ID: 490261
Sample Name:
vXVHRRGG7c.exe
Cookbook: default.jbs
Time: 10:22:00
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report vXVHRRGG7c.exe

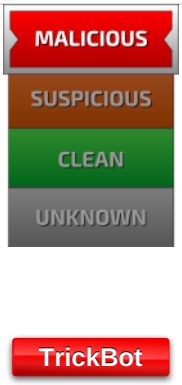
Overview

General Information

Sample Name:	vXVHRRGG7c.exe
Analysis ID:	490261
MD5:	051c20fd814ac34..
SHA1:	6d4d301594ba01..
SHA256:	7aa215495949e7..
Tags:	exe TrickBot
Infos:	

Most interesting Screenshot:

Detection

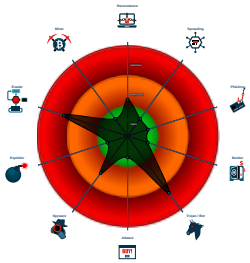


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Yara detected Trickbot
- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for dropp…
- Writes to foreign memory regions
- Allocates memory in foreign process…
- May check the online IP address of …
- Found evasive API chain (trying to d…
- Tries to detect virtualization through…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- vXVHRRGG7c.exe (PID: 3028 cmdline: 'C:\Users\user\Desktop\vXVHRRGG7c.exe' MD5: 051C20FD814AC34FFCFADD56EC872BE0)
  - wermgr.exe (PID: 2944 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
  - cmd.exe (PID: 4404 cmdline: C:\Windows\system32\cmd.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- cmd.exe (PID: 720 cmdline: C:\Windows\SYSTEM32\cmd.exe /c 'C:\Users\user\AppData\Local\browDownload3D\cmd01.bat' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vXVHRRGG7c.exe (PID: 1140 cmdline: C:\Users\user\AppData\Local\browDownload3D\vXVHRRGG7c.exe MD5: 051C20FD814AC34FFCFADD56EC872BE0)
    - wermgr.exe (PID: 760 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
    - cmd.exe (PID: 3560 cmdline: C:\Windows\system32\cmd.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- **cleanup**

Malware Configuration

Threatname: Trickbot

```
{
  "ver": "2000033",
  "gtag": "tot153",
  "servs": [
    "179.42.137.102:443",
    "191.36.152.198:443",
    "179.42.137.104:443",
    "179.42.137.106:443",
    "179.42.137.108:443",
    "202.183.12.124:443",
    "194.190.18.122:443",
    "103.56.207.230:443",
    "171.103.187.218:443",
    "171.103.189.118:443",
    "18.139.111.104:443",
    "179.42.137.105:443",
    "186.4.193.75:443",
    "171.101.229.2:443",
    "179.42.137.107:443",
    "103.56.43.209:443",
    "179.42.137.110:443",
    "45.181.207.156:443",
    "197.44.54.162:443",
    "179.42.137.109:443",
    "103.59.105.226:443",
    "45.181.207.101:443",
    "117.196.236.205:443",
    "72.224.45.102:443",
    "179.42.137.111:443",
    "96.47.239.181:443",
    "171.100.112.190:443",
    "117.196.239.6:443"
  ],
  "autorun": [
    "pwgrabb",
    "pwgrabc"
  ],
  "ecc_key": "RUNTMzAAAAAL/ZqmMPBLaRfg1hPOtFJrZz2Zi2/EC4B3fiX8VnaOUVKndBr+jEqWc7mw4v3ADTiwp64K5QKe1LZ27jUZxL4bWjxARPo85hv72nuedeZhRQ+adQQ/gIsV869MycRzghc="
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.400799901.0000000000FF4000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
