ID: 339438
Sample Name: VCPjXmY0pr
Cookbook: default.jbs
Time: 03:08:55
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

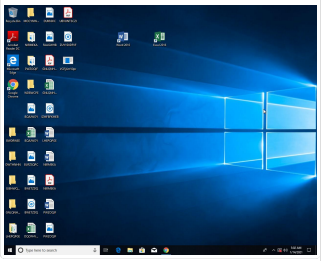
Analysis Report VCPjXmY0pr

Overview

General Information

Sample Name:	VCPjXmY0pr (renamed file extension from none to exe)
Analysis ID:	339438
MD5:	053ddb3b6e38f9b.
SHA1:	2f26c6f5a9dbf6b…
SHA256:	2d8151dabf891cf..

Most interesting Screenshot:



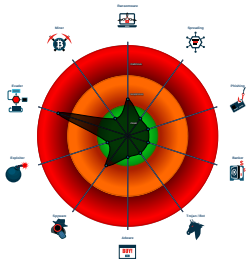
Detection

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected unpacking (overwrites its o…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- .NET source code contains potentia…
- .NET source code references suspic…
- Machine Learning detection for samp…
- Contains long sleeps (>= 3 min)
- Detected potential crypto function
- Drops PE files
- Enables debug privileges
- Entry point lies outside standard sec…

Classification



Startup

- **System is w10x64**
- VCPjXmY0pr.exe (PID: 4792 cmdline: 'C:\Users\user\Desktop\VCPjXmY0pr.exe' MD5: 053DDB3B6E38F9BDBC5FB51FDD44D3AC)
  - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
VCPjXmY0pr.exe	apt_RU_Turla_Kazuar_DebugView_peFeatures	Turla mimicking SysInternals Tools- peFeatures	JAG-S	
VCPjXmY0pr.exe	APT_MAL_RU_Turla_Kazuar_May20_1	Detects Turla Kazuar malware	Florian Roth	• 0x69f62:$s1: Sysinternals • 0x69f74:$s1: Sysinternals • 0x6b4e4:$s2: Test Copyright • 0x69f3c:$op1: 0D 01 00 08 34 2E 38 30 2E 30 2E 30 0 0 00 13 01

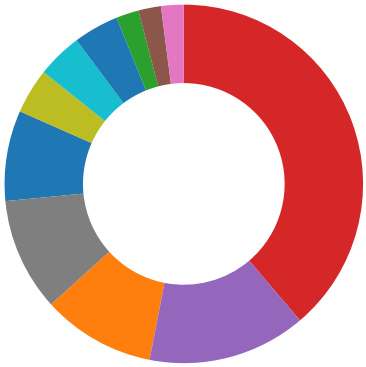
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\7092ee1bf1e386348e9ed2a7b68b7ab2.dll	Turla_KazuarRAT	Detects Turla Kazuar RAT described by DrunkBinary	Markus Neis / Florian Roth	• 0x642:$x1: ~1.EXE

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

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

Compliance:

- Detected unpacking (overwrites its own PE header)

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (overwrites its own PE header)
- .NET source code contains potential unpacker

HIPS / PFW / Operating System Protection Evasion:

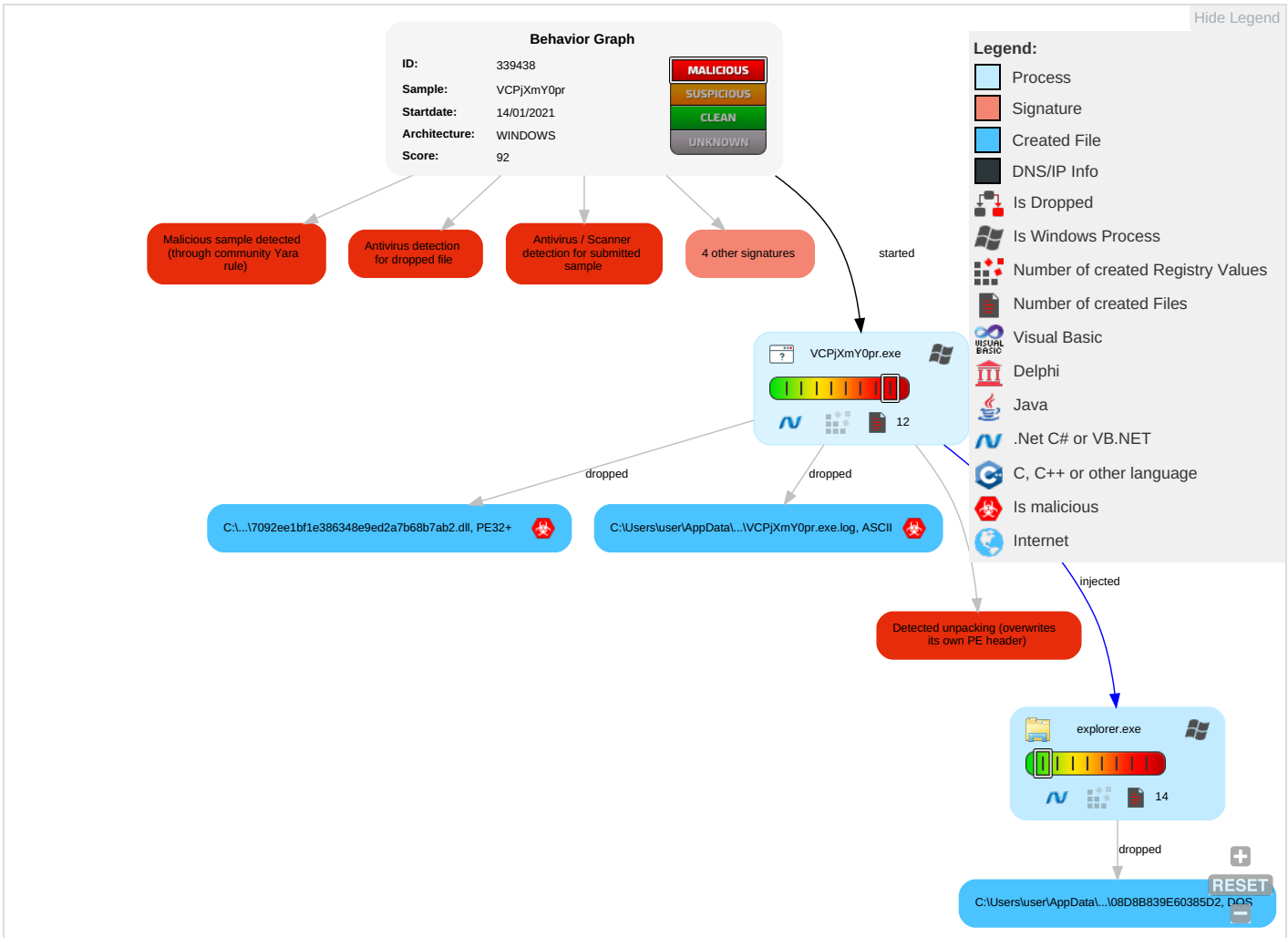
- .NET source code references suspicious native API functions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Rer Ser Effe

