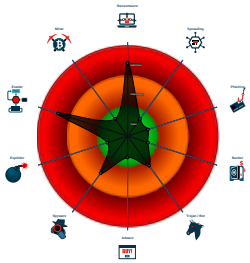
CryptOne Shade

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

Signatures

- Yara detected Shade Ransomware
- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Detected CryptOne packer
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Found Tor onion address
- Contains functionalty to change the …
- May use the Tor software to hide its…
- Deletes shadow drive data (may be …
- Drops PE files with benign system n…
- Uses 32bit PE files

Classification



- **System is w10x64**
- yjOapKcgE1.exe (PID: 6320 cmdline: 'C:\Users\user\Desktop\yjOapKcgE1.exe' MD5: 1D46AFB839B846EDE01CB925470F0488)
- csrss.exe (PID: 5888 cmdline: 'C:\ProgramData\Windows\csrss.exe' MD5: 1D46AFB839B846EDE01CB925470F0488)
- csrss.exe (PID: 5636 cmdline: 'C:\ProgramData\Windows\csrss.exe' MD5: 1D46AFB839B846EDE01CB925470F0488)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: csrss.exe PID: 5636	JoeSecurity_Shade	Yara detected Shade Ransomware	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file

Networking:

- Found Tor onion address

Spam, unwanted Advertisements and Ransom Demands:

- Yara detected Shade Ransomware
- Contains functionalty to change the wallpaper
- Deletes shadow drive data (may be related to ransomware)

Data Obfuscation:

- Detected CryptOne packer

Persistence and Installation Behavior:

- Drops PE files with benign system names

Hooking and other Techniques for Hiding and Protection:

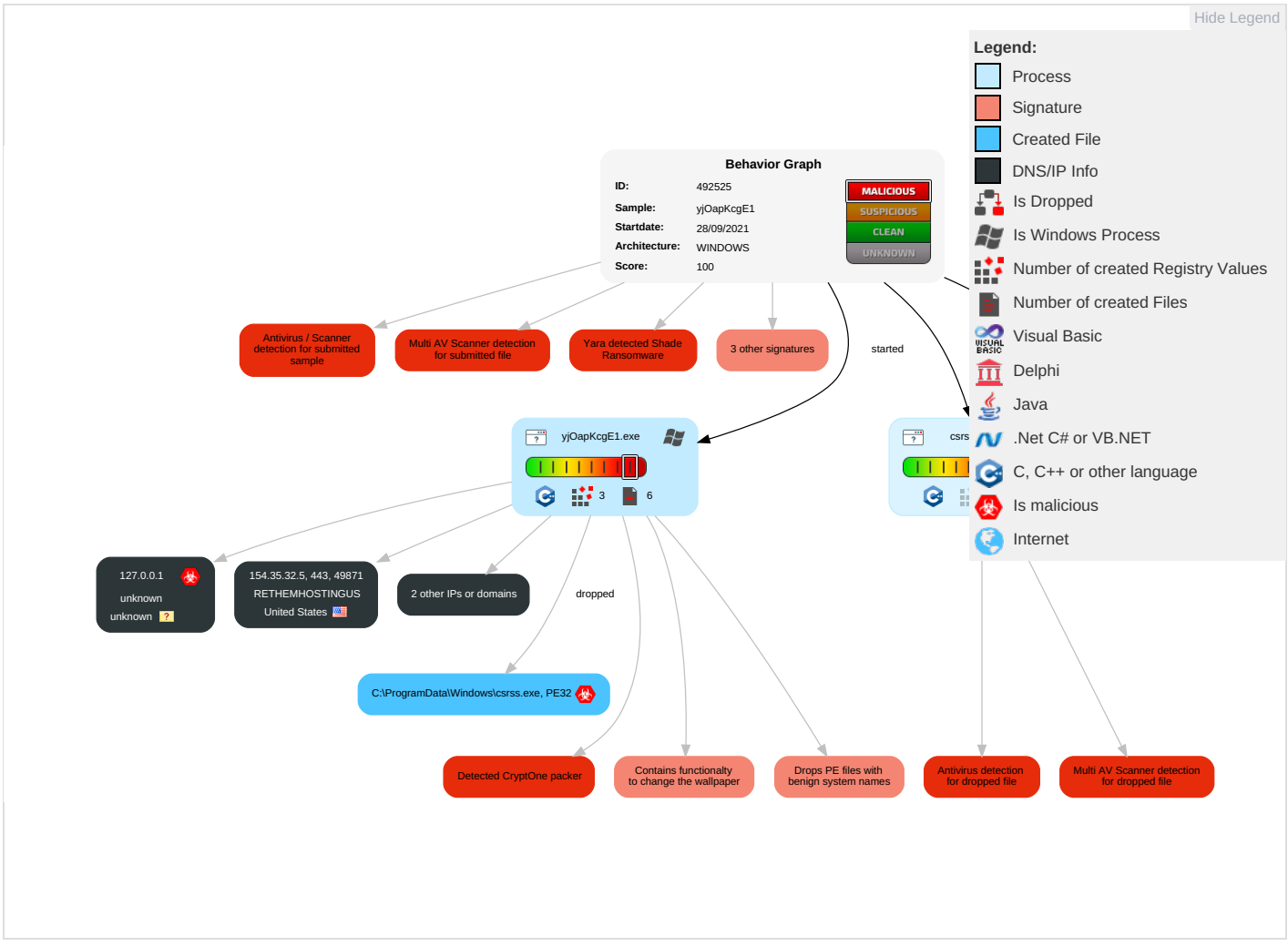
- May use the Tor software to hide its network traffic