0000000A.00000002.400763097.0000000000FB0000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000001.00000002.304517846.0000000002464000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
0000000A.00000002.400850600.0000000001261000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000001.00000002.304704482.00000000024A1000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.vXVHRRGG7c.exe.24a0000.3.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
10.2.vXVHRRGG7c.exe.1260000.3.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
1.2.vXVHRRGG7c.exe.23e052e.1.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
10.2.vXVHRRGG7c.exe.fb052e.2.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
1.2.vXVHRRGG7c.exe.23e052e.1.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Click to see the 1 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

May check the online IP address of the machine

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Stealing of Sensitive Information:

Yara detected Trickbot

Remote Access Functionality:

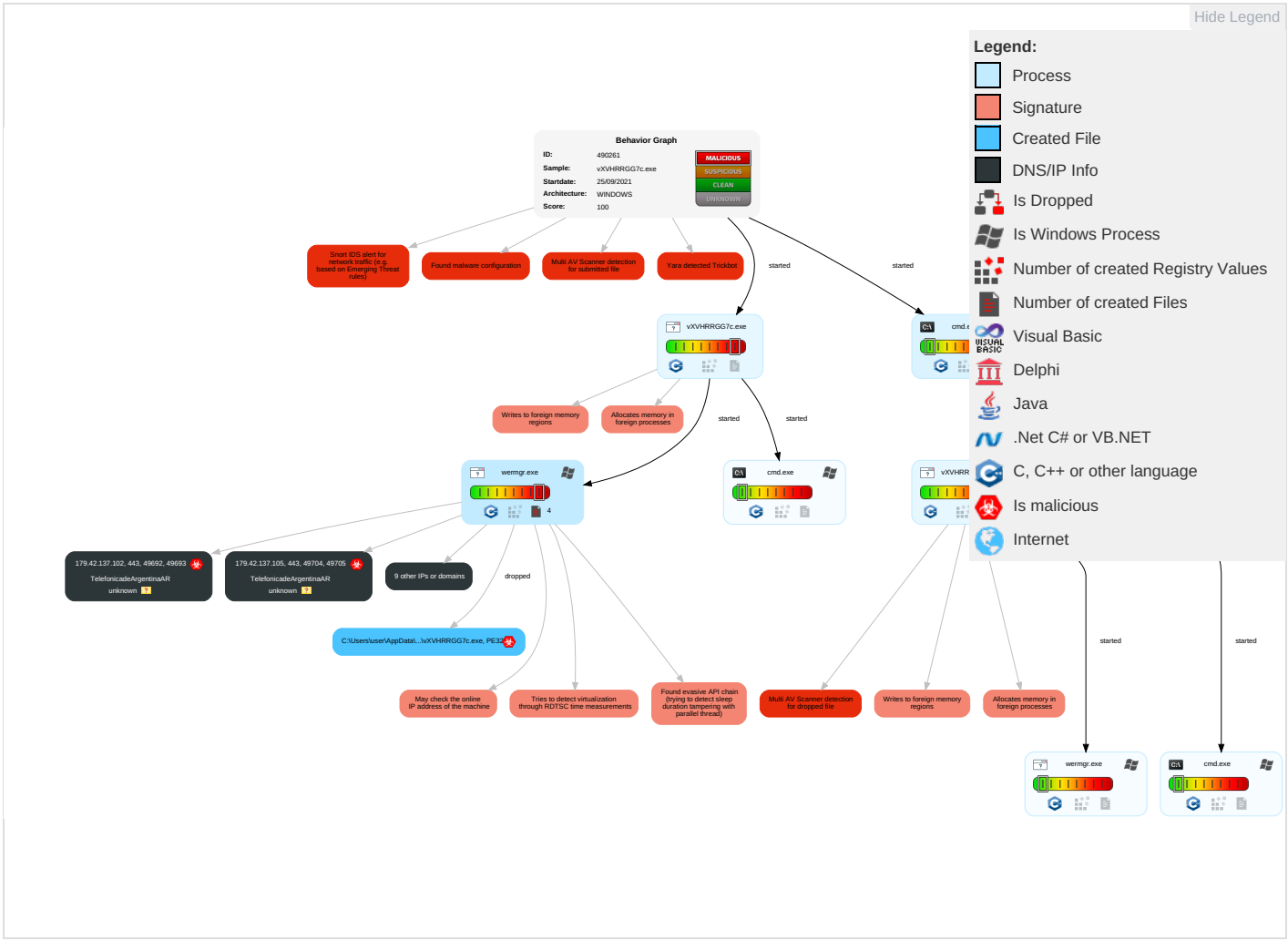
Yara detected Trickbot

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	Scripting 1	Application Shimming 1	Process Injection 2 1 1	Masquerading 1	Input Capture 2	System Time Discovery 2	Remote Services	Input Capture 2	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communica
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Application Shimming 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 3	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 2 4	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Statio

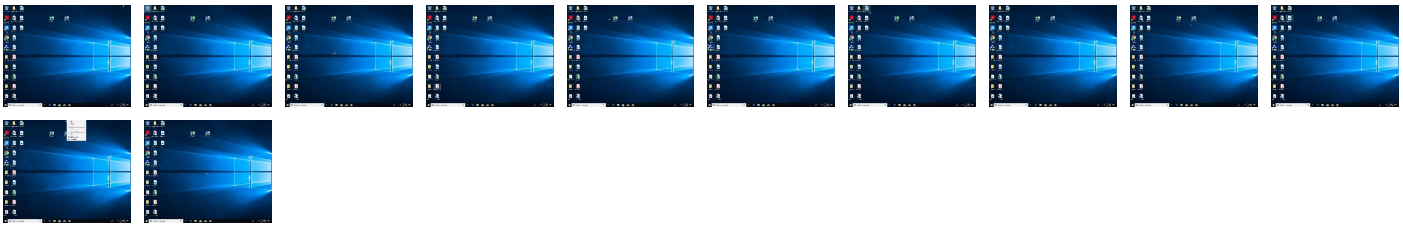
Behavior Graph



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
vXVHRRGG7c.exe	22%	ReversingLabs	Win32.Trojan.TrickBot	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\browDownload3D\vXVHRRGG7c.exe	22%	ReversingLabs	Win32.Trojan.TrickBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.vXVHRRGG7c.exe.23e052e.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.vXVHRRGG7c.exe.24a0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.vXVHRRGG7c.exe.1260000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.vXVHRRGG7c.exe.fb052e.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
icanhazip.com	104.18.7.156	true	false		high
9.52.17.84.dnsbl-1.uceprotect.net	unknown	unknown	false		unknown
9.52.17.84.zen.spamhaus.org	unknown	unknown	false		high
9.52.17.84.cbl.abuseat.org	unknown	unknown	false		high
9.52.17.84.b.barracudacentral.org	unknown	unknown	false		high
9.52.17.84.spam.dnsbl.sorbs.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://icanhazip.com/	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
179.42.137.102	unknown	unknown		22927	TelefonicadeArgentinaAR	true
104.18.7.156	icanhazip.com	United States		13335	CLOUDFLARENETUS	false
179.42.137.105	unknown	unknown		22927	TelefonicadeArgentinaAR	true
59.4.68.75	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