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Rem Ser Effe
Valid Accounts	Native API 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Rem Tra Witl Aut
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Rem Wip Witl Aut
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obt Dev Clo Bac
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

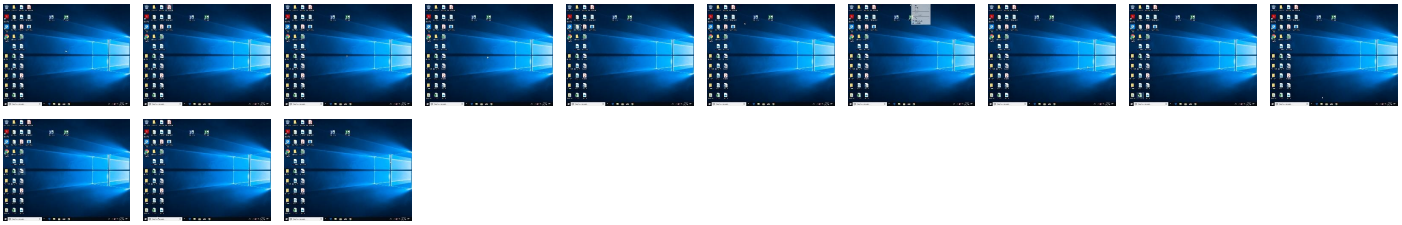
Behavior Graph



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
VCPjXmY0pr.exe	76%	Virustotal		Browse
VCPjXmY0pr.exe	73%	ReversingLabs	ByteCode-MSIL.Trojan.Cassowar	
VCPjXmY0pr.exe	100%	Avira	TR/Crypt.XPACK.Gen	
VCPjXmY0pr.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\7092ee1bf1e386348e9ed2a7b68b7ab2.dll	100%	Avira	HEUR/AGEN.1126242	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.VCPjXmY0pr.exe.62480000.1.unpack	100%	Avira	HEUR/AGEN.1126242		Download File
0.0.VCPjXmY0pr.exe.9b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.VCPjXmY0pr.exe.9b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.weauthenticate.co.uk/wp-content/languages/index.php	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://www.weauthenticate.co.uk/wp-content/languages/index.php1https://jaireve.co/wp-content/langua	0%	Avira URL Cloud	safe	
http://go.micros	0%	URL Reputation	safe	
http://go.micros	0%	URL Reputation	safe	
http://go.micros	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://jaireve.co/wp-content/languages/index.php	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false		high
http://https://www.weauthenticate.co.uk/wp-content/languages/index.php	VCPjXmY0pr.exe, 00000000.00000 002.688799779.0000000003011000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.weauthenticate.co.uk/wp-content/languages/index.php1https://jaireve.co/wp-content/langua	VCPjXmY0pr.exe, 00000000.00000 002.688799779.0000000003011000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://go.micros	VCPjXmY0pr.exe, 00000000.00000 002.685997706.0000000000E1A000 .00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://jaireve.co/wp-content/languages/index.php	VCPjXmY0pr.exe, 00000000.00000 002.688799779.0000000003011000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000001.0000000 0.666551645.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000001.0000000 0.678657512.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339438
Start date:	14.01.2021
Start time:	03:08:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VCPjXmY0pr (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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.evad.winEXE@1/13@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 6.3% (good quality ratio 5.5%) • Quality average: 81.8% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
03:10:08	API Interceptor	1099x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\7092ee1bf1e386348e9ed2a7b68b7ab2.dll	
Process:	C:\Users\user\Desktop\VCPjXmY0pr.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	8704
Entropy (8bit):	3.43117265490537
Encrypted:	false
SSDEEP:	96:ZfffhRFqx1h0OIs+gJvtYjCT9018zSTJlBLx4ZW5:1ffhRA1dNt+CT9c8+bhx4E
MD5:	3A73460B3E70A0F3F6F0CBF0C73EFECF
SHA1:	15FE33F04BA640E818A29E954D2DF5CC29646D05
SHA-256:	3A948163073EDCD69A47F69EAFBC088C267CDE7AA752866DF516EA948BF62660
SHA-512:	893E49E9DC3F57B93049BBD5322682EA0875E2A034DB9A74C13C7A6901464932C7C8F16A9EC97F8D4A96C8B839811FC80A41A1589FF4740310436AA33FE2D632
Malicious:	**true**
Yara Hits:	• Rule: Turla_KazuarRAT, Description: Detects Turla Kazuar RAT described by DrunkBinary, Source: C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\7092ee1bf1e386348e9ed2a7b68b7ab2.dll, Author: Markus Neis / Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...F..V....."....0.....Hb..... ....p..V.....P..<.....H.....text...`..... .P`.wtf..... .....`. `..rdata.....@.....@.P@.pdata..<....P.....@.0@.xdata..,....`.....@.0@.edata..V....p.....@.0@.idata..... .....@.0..... ....