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2 2	Eavesdrop on Insecure Network Communicatic
Default Accounts	Command and Scripting Interpreter 2	Application Shimming 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 1	Application Shimming 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Multi-hop Proxy 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 2	Software Packing 1 3	NTDS	System Information Discovery 4 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Proxy 2	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Process Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellula Base Station

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
yjOapKcgE1.exe	67%	Virustotal		Browse
yjOapKcgE1.exe	69%	Metadefender		Browse
yjOapKcgE1.exe	87%	ReversingLabs	Win32.Ransomware.AvaddonCrypt	
yjOapKcgE1.exe	100%	Avira	TR/Crypt.XPACK.Gen2	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\Windows\csrss.exe	100%	Avira	TR/Crypt.XPACK.Gen2	
C:\ProgramData\Windows\csrss.exe	67%	Virustotal		Browse
C:\ProgramData\Windows\csrss.exe	69%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\ProgramData\Windows\csrss.exe	87%	ReversingLabs	Win32.Ransomware.AvaddonCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.csrss.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
0.2.yjOapKcgE1.exe.400000.0.unpack	100%	Avira	TR/Crypt.FKM.Gen		Download File
4.2.csrss.exe.2480000.2.unpack	100%	Avira	TR/Crypt.FKM.Gen		Download File
2.2.csrss.exe.400000.0.unpack	100%	Avira	TR/Crypt.FKM.Gen		Download File
2.2.csrss.exe.2480000.2.unpack	100%	Avira	TR/Crypt.FKM.Gen		Download File
0.2.yjOapKcgE1.exe.2270000.2.unpack	100%	Avira	TR/Crypt.FKM.Gen		Download File
2.0.csrss.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
0.0.yjOapKcgE1.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
4.2.csrss.exe.400000.0.unpack	100%	Avira	TR/Crypt.FKM.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://a4ad4ip2xzclh6fd.onionreg.phpprog.phperr.phpcmd.phpsys.phpshd.phpmail.php?&v=b=i=k=ss=e=c=f=s	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.35.32.5	unknown	United States		14987	RETHEMHOSTINGUS	false
76.73.17.194	unknown	United States		25921	LUS-FIBER-LCGUS	false
193.23.244.244	unknown	Germany		50472	CHAOS-ASDE	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492525
Start date:	28.09.2021
Start time:	19:35:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 44s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	yjOapKcgE1 (renamed file extension from none to 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:	21