171.103.189.118	unknown	Thailand		7470	TRUEINTERNET-AS-APTRUEINTERNETCoLtdTH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490261
Start date:	25.09.2021
Start time:	10:22:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 54s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	vXVHRRGG7c.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:	17
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.troj.evad.winEXE@13/3@6/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 63.1% (good quality ratio 61.3%) • Quality average: 84.9% • Quality standard deviation: 24%
HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:23:01	API Interceptor	22x Sleep call for process: wermgr.exe modified
10:23:38	Task Scheduler	Run new task: Browser Downloader for Windows3D path: C:\Users\user\AppData\Local\browDownload3D\cmd0 1.bat

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
179.42.137.102	triage_dropped_file.dll	Get hash	malicious	Browse	
104.18.7.156	EZOHPAvupB.exe	Get hash	malicious	Browse	• icanhazip.com/
	rOz6omkS6Wba5EJ.exe	Get hash	malicious	Browse	• icanhazip.com/
	pCdWi9AqhY.exe	Get hash	malicious	Browse	• icanhazip.com/
	GP7V5TKo7I0VmTQ.exe	Get hash	malicious	Browse	• icanhazip.com/
	Bank Details.exe	Get hash	malicious	Browse	• icanhazip.com/
	TtkRZtP1Jq.exe	Get hash	malicious	Browse	• icanhazip.com/
	Bank Details.docx	Get hash	malicious	Browse	• icanhazip.com/
	aZq3gco8Ab.exe	Get hash	malicious	Browse	• icanhazip.com/
	wuH92YGkZk.exe	Get hash	malicious	Browse	• icanhazip.com/
	3VFWIsGexy.exe	Get hash	malicious	Browse	• icanhazip.com/
	tB94D01Kyl.exe	Get hash	malicious	Browse	• icanhazip.com/
	v4oeJd6Cqv.exe	Get hash	malicious	Browse	• icanhazip.com/
	GC6Vdq1xoX.exe	Get hash	malicious	Browse	• icanhazip.com/
	QTL_000027401622208.exe	Get hash	malicious	Browse	• icanhazip.com/
	3RQvR8bIfa.exe	Get hash	malicious	Browse	• icanhazip.com/
	IMG_8035002078801.doc	Get hash	malicious	Browse	• icanhazip.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9BbTEjaJ8m.exe	Get hash	malicious	Browse	• icanhazip.com/
	9088890000.exe	Get hash	malicious	Browse	• icanhazip.com/
	A742.exe	Get hash	malicious	Browse	• icanhazip.com/
	EDL_0412000145200.exe	Get hash	malicious	Browse	• icanhazip.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
icanhazip.com	EZOHPAvupB.exe	Get hash	malicious	Browse	• 104.18.7.156
	Product_Specifications_Details_202330_RFQ.docx.docx	Get hash	malicious	Browse	• 104.18.7.156
	rOz6omkS6Wba5EJ.exe	Get hash	malicious	Browse	• 104.18.7.156
	jHEJ28U6Aj.exe	Get hash	malicious	Browse	• 104.18.6.156
	pCdWi9AqhY.exe	Get hash	malicious	Browse	• 104.18.7.156
	GP7V5TKo7I0VmTQ.exe	Get hash	malicious	Browse	• 104.18.7.156
	Bank Details.exe	Get hash	malicious	Browse	• 104.18.7.156
	TtkRZtP1Jq.exe	Get hash	malicious	Browse	• 104.18.7.156
	uP8CYt2gvb.exe	Get hash	malicious	Browse	• 104.18.6.156
	nKHk75RJEi.exe	Get hash	malicious	Browse	• 104.18.6.156