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\c34b132bff0230a28757d24f730ae477\aa898d6f9ffba4432ce9bb2a8b2154f7	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.875
Encrypted:	false
SSDEEP:	3:AHGaufVR:faufb
MD5:	E8AD3C40BB7406C96C34C723E602058E
SHA1:	54FADCACF2B8CE54A8B600D05CFAF19E4B85C20F
SHA-256:	908969C5720C3971B4237AAF5C4B6B7FFEA9D01E9326597D7306574479D75DD5
SHA-512:	3FB9282CD9F116AD9DC814347F096F903C607D8C4E3C6CBD31F3C97414F986BC2216E7CDA33BFBD63E26B66F67AD609B1395B17660E48CC503F719BC58EDC7F
Malicious:	false
Reputation:	low
Preview:	#w...K:2..Y..

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\c34b132bff0230a28757d24f730ae477\aace0a8af5e9a62f21d9da31e5909f00	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.875
Encrypted:	false
SSDEEP:	3:h74uK5:h65
MD5:	2380A415BADE4A821DC65C0FBF0B4502
SHA1:	D66BBA11FC460C1CF46A1A98AD09505C40709C30
SHA-256:	BCC90DEDF52059B2CD9275E6214EAA7A274926B1C780D104A645F9FC13E4BFDF
SHA-512:	437857CD1239F7FD0A701F7963DDA722BDF8D0DB539E33C96BB1FA3ECC60A804459CC0E736EEF4AFA04D466DA763CA4EEF4606E762F00EF44F950B7300DA103
Malicious:	false
Reputation:	low
Preview:	.C7.....u.i...

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\c34b132bff0230a28757d24f730ae477\b96aff2c7cf2b4afd20609e7a7ab021c	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	5.887492001110317
Encrypted:	false
SSDEEP:	3:OK/aggxrF8RzBRnim0DUUxHcBzWQVNz8:laxxB8VBRim4CzM

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\c34b132bff0230a28757d24f730ae477\b96aff2c7cf2b4afd20609e7a7ab021c	
MD5:	953D1568BAFDE7852BCD093EC0913C0B
SHA1:	EC707DC054F1D17E13A167FB18EE3409A9A5F7E6
SHA-256:	7A4DD0D6823D35E521E3D6757F52A625B3EB5EDF6E113D51556FA49C60408710
SHA-512:	892E0F92386EA4D060DABBBD0E75950BBFEB964189704DD793581764A49EF6B8EDA75A21D2098DB2A61E18C93BA8242C4BE6CA8FEA4BD768DAD32B7784AE78 68
Malicious:	false
Reputation:	low
Preview:	.....[.o.E.~.C.+z@. ...4.Q.....R..gR.Gk|..}\..M_9A&...$.....[.uQ_`h.E..

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839D84BA13E	
Process:	C:\Users\user\Desktop\VCPjXmY0pr.exe
File Type:	data
Category:	dropped
Size (bytes):	112
Entropy (8bit):	6.425614855073995
Encrypted:	false
SSDEEP:	3:sXNwEk8Ml+Bu0XoiRz95EPmaQki47a/zBiSaO:kyN8vKys6+8zBiK
MD5:	04CF6AEB7D2035FF39ACDBBCC8B2527D
SHA1:	C52200EFE8AA944C568490E82E50D9F75874A694
SHA-256:	C38B2BAE911E4FF846A7F89568FC9ABFD742A7887AA86DEC321CF87F3D8AAC62
SHA-512:	AAC78E59645D80658063CCA85585A9D42B8BAE8E748F3673D2A01BEBD53C09961B8C82AE2A85DE402FF791735F68252A741BDDA1E5FAE01903912ECE1B8636A 7
Malicious:	false
Reputation:	low
Preview:	/E...$....9B.....k.U.J.....M7b.9..s..'..t{.^A..J..}K...c..x.....-..$5.....C^.....t.A%..x-.....E`..K..,.?.

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839D871C6B0	
Process:	C:\Users\user\Desktop\VCPjXmY0pr.exe
File Type:	data
Category:	dropped
Size (bytes):	112
Entropy (8bit):	6.340706149678221
Encrypted:	false
SSDEEP:	3:pUtDciGq8DOSt7rUbf1vEFYi:atlicDOilbpYYi
MD5:	319E0F44349BF2868F0A52D6F22E7FEF
SHA1:	A2424982B6D02A3AE491CB1C66AD0315EC7B98D6
SHA-256:	BDD5918AB0460E88391E6480FB17055B153513C99CE28C2652521870DFF5502A
SHA-512:	DF1CE6259192E8A6372C271628A0C63555DABD833528D2E640B281AC0C673AC5AE3129DD5F443507622669EAD2CB06C34E6A1F1020E13AA4E71A2EAE35E6B76 A
Malicious:	false
Reputation:	low
Preview:	s..+.@..a.....\.[=..w.....n....2....i."(...F...w.:]....#...&+.1..4..Y6...+0N[.o@...6...p.z....I..