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.evad.winEXE@3/3@0/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 57% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:36:56	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Client Server Runtime Subsystem "C:\ProgramData\Windows\csrss.exe"
19:37:06	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Client Server Runtime Subsystem "C:\ProgramData\Windows\csrss.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
154.35.32.5	IEsSSwba4T.exe	Get hash	malicious	Browse	
	NtA6ABwq75.exe	Get hash	malicious	Browse	
	OR1kcoDd2F.exe	Get hash	malicious	Browse	
	y2N49ht6t4.exe	Get hash	malicious	Browse	
	2te6lkdbJu.exe	Get hash	malicious	Browse	
	fu3fXqZvuo.exe	Get hash	malicious	Browse	
	jTI7J7BCUj.exe	Get hash	malicious	Browse	
	75dZK4LPMP.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Encoder.10507.20567.exe	Get hash	malicious	Browse	
	437#U0435.js	Get hash	malicious	Browse	
	437#U0435.js	Get hash	malicious	Browse	
	437#U0435.js	Get hash	malicious	Browse	
	1.12.2018.js	Get hash	malicious	Browse	
	1.12.2018.js	Get hash	malicious	Browse	
	1.12.2018.js	Get hash	malicious	Browse	
	1.12.2018.js	Get hash	malicious	Browse	
	1.12.2018.js	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1.12.2018.js	Get hash	malicious	Browse	
	1.12.2018.js	Get hash	malicious	Browse	
	1.12.2018.js	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RETHEMHOSTINGUS	IEsSSwba4T.exe	Get hash	malicious	Browse	• 154.35.32.5
	NtA6ABwq75.exe	Get hash	malicious	Browse	• 154.35.32.5
	OR1kcoDd2F.exe	Get hash	malicious	Browse	• 154.35.32.5
	y2N49ht6t4.exe	Get hash	malicious	Browse	• 154.35.32.5
	Cx1HKT0xhO.exe	Get hash	malicious	Browse	• 154.35.175.225
	ac1khvFT2V.exe	Get hash	malicious	Browse	• 154.35.175.225
	re.a1rmv4l	Get hash	malicious	Browse	• 149.9.143.167
	2te6IkdbJu.exe	Get hash	malicious	Browse	• 154.35.32.5
	fu3fXqZvuo.exe	Get hash	malicious	Browse	• 154.35.32.5
	jTI7J7BCUj.exe	Get hash	malicious	Browse	• 154.35.32.5
	75dZK4LPMP.exe	Get hash	malicious	Browse	• 154.35.32.5
	e4phNkmjAJ	Get hash	malicious	Browse	• 154.35.8.244
	oEF7GAiRIg	Get hash	malicious	Browse	• 154.35.8.254
	SecuriteInfo.com.W32.MSIL_Kryptik.EWM.genEldorado.30775.exe	Get hash	malicious	Browse	• 154.35.175.225
	97238623.exe	Get hash	malicious	Browse	• 154.35.175.225
	FB11.exe	Get hash	malicious	Browse	• 154.35.175.225
	HUahIwV82u.exe	Get hash	malicious	Browse	• 154.35.175.225
	6d0000.exe	Get hash	malicious	Browse	• 154.35.175.225
	osiris.exe	Get hash	malicious	Browse	• 154.35.175.225
	6729001591617.exe	Get hash	malicious	Browse	• 154.35.175.225