	Bank Details.docx	Get hash	malicious	Browse	• 104.18.7.156
	aZq3gco8Ab.exe	Get hash	malicious	Browse	• 104.18.7.156
	DsGo26G94d.exe	Get hash	malicious	Browse	• 104.18.6.156
	wuH92YGkZk.exe	Get hash	malicious	Browse	• 104.18.7.156
	3VFWIsGexy.exe	Get hash	malicious	Browse	• 104.18.7.156
	tB94D01Kyl.exe	Get hash	malicious	Browse	• 104.18.7.156
	v4oeJd6Cqv.exe	Get hash	malicious	Browse	• 104.18.7.156
	GC6Vdq1xoX.exe	Get hash	malicious	Browse	• 104.18.6.156
	QTL_000027401622208.exe	Get hash	malicious	Browse	• 104.18.7.156
	z5WnxHv7bg.exe	Get hash	malicious	Browse	• 104.18.6.156

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	KqXA36ARxD.exe	Get hash	malicious	Browse	• 104.21.95.21
	p7jfy1lZgl.exe	Get hash	malicious	Browse	• 172.67.169.45
	RgproFrlyA.exe	Get hash	malicious	Browse	• 172.67.212.186
	qUaCp2QNnD.exe	Get hash	malicious	Browse	• 162.159.130.233
	XMae11M5yg	Get hash	malicious	Browse	• 172.69.163.248
	D4DCAA41641BD14406B3FA2A1CEE1E97DE93329B9F901.exe	Get hash	malicious	Browse	• 104.21.41.75
	bfHSvjklSW	Get hash	malicious	Browse	• 198.41.197.73
	Dkvunfebdprvvugtyhevcozxmecjaaclna.exe	Get hash	malicious	Browse	• 162.159.133.233
	Dkvunfebdprvvugtyhevcozxmecjaaclna.exe	Get hash	malicious	Browse	• 162.159.134.233
	Hilix.x86	Get hash	malicious	Browse	• 104.29.243.68
	Silver_Light_Group_DOC030273211220213.exe	Get hash	malicious	Browse	• 162.159.135.233
	18vaq1Ah2l	Get hash	malicious	Browse	• 104.31.160.209
	IC-230921 135838 ggo.htm	Get hash	malicious	Browse	• 104.16.19.94
	3LNSjXtdQS.exe	Get hash	malicious	Browse	• 172.67.162.27
	COURT-ORDER#S12GF803_zip.exe	Get hash	malicious	Browse	• 23.227.38.74
	4qwvsVLRyN.exe	Get hash	malicious	Browse	• 162.159.133.233
	Minehack3.1.exe	Get hash	malicious	Browse	• 162.159.129.233
	DHL 03845435654.pdf.exe	Get hash	malicious	Browse	• 162.159.135.233
	DHL Awb_ Docs 5544834610_pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	file.exe	Get hash	malicious	Browse	• 104.21.47.211
TelefonicadeArgentinaAR	vLaqS0RiE0.exe	Get hash	malicious	Browse	• 179.42.137.110
	ndx4U5fTTa	Get hash	malicious	Browse	• 181.20.78.210
	rW182CWZHv	Get hash	malicious	Browse	• 201.181.242.170
	XMae11M5yg	Get hash	malicious	Browse	• 179.41.145.204
	LkypMws5yh	Get hash	malicious	Browse	• 181.21.231.163
	ztXN1Pfp4G.exe	Get hash	malicious	Browse	• 179.42.137.109

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	shinto.x86	Get hash	malicious	Browse	• 179.42.3.58
	EZOHPAvupB.exe	Get hash	malicious	Browse	• 179.42.137.107
	ydUqlLF7lK.exe	Get hash	malicious	Browse	• 179.42.137.108
	ydUqlLF7lK.exe	Get hash	malicious	Browse	• 179.42.137.107
	52uSca10l1.exe	Get hash	malicious	Browse	• 179.42.137.106
	GVlpP9RL5t	Get hash	malicious	Browse	• 186.132.129.176
	jKira.x86	Get hash	malicious	Browse	• 190.176.115.106
	jKira.arm	Get hash	malicious	Browse	• 190.176.94.237
	mirai.arm	Get hash	malicious	Browse	• 190.175.168.186
	XyMjGu74RX	Get hash	malicious	Browse	• 186.63.134.210