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839DB822E39	
Process:	C:\Users\user\Desktop\VCPjXmY0pr.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	5.45996250072116
Encrypted:	false
SSDEEP:	3:6vnfE9eE6p34lDuIKfi05mo:6vfacIQ3a05mo
MD5:	9D768A2AB59047A57AEF0EAB9E9150B2
SHA1:	83EEAE11C1D5A20E0E25460EEF81E1082F76DB0D
SHA-256:	8ABF552B4A6E556BC85B59AE6E9E3FB16C3EC8F854C2AE60CCC4F7AEC1D8851F
SHA-512:	DE02C768597E92B80F9521F175F157F42EDB93677F4CC3DACD64FE623248233E2B39317264789990833DAE43ED6C5555085528DBC2984FF607EED00262D2C4DF
Malicious:	false
Reputation:	low
Preview:	j.....&..Z/..|.!t.r..].&KBm..."..w...j..\.

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E1CB7D93	
Process:	C:\Users\user\Desktop\VCPjXmY0pr.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E1CB7D93	
Size (bytes):	112
Entropy (8bit):	6.447849006821076
Encrypted:	false
SSDEEP:	3:O+TBwCUvplvLspBqgryUrh9MkbfPwNVO4UC/Rt8Dq0n:ODZvplD8bmUckb3s84Uxm0n
MD5:	0599E47354E7869D17E2F2D371FD9A4D
SHA1:	7803D02514AB30E1F253E4D84C421C30CE1B11E7
SHA-256:	55B8ED3B56C23F3D9248BEB993209845144AC3A5C47AD13C61B43469ED98AD42
SHA-512:	523E40048250FCA70294E8D6772EF01B67892C88234F93F1A09C42CE2429DBF1B1D32C1778F94CE3F6166E843A7E9DBAC8A6CCF2AC0C04EFB374F4ECAC0BC68
Malicious:	false
Reputation:	low
Preview:	3,.vn6L...g..+...1....Z....jY..:#{*....t.ut.....-..)DX_.E'......n|.E.4.S...Qd....R.;.Z.V..i...$.C...J...

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E2B523CD	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	7.0259606872645275
Encrypted:	false
SSDEEP:	6:g1BKVEea8HZl9eb98ImCyn3y1wZnMKPbMYFX4B6Y7qsd:8Km85feHmPawlMKznDAld
MD5:	A1B3A295D26298A2690581AF0F45429A
SHA1:	8B23E45823F0737A69546206D4FE068BD60247EF
SHA-256:	8CFAB883110C21EEEA84C7903C06CAA00E3363D8B1D4DC9DEC607572FACB5847
SHA-512:	C4D34C54AF358FB2CBEAD88E6F7E752DCCFEB2E61FA1307594B20E764BB03AABC27440208E557771C86B5EF7C248C69959E2772956D086B7B45D513CD9B435A0
Malicious:	false
Reputation:	low
Preview:	.i.Q...4U.....!.._....{...5.p.....6&.T@EE.'M..O.,.f <_...`.6<.CR.Y....iC.,K|....w...)./..Rm7...\5C..(..Z.../..%.,<..7.F.....D...A..I).l....s..yU.II..0=Z..`..)Y\m.n.....d+.....$.}....R..t.e.J".....tL..p'i.d&...

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E2E27076	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	112
Entropy (8bit):	6.443471997931137
Encrypted:	false
SSDEEP:	3:rrFk2aaAcIDX84Ba8eCrJKe2I53/4PR6SfudY2Z:/FmaAcIDpBAKKe2I5P4Bu5
MD5:	695E1879159A131D5C0C4B59022ECE8B
SHA1:	6BF6D3A77BA01036B4E1E46067EDCB03204EE36C
SHA-256:	AE5EDC93F81ED89E59E0131A65D52F393788CF49E05D1745CCFC52987A61E746
SHA-512:	6E4B4D8F22ACE43B1D259746C600D00C5A93F59FB37B02DF0D4382444C27E0A5188DC2EE7D0F22789EB8722D3C84EA180B39E9B4CDE6E88C92BA908EDDB9538
Malicious:	false
Reputation:	low
Preview:	.w..,..\..`..ES.M..Px.R0..V.m&.%|V...3SZa.../.....[.wNBa}=...,#..i.....l.....jx..W..R.u..z...J..(&.O.=z..h

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E3016F16	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	7.145086064205293
Encrypted:	false
SSDEEP:	6:a/dFNm6M9v2NxGv40aINKg2E8DEo1PeTuc4yL8ujKSFN4:aFmbh2CFJaPcuQLzjNFC
MD5:	BE6561A67D1AB00A681AF4CB12642ECC
SHA1:	56A0615D4CF52D94D4D8A65422431AC27A0220D0
SHA-256:	D737A8B6845D5FE17E669CA15941817C307070AD0C9780C2E6A5981350F5F147
SHA-512:	0256E2B6ED67E75FA7BA46C177C9B1945CF1FC693F3FBC50FECEBAFB6F1978AA9B53B8E5B27B7B02C9AB526431376A5E02579A8A0204C8A5FF612BFA1A994AF3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E3016F16	
Preview:	D#.%.....948.....O.G..qIT..O...@.]Q..|..`.....8l'.O.....:7.K..9...0.;....|W..fd..a..f.F.....h8>.N...J..3..&.....YHL.6..4...W.~xz.....P..:.3J...HO.r.....(y.....q..^.....7zb@.1..S7.<=c.J.6,..\._.....;.*.b..1.....dk