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
1be3ecebe5aa9d3654e6e703d81f6928	OR1kcoDd2F.exe	Get hash	malicious	Browse	• 193.23.244.244
	i0DixfP527.exe	Get hash	malicious	Browse	• 193.23.244.244
	zjnO2flTJj.exe	Get hash	malicious	Browse	• 193.23.244.244
	fu3fXqZvuo.exe	Get hash	malicious	Browse	• 193.23.244.244
	-2019.xls.js	Get hash	malicious	Browse	• 193.23.244.244
	-2019.xls.js	Get hash	malicious	Browse	• 193.23.244.244
	0-10-2019.js	Get hash	malicious	Browse	• 193.23.244.244
	2c.exe	Get hash	malicious	Browse	• 193.23.244.244
	Uy5w2nr1M7.exe	Get hash	malicious	Browse	• 193.23.244.244
	9.03.docx.js	Get hash	malicious	Browse	• 193.23.244.244
	9.03.docx.js	Get hash	malicious	Browse	• 193.23.244.244
	8.29.docx.js	Get hash	malicious	Browse	• 193.23.244.244
	8.29.docx.js	Get hash	malicious	Browse	• 193.23.244.244
	8.19.docx.js	Get hash	malicious	Browse	• 193.23.244.244
	8.19.docx.js	Get hash	malicious	Browse	• 193.23.244.244
	8.20.docx.js	Get hash	malicious	Browse	• 193.23.244.244
	0812.docx.js	Get hash	malicious	Browse	• 193.23.244.244
	08-06.doc.js	Get hash	malicious	Browse	• 193.23.244.244
	0807.docx.js	Get hash	malicious	Browse	• 193.23.244.244
	0807.docx.js	Get hash	malicious	Browse	• 193.23.244.244

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Windows\csrss.exe	
Process:	C:\Users\user\Desktop\yjOapKcgE1.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1244429
Entropy (8bit):	7.173731916265485
Encrypted:	false
SSDEEP:	24576:XHtrdKYVVSrqGDohJ3STZG8vIn/sCBGnWsY0Dy0:XHtV7GwBSTc8An/4YF0
MD5:	1D46AFB839B846EDE01CB925470F0488
SHA1:	8CFFC99CDA16D5D6B5192C62FEFAE6C0AC89B33D
SHA-256:	D158534622B057B387A617EBE2931FEF6D5C7D386B6DFBEB652C4781846F87C1
SHA-512:	888862EF478C79823A56AF36F303E5A5686CE31BFDCB4E9B630E8BEA791F10BF52F22B7FDB24BE4B01B6087292467B45EBEB52D4F954B482F24094AF14F64F10
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 67%, Browse • Antivirus: Metadefender, Detection: 69%, Browse • Antivirus: ReversingLabs, Detection: 87%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.>.X.m.X.m.X.m...m.X.m.X.m.Y.m..Qm.X.m.X.m.X.m..Fm .X.m..Cm.X.mRich.X.m.....PE..L....Zv\.....2.....`8.....P....@..... .....[..x..... .....P.....text...<1.....2..... ..`.rdata...+...P.....6.....@..@.data...X.....b.....@....rsrc.....d.....@..@..... ....

C:\Users\user\AppData\Local\Temp\6893A5D897\state.tmp	
Process:	C:\Users\user\Desktop\yjOapKcgE1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	199
Entropy (8bit):	4.78811407542215
Encrypted:	false
SSDEEP:	6:SbdWwxXN51+3tnXr87+QVe2vwR/EtbWCd8D5Hu:bwxXnc3tXr87HVBvwNi2Hu
MD5:	EE3B9638644A5EE616E2216088445594
SHA1:	E36AC55FE4BFCCF53CA10A36A53CA916ACD64EBB
SHA-256:	9FFE9AF033FBE8847C4992D95ADE7F8EDADF6124A7356E98E9A3CFFA455A6212
SHA-512:	F244B2DE284D60E17F83F3EA1652DFDFF1446C5181A53F9C13B4D445B7743133945A24EC06F2F7AA9E78C66D87DE83857D61FDF799DCC96FA716DC0B41503F3
Malicious:	false
Reputation:	low
Preview:	# Tor state file last generated on 2021-09-28 19:36:53 local time..# Other times below are in UTC..# You *do not* need to edit this file.....TorVersion Tor 0.2.5.10..Last Written 2021-09-29 02:36:53..