	b3astmode.x86	Get hash	malicious	Browse	• 190.48.196.82
	b3astmode.arm7	Get hash	malicious	Browse	• 186.131.140.192
	b3astmode.arm	Get hash	malicious	Browse	• 190.175.143.215
	ii1tf3xFJ1	Get hash	malicious	Browse	• 179.42.113.208

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\browDownload3D\cmd01.bat	
Process:	C:\Windows\System32\wermgr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1204
Entropy (8bit):	4.291933112891695
Encrypted:	false
SSDEEP:	24:aEAlQS4pfPEwdw2FXipgMzD/97G3E4tV/+tBaBy:0l4pf8xIXiT9oE4t5YBl
MD5:	D2B6BA2379B3DBCC6F757D92D20C3E47
SHA1:	6584EB2FFC0C3308021BF6BE7C395DC8D22F0A4C
SHA-256:	09D14E5C54A44526E36E78A9BD97A5BD4F460578523DF6B824D160EB188BA781
SHA-512:	ABA8AFCE4DCF0DDC0CE07B57F521063747B38F3BC7692A020DD10E227D12286B1701ACB45CD91397DF79FFB56E34D0885D0902968C4ECADDF013D21BF8AA58E
Malicious:	false
Reputation:	low
Preview:	set irml=set..%irml% epceq= ..%irml%%epceq%epiva==..%irml%%epceq%qvnl%epiva%own..%irml%%epceq%frvp%epiva%r..%irml%%epceq%uovekb%epiva%c..%irml%%epceq%ubixnl%epiva%exe..%irml%%epceq%kumkbx%epiva%HRR..%irml%%epceq%dppcdc%epiva%tar..%irml%%epceq%dnuqid%epiva%d3..%irml%%epceq%pvjhbj%epiva%Loc..%irml%%epceq%uodh%epiva%C..%irml%%epceq%luafbs%epiva%\..%irml%%epceq%ktgdh%epiva%rd..%irml%%epceq%gvsjad%epiva%z..%irml%%epceq%fylvab%epiva%owD..%irml%%epceq%socvxl%epiva%D..%irml%%epceq%qqwrtb%epiva%b..%irml%%epceq%aaymq%epiva%G7..%irml%%epceq%lshlj%epiva%p..%irml%%epceq%obec%epiva%Us..%irml%%epceq%qhsete%epiva%ata..%irml%%epceq%kekdbx%epiva%Ap..%irml%%epceq%vsem%epiva%loa..%irml%%epceq%drtmim%epiva%s..%irml%%epceq%cfjl%epiva%:..%irml%%epceq%ehhp%epiva%ha..%irml%%epceq%kplf%epiva%ers..%irml%%epceq%xfjrim%epiva%vXV..%irml%%epceq%abosow%epiva%G..%irml%%epceq%poiosr%epiva%...%irml%%epceq%lbqmm%epiva%t..%irml%%epceq%ixmxcv%epiva%al..%drtmim%%dppcdc%%lbqmm%%epceq%%uodh%%cfjl%%luafbs%%obec%%kplf%%luafbs%%

C:\Users\user\AppData\Local\browDownload3D\settings.ini	
Process:	C:\Windows\System32\wermgr.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	10233
Entropy (8bit):	5.10582120432788
Encrypted:	false
SSDEEP:	192:DdBYKtc+6GXBMGHbQNw5vfbG6RCFUzBT6N0HDFeCKE4M:DdBYCVQhGzd6ujrKLM
MD5:	5775E804AA3B7F597C3D9429B8A5B28C
SHA1:	807E2E18366E0F4E7891A21475303B02D28F6901
SHA-256:	DA06E0B6863552469522446B05BFA91AFB9A7F683CE44C83B849D3EDC355E08D

C:\Users\user\AppData\Local\browDownload3D\settings.ini	
SHA-512:	7CE3D1697DD723EE28F38F9625AF1DD0BC72C51F7D71F801CC8C7701C82B856497DD6F660ED80D5D616C0C6667113EA5E3A764ED1423CE027FFA6ED79CA678 7
Malicious:	false
Reputation:	low