C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E60385D2	
Process:	C:\Windows\explorer.exe
File Type:	DOS executable (COM, 0x8C-variant)
Category:	dropped
Size (bytes):	240
Entropy (8bit):	7.132088499710445
Encrypted:	false
SSDEEP:	6:iEO5b4sVVXSUZReqGbGODHVbYg0sV6/Id3B:iES/bZLGSObxYD0U+x
MD5:	A04816CC69F45D2D35B2B17E0825E516
SHA1:	A39ED2ACB35D964DA48CA471B6C195F3CEE2DCE8
SHA-256:	CF822EB734FE7C86232D3B73F14F75F20BC04E1D5D8AF273F2AA74009075CEAD
SHA-512:	57B2F9B5ABA74F6007E522FC155B3AE1858DC2A685C02D4AD44B7B350E85CFB8FBC6B01AC7CF34AE1A6905D8B0FF1A248F17EAF07D87ED576982B559672FCAFB
Malicious:	false
Reputation:	low
Preview:	.bd..Wr'^.)..NHA.'..y....2....Ib....n.C*...D.2.1n3$..pyB..:..b.j./..Q,*.8*yy<..u.. ..-....e...gN..-##})j.....t@.}."La.W./..'d}.0...?....Qf.....]..hz.dQo..y].pJ.....S....KN....J..[.....=F.f~E.pP.i...L.'TZ..sx...v.....%.~#....$

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\VCPjXmY0pr.exe.log	
Process:	C:\Users\user\Desktop\VCPjXmY0pr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	799
Entropy (8bit):	5.2380578532104165
Encrypted:	false
SSDEEP:	12:Q3LaJcP0x8FcX8LB0hK9cLK9Vi0kaHYGLi1B01kKVdisk70Hy+/Qav:MLc98iKSKSaYgioQ9+r
MD5:	E40C5BC96D6AB83BC7FB974CB8E061E8
SHA1:	3C16DFDC96D788A19EABDA33C7BDD9ED50482741
SHA-256:	3A40B63B6B44AB0E10C27B379DAC944CE97515D2686C966CB6949D20C1E4AAFD
SHA-512:	55293DE42130B23FD18E0DC27FD92DC457CDBC5F34FD99C8C1DF8D4E8D15B69679C7B07C8DEDD837D3D1B3DB6DBC11A4DB099B9AEB86122950D060F6A960CD
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System\1201f26cb986c93f55044bb4fa22b294\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.ServiceProce#\5e91b88ac0255894c4e0248b14fc4649\System.ServiceProcess.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuratio#\6425e89da7aea5916b90f1899ae542fb\System.Configuration.Install.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\b12bbcf27f41d96fe44360ae0b566f9b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\454c09ea87bde1d5f545d60232083b79\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Management\ae8d6eb6689c9ca2facd0d2924080164\System.Management.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.084065739720612
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	VCPjXmY0pr.exe
File size:	441344
MD5:	053ddb3b6e38f9bdbc5fb51fdd44d3ac
SHA1:	2f26c6f5a9dbf6bfb7690cb6949536775d1def92
SHA256:	2d8151dabf891cf743e67c6f9765ee79884d024b10d265119873b0967a09b20f

General

SHA512:	27c71d1565a7aa50f653c10e60e9b3316a7fc3817f8b38c6ef368c02b6397d803f3a4a9ec94c31c48d1a6fb24fc165aad1efb97d88a3ef7e8dabc6e3c1fdb4ea
SSDEEP:	12288:u2xqzEzF/N1XnGuceEvjYRi8XYDfHI240uW+GciFav2zDqlhE:hZF1RK
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L.....TZ.........."...0.............N.... ....@.. ....…@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46cf4e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5A54D3B4 [Tue Jan 9 14:37:40 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6cef4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6e000	0x638	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x70000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6af54	0x6b000	False	0.478949145736	data	6.09544139324	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x638	0x800	False	0.32275390625	data	3.47697527169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x70000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x6e0a0	0x3a6	data		
RT_MANIFEST	0x6e448	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Test Copyright
Assembly Version	4.80.0.0
InternalName	Agent.exe
FileVersion	4.80.0.0
CompanyName	Sysinternals
LegalTrademarks	Sysinternals
Comments	Sysinternals DebugView
ProductName	Sysinternals DebugView
ProductVersion	4.80.0.0

Description	Data
FileDescription	Sysinternals DebugView
OriginalFilename	Agent.exe

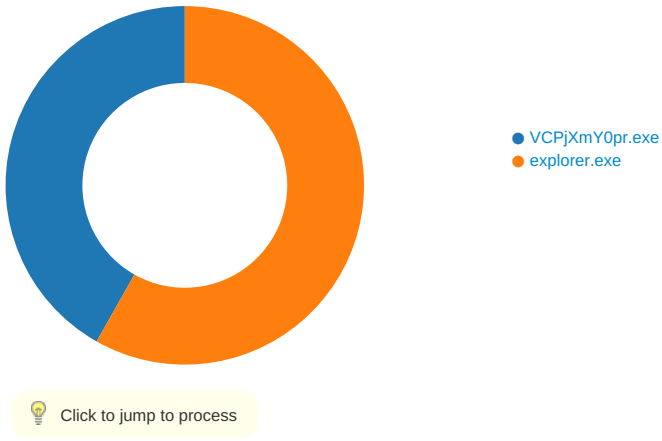
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: VCPjXmY0pr.exe PID: 4792 Parent PID: 6024