C:\Users\user\AppData\Local\Temp\6893A5~1\state (copy)	
Process:	C:\Users\user\Desktop\yjOapKcgE1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	199
Entropy (8bit):	4.78811407542215
Encrypted:	false
SSDEEP:	6:SbdWwxXN51+3tnXr87+QVe2vwR/EtbWCd8D5Hu:bwxXnc3tXr87HVBvwNi2Hu
MD5:	EE3B9638644A5EE616E2216088445594
SHA1:	E36AC55FE4BFCCF53CA10A36A53CA916ACD64EBB
SHA-256:	9FFE9AF033FBE8847C4992D95ADE7F8EDADF6124A7356E98E9A3CFFA455A6212
SHA-512:	F244B2DE284D60E17F83F3EA1652DFDFF1446C5181A53F9C13B4D445B7743133945A24EC06F2F7AA9E78C66D87DE83857D61FDF799DCC96FA716DC0B41503F3
Malicious:	false
Reputation:	low
Preview:	# Tor state file last generated on 2021-09-28 19:36:53 local time..# Other times below are in UTC..# You *do not* need to edit this file.....TorVersion Tor 0.2.5.10..Last Written 2021-09-29 02:36:53..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.173731916265485

General

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:	yjOapKcgE1.exe
File size:	1244429
MD5:	1d46afb839b846ede01cb925470f0488
SHA1:	8cffc99cda16d5d6b5192c62fefae6c0ac89b33d
SHA256:	d158534622b057b387a617ebe2931fef6d5c7d386b6dfbeb652c4781846f87c1
SHA512:	888862ef478c79823a56af36f303e5a5686ce31bfdcb4e9b630e8bea791f10bf52f22b7fdb24be4b01b6087292467b45ebeb52d4f954b482f24094af14f64f10
SSDEEP:	24576:XHtrdKYVVSrqGDohJ3STZG8vIn/sCBGnWsY0Dy0:XHtV7GwBSTc8An/4YF0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.>.X.m.X.m.X.m...m.X.m.X.m.Y.m..Qm.X.m.X.m.X.m..Fm.X.m..Cm.X.mRich.X.m.....PE..L....Zv\.....2.....

File Icon

Icon Hash:	f8e0e4e8ecccc870

Static PE Info

General

Entrypoint:	0x513860
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5C765ADF [Wed Feb 27 09:39:43 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	b90027f65707ca9644c551e337fa02ad

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x11313c	0x113200	False	0.805441773626	data	7.1245745803	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x115000	0x2b2e	0x2c00	False	0.416725852273	data	5.57043666657	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x118000	0x358	0x200	False	0.640625	data	4.12281643222	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x119000	0xeead8	0x18c00	False	0.767617582071	data	7.1377470027	IMAGE_SCN_CNT_INITIALIZED_DATA, 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

Network Port Distribution

TCP Packets

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: yjOapKcgE1.exe PID: 6320 Parent PID: 6552

General

Start time:	19:36:46
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\yjOapKcgE1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\yjOapKcgE1.exe'
Imagebase:	0x400000
File size:	1244429 bytes
MD5 hash:	1D46AFB839B846EDE01CB925470F0488
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: csrss.exe PID: 5888 Parent PID: 3440

General

Start time:	19:37:06
Start date:	28/09/2021
Path:	C:\ProgramData\Windows\csrss.exe
Wow64 process (32bit):	true
Commandline:	'C:\ProgramData\Windows\csrss.exe'
Imagebase:	0x400000
File size:	1244429 bytes
MD5 hash:	1D46AFB839B846EDE01CB925470F0488
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 67%, Virustotal, Browse • Detection: 69%, Metadefender, Browse • Detection: 87%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

Analysis Process: csrss.exe PID: 5636 Parent PID: 3440

General

Start time:	19:37:14
Start date:	28/09/2021
Path:	C:\ProgramData\Windows\csrss.exe
Wow64 process (32bit):	true
Commandline:	'C:\ProgramData\Windows\csrss.exe'
Imagebase:	0x400000
File size:	1244429 bytes
MD5 hash:	1D46AFB839B846EDE01CB925470F0488
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

Disassembly

Code Analysis