Preview:	[seqygcmamoqsag]..yomyuog=s ww pysii..okowickwwwe=fs cmc gs cywek..hyysmcocy mmg=ggk wysw qqekwcsk o uuam nsyw ogu fo aqeeuk mm ywyiy yuecu iocuks g ii..nouseai=sy ugeq gqcskig caqqi nsosai o vi maec p iyc wq..icsakqqowwecg=eg sy i qou s cuou coaim aiysys b ..cc =kauacsg eg sgsm xe o qg a..ti =sw wmga uuc c pwueie wacqwi wmcyeuy qkegmsg a giu iycu bwkcug ymc eam..mauqc=ikkwys cogsw sowmi ck gaysc yu iomq dca kgakqw wo oy wq cqmw i puamk gy..cyik c=pwamueus cmqawo aw..[bgkocw]..scskmssykcm=o rsaim sgkkim siokcuo s lgwgk kggq l l ck eouug yq ws kq yo y..ieska=kukgkose..gec oiays puu=scaoi hk f yse sg w ogiyso yo..oa vkskke=ycsi qa vkyg ss as pi kkmewyua yakaeko..uugceqm msg=dcu dayi sou w jkc p ikqqkiic ykksq o cukqey auikk geasio..l w=ragema xygmceq uwo wqiwy kui ie fue oqa yuwa t..oei=humyeqso..mugc v f =pu cymw ysysmq ui k ko woe aey oamwe a oogekusk ecgccu aewwsy..mcycsyi=fecguu..kkoses roye=ekgiio a bsusa oy yk cwa im wuwi..cwouuicgu=qkgymggy..josicqw=aswwiu ick qw

C:\Users\user\AppData\Local\browDownload3D\vXVHRRGG7c.exe	
Process:	C:\Windows\System32\wermgr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	528443
Entropy (8bit):	7.022615303042581
Encrypted:	false
SSDEEP:	12288:cbVMh0tRyr3W3SZniM+uwkMx8nXoTT0WJZmo:WMh0tRy53lY8X2xJZmo
MD5:	051C20FD814AC34FFCFADD56EC872BE0
SHA1:	6D4D301594BA01B9E4D8EAC59DC839090F090FDF
SHA-256:	7AA215495949E721B9AE8B3B28CB728AC3B3240438E67F2CC4F3BE2711D3D319
SHA-512:	9A0F400CED3CEA1B366862AB4DDDE79D8C50D2D93AF5ABF9681207ACD5BD7D9652CCA8F213FA0FE26B7FC78184110256723D47287B8A7AA4E69B8F3CAF7D5 25
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 22%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....yq..."..."..."..."..."..."2..";.."..."P.."..."..."..."P.."..."Rich..."..... .....PE..L...}..`.....`.....W.....p....@.....P.....`.....P.....Pv.....p..L..... .....text....S.....`..... ..`.rdata...y...p.....p.....@..@.data....P..... .....@....rsrc.....P.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.022615303042581
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	vXVHRRGG7c.exe
File size:	528443
MD5:	051c20fd814ac34ffcfadd56ec872be0
SHA1:	6d4d301594ba01b9e4d8eac59dc839090f090fdf
SHA256:	7aa215495949e721b9ae8b3b28cb728ac3b3240438e67f 2cc4f3be2711d3d319
SHA512:	9a0f400ced3cea1b366862ab4ddde79d8c50d2d93af5abf 9681207acd5bd7d9652cca8f213fa0fe26b7fc781841102 56723d47287b8a7aa4e69b8f3caf7d5025
SSDEEP:	12288:cbVMh0tRyr3W3SZniM+uwkMx8nXoTT0WJZmo :WMh0tRy53lY8X2xJZmo
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....yq..."... "..."..."..."..."..."2..";.."..."P.."..."..."..."P.."..."Rich..."..... .....PE..L...}..`.....

File Icon

Icon Hash:	71b018ccc6577131

Static PE Info

General

Entrypoint:	0x4057bd
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x60E4CA7D [Tue Jul 6 21:26:21 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:	675872e23dfc0f62ffbc2f69c316f4bc

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x253a6	0x26000	False	0.545088918586	data	6.48403042151	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x27000	0x79ee	0x8000	False	0.326416015625	data	4.81513775397	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2f000	0x50e8	0x2000	False	0.391357421875	data	4.59613450041	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x35000	0x4f6e8	0x50000	False	0.779440307617	data	7.23576523208	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/25/21-10:23:39.069395	TCP	2404342	ET CNC Feodo Tracker Reported CnC Server TCP group 22	49719	443	192.168.2.3	59.4.68.75