General

Start time:	03:09:41
Start date:	14/01/2021
Path:	C:\Users\user\Desktop\VCPjXmY0pr.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\VCPjXmY0pr.exe'
Imagebase:	0x9b0000
File size:	441344 bytes
MD5 hash:	053DDB3B6E38F9BDBC5FB51FDD44D3AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA950E8527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA950E8527	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA950E8527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA950E8527	unknown
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA952A8147	CreateDirectoryW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA952A8147	CreateDirectoryW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839D84BA13E	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839D871C6B0	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839DB822E39	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\7092ee1bf1e386348e9ed2a7b68b7ab2.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E1CB7D93	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\VCPjXmY0pr.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA95436184	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839D84BA13E	unknown	112	2f 45 d8 02 97 24 84 8d b5 ee 39 42 be ca 99 e8 01 d9 6b 84 55 81 4a 18 9b 11 1d 14 4d 37 62 d2 39 dc 89 0a 73 8d bf 27 0d 07 74 7b c9 ab 5e 41 f9 c1 4a ff d7 7d 4b db 0d 9a 63 94 bf 78 c5 e5 b5 00 dc f4 c3 e2 2d 9e 98 24 35 0f bd cf d4 cd 43 5e c4 17 ce 1d 0d ad 74 ff 41 25 a0 d4 78 2d e7 16 a4 f6 88 45 60 e5 e3 4b b2 ef 2c c2 3f 92	/E...$....9B......k.U.J.....M7b.9...s..'..t{..^A..J..}K...c..x........-..$5.....C^......t.A%..x-.....E`..K..,.?.	success or wait	1	7FFA952A8147	WriteFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839D871C6B0	unknown	112	73 f8 e6 2b d7 40 f5 ee 61 d5 eb a5 be ec 7f 9c 5c a0 5b 3d 8e f3 77 09 f3 d0 01 92 a9 a9 18 fd 6e f9 84 af e9 32 87 9d 8a d0 69 c4 22 28 be af dd 46 ec b6 eb f6 77 cb 86 3a 20 5d cb d6 f2 ef a7 23 f6 91 d2 26 2b b7 31 10 a0 34 c9 a3 de b6 59 36 a6 c7 92 86 2b 30 4e 5b b6 6f 40 bd b2 a5 36 19 cb f5 70 da 7a bf d3 a8 e1 b3 e6 49 bd 07	s..+.@..a.......\.[=..w.........n....2....i."(...F....w..:].....#...&+.1..4....Y6....+0N[.o@...6...p.z......I..	success or wait	1	7FFA952A8147	WriteFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839DB822E39	unknown	48	6a be c8 b9 8a 02 ba 8b ae 26 84 f3 89 5a 2f 1f 0a 7c dd 88 21 74 be 72 19 92 5d 00 26 4b 42 6d ef e1 97 1e 22 e7 11 77 a1 d6 0e 6a 14 fb 5c 8d	j........&...Z/..|..!t.r..].&KBm...."..w...j..\.	success or wait	1	7FFA952A8147	WriteFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\7092ee1bf1e386348e9ed2a7b68b7ab2.dll	unknown	8704	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 86 07 00 46 9f b9 56 00 00 00 00 00 00 00 00 f0 00 2e 22 0b 02 02 19 00 14 00 00 00 1c 00 00 00 00 00 00 c4 30 00 00 00 10 00 00 00 00 48 62 00 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 90 00 00 00 04 00 00 09 c8 00 00 03 00 00 00 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..d...F..V...........".................0........Hb...	success or wait	1	7FFA952A8147	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E1CB7D93	unknown	112	33 2c cf bc 76 6e 36 4c ca 15 e7 67 83 e2 9f 2b 03 a7 f6 31 96 d1 e6 e1 8d 5a ef 2e f4 95 6a 59 1a 0c 3a 23 7b 2a 09 0c e4 94 09 74 c5 b1 75 74 8d d3 ff 89 d7 2d 0c d3 29 44 58 5f cc 95 45 27 c7 f4 e1 be d3 1d b0 6e 7c f2 45 ce b2 34 f0 53 ae bd b5 51 64 85 fd b3 a0 52 18 3b b0 5a 18 56 81 01 69 13 96 f1 24 8d 43 d0 e0 e6 4a 7f a8 d1	3,..vn6L...g...+...1.....Z....jY..:#{*.....t..ut.....-..)DX_..E'.......n|.E..4.S...Qd....R.;.Z.V..i...$.C...J...	success or wait	1	7FFA952A8147	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\VCPjXmY0pr.exe.log	unknown	799	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 36 34 5c 53 79 73 74 65 6d 5c 31 32 30 31 66 32 36 63 62 39 38 36 63 39 33 66 35 35 30 34 34 62 62 34 66 61 32 32 62 32 39 34 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 36 34 5c 53 79 73 74 65 6d 2e 53 65 72 76 69 63 65 50 72 6f 63 65 23 5c 35 65 39 31 62 38 38 61 63 30 32 35 35 38 39 34 63 34 65 30 32 34 38 62 31 34 66 63 34 36 34 39 5c 53 79 73 74 65 6d 2e 53 65 72 76 69 63 65 50 72 6f 63 65 73 73 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System\1201f26cb986c93f55044bb4fa22b294\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.ServiceProce#\5e91b88ac0255894c4e0248b14fc4649\System.ServiceProcess.n	success or wait	1	7FFA954361CE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFA95115C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FFA95115C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFA95235AF3	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFA95115C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	7FFA95115C7C	unknown

Analysis Process: explorer.exe PID: 3424 Parent PID: 4792

General

Start time:	03:09:51
Start date:	14/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA950E8527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA950E8527	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA950E8527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA950E8527	unknown
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\c34b132bff0230a28757d24f730ae477	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA952A8147	CreateDirectoryW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E2B523CD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\c34b132bff0230a28757d24f730ae477\b96aff2c7cf2b4afd20609e7a7ab021c	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E2E27076	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E3016F16	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\c34b132bff0230a28757d24f730ae477\aa898d6f9ffba4432ce9bb2a8b2154f7	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f380f48483b8b97877915a9f677dafb7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA952A8147	CreateDirectoryW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\8c3548dc7fceab9ef287458b1a7aff78	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA952A8147	CreateDirectoryW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E60385D2	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\c34b132bff0230a28757d24f730ae477\aace0a8af5e9a62f21d9da31e5909f00	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA952A8147	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\9d e699449c084cfcaf7aae165ca409d7 \f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E2B523CD	unknown	240	1d 69 88 51 b0 e0 8a 34 55 9e de 81 bc 8f c3 c3 f6 21 c1 af 5f 0f c3 16 ec 7b af 01 12 35 ce 70 1e a5 8e ef e6 a3 ee ad e2 08 36 26 c5 54 40 45 45 94 27 4d bd 81 4f b3 2c ef bc 66 20 3c 5f 83 ba f3 b2 60 ab 36 3c 90 43 52 f4 8e 59 f6 1a e7 d1 69 43 e7 2c 4b 7c a6 ec ac d9 a3 04 77 ad 9e 01 29 17 2f cf b3 e6 52 6d 37 b9 ab 0b 5c 35 43 12 bc 28 f0 fd 5a b9 0d 86 2f c2 09 25 e7 2c 3c a1 ef 8b 37 e8 46 b6 f8 bf 95 8e e1 ab e7 bd 18 17 44 9b b2 f1 41 08 c3 49 29 91 6c bc 8e 19 ec 73 92 fe 79 55 e8 49 49 92 ca 30 3d 5a 96 90 60 12 f3 29 59 5c 6d d8 6e f3 d8 1c a1 81 ec cc cd da 12 64 2b 19 a7 ce e3 bf e7 18 24 e3 7d db b6 e9 ac 83 fa df 52 f5 90 74 9b 65 95 4a 22 fd b2 89 db ee 74 4c b5 ef 70 27 69 bb 64 26 f2 2e f6	.i.Q...4U.....!._....{...5 .p.....6&.T@EE.'M..O.,.. f <_....`.6<.CR..Y....iC.,K|... ...w...)./...Rm7...\5C..(..Z.. ./..%.,<...7.F.....D...A ..I).l....s..yU.II..0=Z..`..)Y \m.n.....d+.....$.}.... ...R..t.e.J".....tL..p'i.d&...	success or wait	1	7FFA952A8147	WriteFile
C:\Users\user\AppData\Local\9d e699449c084cfcaf7aae165ca409d7 \c34b132bff0230a28757d24f730ae 477\b96aff2c7cf2b4afd20609e7a7ab021c	unknown	80	c5 f1 ef f7 1f 5b b5 6f da bf 45 f1 96 7e e3 43 05 2b 7a 40 d8 20 82 ff 92 34 96 51 05 98 b8 12 8f de 91 c2 e7 c4 52 b2 ec 95 bc 67 52 e6 47 6b 7c c5 c8 7d 5c 14 e2 4d 5f 39 41 26 bf 07 b5 24 05 f5 c2 01 96 5b 8d 75 51 5f 60 68 b8 45 85 05	.....[.o..E..~.C.+z@. ...4.Q.. .....R....gR.Gk|..}\..M_9A &...$.....[.uQ_`h.E..	success or wait	1	7FFA952A8147	WriteFile
C:\Users\user\AppData\Local\9d e699449c084cfcaf7aae165ca409d7 \f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E2E27076	unknown	112	91 77 ce e0 2c 0f e1 5c f8 fe 60 ff 1d 45 53 e4 4d f0 a8 bf a1 50 78 c9 52 30 b6 f1 56 95 6d 26 f2 25 7c 56 f3 f6 e4 33 53 5a 61 a3 ce bb f5 2f 8f 0e e5 cc b5 ef 5b ac 77 4e 42 61 7d 3d e2 c1 fa 2c 23 f5 f2 69 de c0 92 be 9b b1 6c 0c 8a ee d5 0c 6a 78 f6 17 57 fe 0a 52 1b 75 11 fd 7a 07 e9 f6 4a ba ec 28 26 b6 4f c4 b8 3d 7a fb 0e 68	.w..,..\..`..ES.M....Px.R0..V. m&.%|V...3SZa..../..... [.wNBa }=...,#..i.....l.....jx..W..R .u..z...J..(&.O..=z..h	success or wait	1	7FFA952A8147	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E3016F16	unknown	240	44 23 ea 9b 25 d0 fc b4 04 10 39 34 38 c9 ab 91 ab 94 b2 91 eb 19 4f d0 a3 47 89 09 71 49 54 ab f4 4f 8b f7 d4 40 1a 5d 51 1d 8c 7c b1 0d 60 1c ec 7f f0 06 91 ee 38 49 27 ae 4f 82 c5 1f 1a ec 3a 37 a1 4b 85 d3 39 8b 83 d9 30 d6 8a 3b b9 c0 b1 c0 7c 57 e2 df 66 64 a8 c9 61 f9 fb 66 c1 46 8c 12 13 19 ee 0a ff 68 38 3e b4 4e af a0 cb 4a c3 e5 33 d7 f5 26 b7 b6 ce d3 88 18 59 48 4c 95 36 d9 e8 34 d7 88 95 0c 57 b6 7e 78 7a fd be 13 b6 89 9a 16 ad cc 50 e9 09 3a e0 33 4a bf aa da 48 4f f3 be 72 9c 9b 0a ac 1a ad 15 df 28 79 ec bb b7 a6 d3 09 cb 71 ee 13 5e da f5 d8 d0 e3 06 18 37 7a 62 40 e7 a9 b5 31 da 10 53 37 d9 3c 3d 63 fa 4a 01 36 2c ba 80 5c d2 5f 18 a5 af 0a c1 02 3b 18 2a d0 62 0b ad 31 a7 b4 f7 94 2e 64 6b	D#..%.....948.....O..G..qlT..O...@.]Q..|..`.....8I'.O.....:7.K..9...0..;....|W..fd..a..f.F.....h8>.N...J..3..&......YHL.6..4....W.~xz.....P..:.3J...HO..r.....(y.....q..^.....7zb@...1..S7.<=c.J.6,..\._.....;.*.b..1.....dk	success or wait	1	7FFA952A8147	WriteFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\c34b132bff0230a28757d24f730ae477\aa898d6f9ffba4432ce9bb2a8b2154f7	unknown	16	23 77 df a2 e9 a2 b7 0c 4b 3a 32 e0 cc 59 bc 0f	#w.....K:2..Y..	success or wait	1	7FFA952A8147	WriteFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\f881b2c16ba8e622f4992b3af2bf31dc\08D8B839E60385D2	unknown	240	8c 62 64 fc b1 57 72 27 5e f9 29 d7 f9 4e 48 41 1d 27 80 d2 79 cd c4 d7 ca 32 ac fa 7f 0c 49 62 aa fc a1 0f 6e 19 43 2a 19 f3 06 44 d7 32 f1 31 6e 33 24 04 f3 70 79 42 05 91 3a 06 d8 62 de 6a a5 2f 9c b4 51 2c 2a e5 38 2a 79 79 3c fd f4 75 1e bd 20 be 10 2d ec fe ab d1 65 d0 f8 eb 67 4e f4 85 8b 1b 2d 23 23 7d 29 6a 01 b3 d4 f2 82 f4 98 fb 74 40 bf 7d ce 22 4c 61 ed 57 9a 2f d8 10 27 64 7d d2 30 00 a4 a9 3f aa df bc c4 1b 51 66 1e e2 81 1b 0c 1e 83 d0 a5 a5 5d d1 9a 07 68 7a e8 64 51 6f f2 e0 79 5d 92 70 4a 8d d8 ee bc 81 e6 cc 53 b9 83 a0 dd 4b 4e ff 1a 83 1c 4a 98 10 5b bf 09 8e b2 e5 3d 46 e1 66 7e 45 8c 70 50 1b 69 8b 0e b7 4c d2 27 54 5a ff 97 73 78 17 b0 c0 76 7f 02 fc 85 bb 0a 25 98 7e 23 8c c9 04 bd 24	.bd..Wr'^.)..NHA.'..y....2....Ib....n.C*...D.2.1n3$..pyB..:..b.j./..Q,*.8*yy<..u.. ..-....e...gN....-##}}j.....t@.}."La.W./..'d}.0...?.....Qf.....]...hz.dQo..y].pJ.....S.....KN....J..[.....=F.f~E.pP.i...L.'TZ..sx...v.....%.~#....$	success or wait	1	7FFA952A8147	WriteFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7\c34b132bff0230a28757d24f730ae477\aace0a8af5e9a62f21d9da31e5909f00	unknown	16	c4 92 43 37 c4 87 fe 01 9e 18 75 ba 69 8b e3 03	..C7.....u.i...	success or wait	1	7FFA952A8147	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFA95115C7C	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FFA95115C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFA95235AF3	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFA95115C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	7FFA95115C7C	unknown
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7 \c34b132bff0230a28757d24f730ae477\aa898d6f9ffba4432ce9bb2a8b2154f7	unknown	4096	success or wait	42	7FFA952A8147	ReadFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7 \c34b132bff0230a28757d24f730ae477\aa898d6f9ffba4432ce9bb2a8b2154f7	unknown	4096	end of file	51	7FFA952A8147	ReadFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7 \c34b132bff0230a28757d24f730ae477\b96aff2c7cf2b4afd20609e7a7ab021c	unknown	4096	success or wait	1093	7FFA952A8147	ReadFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7 \c34b132bff0230a28757d24f730ae477\b96aff2c7cf2b4afd20609e7a7ab021c	unknown	4096	end of file	1092	7FFA952A8147	ReadFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7 \c34b132bff0230a28757d24f730ae477\aace0a8af5e9a62f21d9da31e5909f00	unknown	4096	success or wait	26	7FFA952A8147	ReadFile
C:\Users\user\AppData\Local\9de699449c084cfcaf7aae165ca409d7 \c34b132bff0230a28757d24f730ae477\aace0a8af5e9a62f21d9da31e5909f00	unknown	4096	end of file	28	7FFA952A8147	ReadFile

Disassembly

Code Analysis