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 25, 2021 10:23:30.876858950 CEST	192.168.2.3	8.8.8.8	0x1704	Standard query (0)	icanhazip.com	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:33.487632036 CEST	192.168.2.3	8.8.8.8	0xc43e	Standard query (0)	9.52.17.84.zen.spamhaus.org	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:33.516525984 CEST	192.168.2.3	8.8.8.8	0xe690	Standard query (0)	9.52.17.84.cbl.abuseat.org	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:33.543143988 CEST	192.168.2.3	8.8.8.8	0x6130	Standard query (0)	9.52.17.84.b.barracudacentral.org	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:33.667074919 CEST	192.168.2.3	8.8.8.8	0xf9a5	Standard query (0)	9.52.17.84.dnsbl-1.uceprotect.net	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:33.693366051 CEST	192.168.2.3	8.8.8.8	0x815f	Standard query (0)	9.52.17.84.spam.dnsbl.sorbs.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 25, 2021 10:23:30.899730921 CEST	8.8.8.8	192.168.2.3	0x1704	No error (0)	icanhazip.com		104.18.7.156	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:30.899730921 CEST	8.8.8.8	192.168.2.3	0x1704	No error (0)	icanhazip.com		104.18.6.156	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:33.513423920 CEST	8.8.8.8	192.168.2.3	0xc43e	Name error (3)	9.52.17.84.zen.spamhaus.org	none	none	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:33.538508892 CEST	8.8.8.8	192.168.2.3	0xe690	Name error (3)	9.52.17.84.cbl.abuseat.org	none	none	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:33.664612055 CEST	8.8.8.8	192.168.2.3	0x6130	Name error (3)	9.52.17.84.b.barracudacentral.org	none	none	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:33.690701962 CEST	8.8.8.8	192.168.2.3	0xf9a5	Name error (3)	9.52.17.84.dnsbl-1.uceprotect.net	none	none	A (IP address)	IN (0x0001)
Sep 25, 2021 10:23:33.735809088 CEST	8.8.8.8	192.168.2.3	0x815f	Name error (3)	9.52.17.84.spam.dnsbl.sorbs.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- icanhazip.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49717	104.18.7.156	80	C:\Windows\System32\wermgr.exe

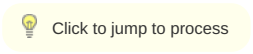
Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:23:30.921077967 CEST	14	OUT	GET / HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.76.0 Host: icanhazip.com

Timestamp	kBytes transferred	Direction	Data
Sep 25, 2021 10:23:30.943857908 CEST	15	IN	HTTP/1.1 200 OK Date: Sat, 25 Sep 2021 08:23:30 GMT Content-Type: text/plain Content-Length: 11 Connection: keep-alive Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET Set-Cookie: __cf_bm=YnuhHc5obdx6JSfdiUyIiKOHJ9bmCLxvJKkUWr0hBbo-1632558210-0-AWnxvEVQ+dgSA 2VpCJroUN0rMjzXW9aG4cCXfqI9Unu9bvJ/EEi8uEXIW0kmM0F8BtJH3m6a4E1nd2TzFl9A4/Q=; path=/; expires=Sat, 25-Sep-21 08:53:30 GMT; domain=.icanhazip.com; HttpOnly; SameSite=None Server: cloudflare CF-RAY: 6942d9d24c454e8b-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 38 34 2e 31 37 2e 35 32 2e 39 0a Data Ascii: 84.17.52.9

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: vXVHRRGG7c.exe PID: 3028 Parent PID: 316

General

Start time:	10:22:54
Start date:	25/09/2021
Path:	C:\Users\user\Desktop\vXVHRRGG7c.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\vXVHRRGG7c.exe'
Imagebase:	0x400000
File size:	528443 bytes
MD5 hash:	051C20FD814AC34FFCFADD56EC872BE0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000001.00000002.304517846.0000000002464000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000001.00000002.304704482.00000000024A1000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000001.00000002.304177777.00000000023E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: wermgr.exe PID: 2944 Parent PID: 3028

General

Start time:	10:22:56
Start date:	25/09/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff7ee4c0000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 4404 Parent PID: 3028

General

Start time:	10:22:57
Start date:	25/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe
Imagebase:	0x7ff6fb440000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 720 Parent PID: 664

General

Start time:	10:23:38
Start date:	25/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SYSTEM32\cmd.exe /c 'C:\Users\user\AppData\Local\browDownload3D\cmd01.bat'
Imagebase:	0x7ff6fb440000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5676 Parent PID: 720

General

Start time:	10:23:39
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vXVHRRGG7c.exe PID: 1140 Parent PID: 720

General

Start time:	10:23:39
Start date:	25/09/2021
Path:	C:\Users\user\AppData\Local\browDownload3D\vXVHRRGG7c.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\browDownload3D\vXVHRRGG7c.exe
Imagebase:	0x400000
File size:	528443 bytes
MD5 hash:	051C20FD814AC34FFCFADD56EC872BE0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 0000000A.00000002.400799901.0000000000FF4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 0000000A.00000002.400763097.0000000000FB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 0000000A.00000002.400850600.0000000001261000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 22%, ReversingLabs
Reputation:	low

Analysis Process: wermgr.exe PID: 760 Parent PID: 1140

General

Start time:	10:23:41
Start date:	25/09/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff7ee4c0000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 3560 Parent PID: 1140

General

Start time:	10:23:42
Start date:	25/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe
Imagebase:	0x7ff6fb440000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis