ID: 458550
Sample Name: 7keerHhHvn.exe
Cookbook: default.jbs
Time: 14:44:19
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

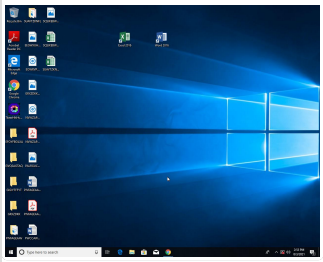
Windows Analysis Report 7keerHhHvn.exe

Overview

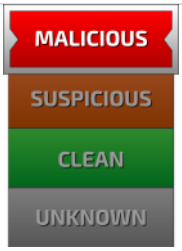
General Information

Sample Name:	7keerHhHvn.exe
Analysis ID:	458550
MD5:	782783574d2d4b..
SHA1:	8eeec0963fa7eaf..
SHA256:	0d2aeb4a2f85b9b.
Tags:	exe Malware
Infos:	

Most interesting Screenshot:



Detection



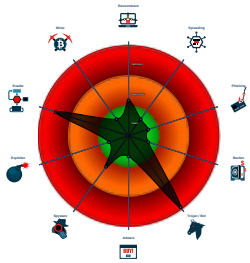
Nanocore GuLoader

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- GuLoader behavior detected
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected GuLoader
- Yara detected Nanocore RAT
- C2 URLs / IPs found in malware con…
- Detected RDTSC dummy instruction…
- Hides that the sample has been dow…
- Hides threads from debuggers
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- 7keerHhHvn.exe (PID: 1056 cmdline: 'C:\Users\user\Desktop\7keerHhHvn.exe' MD5: 782783574D2D4B67666B77B686C2E673)
  - RegAsm.exe (PID: 2476 cmdline: 'C:\Users\user\Desktop\7keerHhHvn.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 3596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- filename1.exe (PID: 2344 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 782783574D2D4B67666B77B686C2E673)
  - RegAsm.exe (PID: 4168 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - RegAsm.exe (PID: 3448 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - RegAsm.exe (PID: 5904 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 4792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- filename1.exe (PID: 5512 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 782783574D2D4B67666B77B686C2E673)
  - RegAsm.exe (PID: 5376 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - RegAsm.exe (PID: 4736 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 5028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "07e10254-b226-4020-a6dd-2e85529c",
  "Group": "FRANCE",
  "Domain1": "mexi11.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 4040,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "",
  "BackupDNSServer": "37.235.1.177"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000029.00000002.780177556.000000001EBB1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000029.00000002.780177556.000000001EBB1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x493f5:$a: NanoCore • 0x4944e:$a: NanoCore • 0x4948b:$a: NanoCore • 0x49504:$a: NanoCore • 0x5cbaf:$a: NanoCore • 0x5cbc4:$a: NanoCore • 0x5cbf9:$a: NanoCore • 0x7567b:$a: NanoCore • 0x75690:$a: NanoCore • 0x756c5:$a: NanoCore • 0x49457:$b: ClientPlugin • 0x49494:$b: ClientPlugin • 0x49d92:$b: ClientPlugin • 0x49d9f:$b: ClientPlugin • 0x5c96b:$b: ClientPlugin • 0x5c986:$b: ClientPlugin • 0x5c9b6:$b: ClientPlugin • 0x5cbcd:$b: ClientPlugin • 0x5cc02:$b: ClientPlugin • 0x75437:$b: ClientPlugin • 0x75452:$b: ClientPlugin
00000026.00000002.767234010.000000001F1D1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000026.00000002.767234010.000000001F1D1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x493f5:$a: NanoCore • 0x4944e:$a: NanoCore • 0x4948b:$a: NanoCore • 0x49504:$a: NanoCore • 0x5cbaf:$a: NanoCore • 0x5cbc4:$a: NanoCore • 0x5cbf9:$a: NanoCore • 0x7567b:$a: NanoCore • 0x75690:$a: NanoCore • 0x756c5:$a: NanoCore • 0x49457:$b: ClientPlugin • 0x49494:$b: ClientPlugin • 0x49d92:$b: ClientPlugin • 0x49d9f:$b: ClientPlugin • 0x5c96b:$b: ClientPlugin • 0x5c986:$b: ClientPlugin • 0x5c9b6:$b: ClientPlugin • 0x5cbcd:$b: ClientPlugin • 0x5cc02:$b: ClientPlugin • 0x75437:$b: ClientPlugin • 0x75452:$b: ClientPlugin
00000029.00000002.780062745.000000001DBB1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
38.2.RegAsm.exe.1e1f3c68.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
38.2.RegAsm.exe.1e1f3c68.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
38.2.RegAsm.exe.1f219616.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x2d0af:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x2d0dc:$x2: IClientNetworkHost
38.2.RegAsm.exe.1f219616.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x145e3:$x2: NanoCore.ClientPluginHost • 0x2d0af:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x156be:$s4: PipeCreated • 0x2e18a:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x145fd:$s5: IClientLoggingHost • 0x2d0c9:$s5: IClientLoggingHost
38.2.RegAsm.exe.1f219616.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 25 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

- Detected RDTSC dummy instruction sequence (likely for instruction hammering)
- Tries to detect Any.run
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

- Writes to foreign memory regions

Stealing of Sensitive Information:

- GuLoader behavior detected

Yara detected Nanocore RAT

Remote Access Functionality:

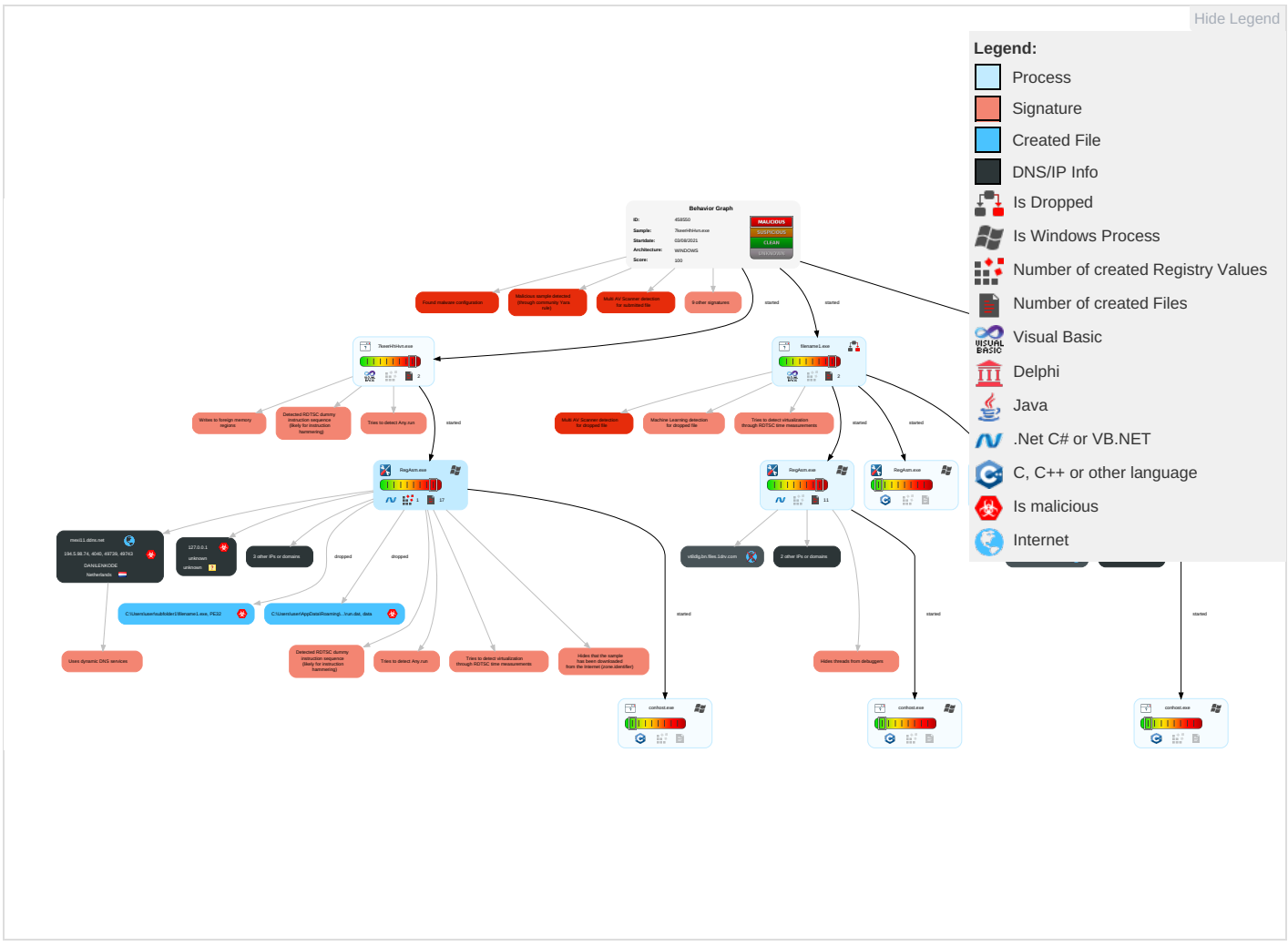
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 1 1 1	Masquerading 1	Input Capture 2 1	Security Software Discovery 6 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavd Inse Netv Com
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Expl Red Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 3 1	Security Account Manager	Virtualization/Sandbox Evasion 2 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Man Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 2 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acce

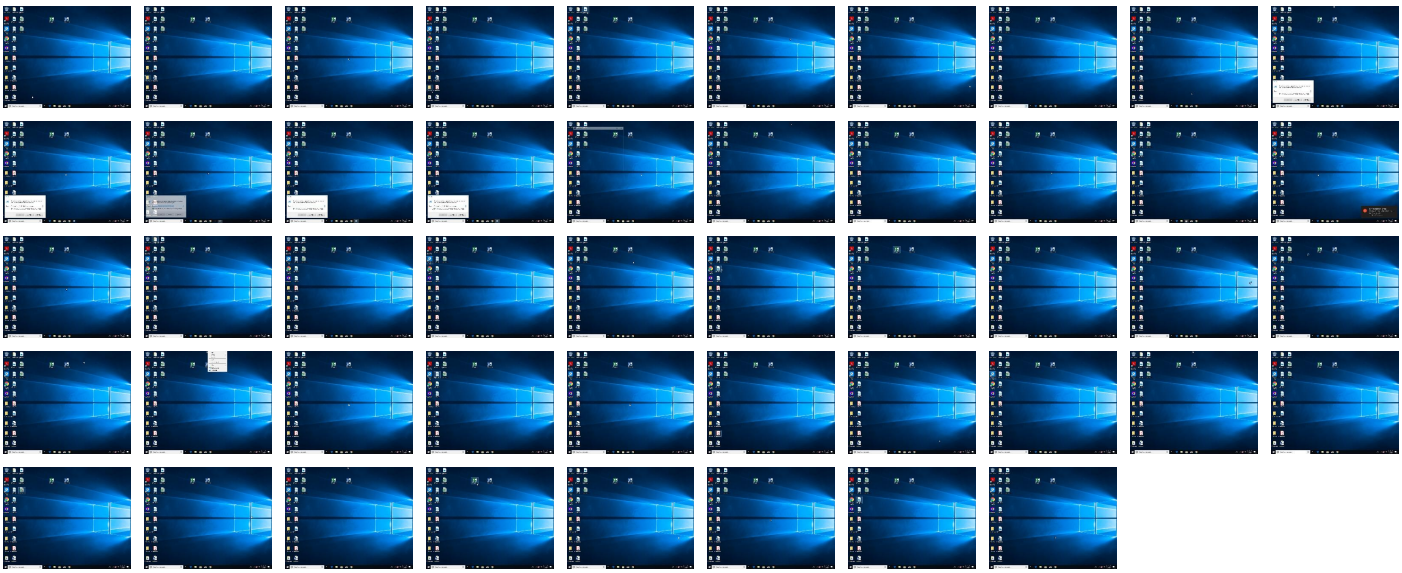
Behavior Graph



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
7keerHhHvn.exe	26%	Virustotal		Browse
7keerHhHvn.exe	27%	ReversingLabs	Win32.Trojan.AgentTesla	
7keerHhHvn.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\subfolder1\filename1.exe	100%	Joe Sandbox ML		
C:\Users\user\subfolder1\filename1.exe	31%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mexi11.ddns.net	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
mexi11.ddns.net	5%	Virustotal		Browse
mexi11.ddns.net	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mexi11.ddns.net	194.5.98.74	true	true	• 5%, Virustotal, Browse	unknown
onedrive.live.com	unknown	unknown	false		high
vt8dlg.bn.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
mexi11.ddns.net	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.74	mexi11.ddns.net	Netherlands		208476	DANILENKODE	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458550
Start date:	03.08.2021
Start time:	14:44:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7keerHhHvn.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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	44
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@18/3@126/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.4% (good quality ratio 1.6%) • Quality average: 13.5% • Quality standard deviation: 21.5%
HCA Information:	• Successful, ratio: 89% • 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
14:47:00	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe
14:47:01	API Interceptor	2932x Sleep call for process: RegAsm.exe modified
14:47:08	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	Purchase.exe	Get hash	malicious	Browse	• 194.5.97.150
	Fec9qUX4at.exe	Get hash	malicious	Browse	• 194.5.97.128
	Ordonnance PL-PB39-210706,pdf.exe	Get hash	malicious	Browse	• 194.5.98.7
	Tzcyxxestkakhuvtmvfdserywturrfjrye.exe	Get hash	malicious	Browse	• 194.5.98.72
	LzbZ4T1iV8.exe	Get hash	malicious	Browse	• 194.5.97.128
	kGSHiWbgq9.exe	Get hash	malicious	Browse	• 194.5.97.128
	loKmeabs9V.exe	Get hash	malicious	Browse	• 194.5.97.128
	1niECmfIcE.exe	Get hash	malicious	Browse	• 194.5.97.94
	Nuzbcdoajgupgalxelbnohzzeonlplvuro.exe	Get hash	malicious	Browse	• 194.5.98.7
	RueoUfi1MZ.exe	Get hash	malicious	Browse	• 194.5.98.3
	Departamento de contadores Consejos de pago 0.exe	Get hash	malicious	Browse	• 194.5.98.7
	04_extracted.exe	Get hash	malicious	Browse	• 194.5.97.18
	scanorder01321.jar	Get hash	malicious	Browse	• 194.5.98.243
	scanorder01321.jar	Get hash	malicious	Browse	• 194.5.98.243
	PO.exe	Get hash	malicious	Browse	• 194.5.98.23
	PO B4007121.exe	Get hash	malicious	Browse	• 194.5.98.7
	WzOSphO1Np.exe	Get hash	malicious	Browse	• 194.5.98.107

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QUOTATION-007222021.exe	Get hash	malicious	Browse	• 194.5.97.145
	PO B4007121.exe	Get hash	malicious	Browse	• 194.5.98.7
	ORDER407-395.exe	Get hash	malicious	Browse	• 194.5.98.23

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Fd5tz8:n5tz8
MD5:	0F6770A104CD85E855C5A5EA85348B17
SHA1:	CD431CBC296446258B44671D7E72667C1B2E37E0
SHA-256:	07687E2CAB23D13E10044B95462C52C12C30F41AED319621FEEBEE9F111D983B
SHA-512:	85689CC95B8D0DD414238D61A1257CAD7228FED52F2BC47DA87571B6725DBBCB2FE3C6F3F72FC9CE73CDD2FAFB34CD33C9C32C28EF7DD2BBA24038D2B643BB4
Malicious:	**true**
Preview:	Y.8..V.H

C:\Users\user\subfolder1\filename1.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	143360
Entropy (8bit):	6.460043863848558
Encrypted:	false
SSDEEP:	3072:S5CCbi+/47tQatuMBmrBeMn5m4vvt6g58:Ai+/g/tuMQlzVntV
MD5:	782783574D2D4B67666B77B686C2E673
SHA1:	8EEEC0963FA7EAF3115335C03315ECC203BABF9B
SHA-256:	0D2AEB4A2F85B9BF8AE3990A3DDEA5A242D0DB5186263E3CCF2435BBC48EC478
SHA-512:	1E500C34D0A1CB7D53661A5759C9D1325A119D86813FD4204F6586B5BF5D16FBF774C694AB6AE367567C38FA38077DD8F1B47991245AFA4B6BA5292B235839FA
Malicious:	**true**

C:\Users\user\subfolder1\filename1.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...S..Q..... .....0.....@.....@.....1.....(....0.. .....text..... . .`.data.....@....rsrc... ....0..... .....@..@...I.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.460043863848558
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	7keerHhHvn.exe
File size:	143360
MD5:	782783574d2d4b67666b77b686c2e673
SHA1:	8eeec0963fa7eaf3115335c03315ecc203babf9b
SHA256:	0d2aeb4a2f85b9bf8ae3990a3ddea5a242d0db5186263e3 ccf2435bbc48ec478
SHA512:	1e500c34d0a1cb7d53661a5759c9d1325a119d86813fd4 204f6586b5bf5d16fbf774c694ab6ae367567c38fa38077d d8f1b47991245afa4b6ba5292b235839fa
SSDEEP:	3072:S5CCbi+/47tQatuMBmrBeMn5m4vvt6g58:Ai+/g/tu MQlzVntV
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....#...B...B ...B..L^...B...`...B...d...B..Rich.B.....PE..L...S..Q..... .....0.....@.....

File Icon

Icon Hash:	c4e8c8cccce0e8e8

Static PE Info

General

Entrypoint:	0x4014b4
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:	0x51ACB753 [Mon Jun 3 15:33:39 2013 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:	fef384fc3a66a559dff455f07d497ca0

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1fcec	0x20000	False	0.384429931641	data	6.7545432225	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x21000	0x11bc	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x23000	0xc20	0x1000	False	0.314453125	data	3.28015845724	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
Chinese	Taiwan	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 14:46:59.369134903 CEST	192.168.2.3	8.8.8.8	0xb6c2	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:00.197516918 CEST	192.168.2.3	8.8.8.8	0x1de6	Standard query (0)	vt8dlg.bn.files.1drv.com	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:04.296108007 CEST	192.168.2.3	37.235.1.174	0xbff2	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:05.292681932 CEST	192.168.2.3	37.235.1.174	0xbff2	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:06.242685080 CEST	192.168.2.3	37.235.1.174	0xbff2	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:08.242249966 CEST	192.168.2.3	37.235.1.174	0xbff2	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:12.354681015 CEST	192.168.2.3	37.235.1.174	0xbff2	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:16.907313108 CEST	192.168.2.3	37.235.1.177	0xf34	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:17.946968079 CEST	192.168.2.3	37.235.1.177	0xf34	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:18.976984024 CEST	192.168.2.3	37.235.1.177	0xf34	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 14:47:21.649106979 CEST	192.168.2.3	37.235.1.177	0xf34	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:26.166146040 CEST	192.168.2.3	37.235.1.177	0xf34	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:35.621997118 CEST	192.168.2.3	8.8.8.8	0x1eda	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:42.986458063 CEST	192.168.2.3	37.235.1.174	0xdd09	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:43.999631882 CEST	192.168.2.3	37.235.1.174	0xdd09	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:45.011310101 CEST	192.168.2.3	37.235.1.174	0xdd09	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:48.230129004 CEST	192.168.2.3	37.235.1.174	0xdd09	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:47:52.277863979 CEST	192.168.2.3	37.235.1.174	0xdd09	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:01.229027033 CEST	192.168.2.3	37.235.1.177	0x347e	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:02.343261957 CEST	192.168.2.3	37.235.1.177	0x347e	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:03.368522882 CEST	192.168.2.3	37.235.1.177	0x347e	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:05.399483919 CEST	192.168.2.3	37.235.1.177	0x347e	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:09.474360943 CEST	192.168.2.3	37.235.1.177	0x347e	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:14.224886894 CEST	192.168.2.3	8.8.8.8	0x6b09	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:19.730734110 CEST	192.168.2.3	37.235.1.174	0xcffd	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:20.757323027 CEST	192.168.2.3	37.235.1.174	0xcffd	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:21.775692940 CEST	192.168.2.3	37.235.1.174	0xcffd	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:23.807049036 CEST	192.168.2.3	37.235.1.174	0xcffd	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:27.854806900 CEST	192.168.2.3	37.235.1.174	0xcffd	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:37.091653109 CEST	192.168.2.3	37.235.1.177	0x6604	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:38.058000088 CEST	192.168.2.3	37.235.1.177	0x6604	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:39.152194023 CEST	192.168.2.3	37.235.1.177	0x6604	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:42.464492083 CEST	192.168.2.3	37.235.1.177	0x6604	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:47.944371939 CEST	192.168.2.3	37.235.1.177	0x6604	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:59.233321905 CEST	192.168.2.3	8.8.8.8	0x5594	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:20.258800983 CEST	192.168.2.3	37.235.1.174	0xdcf7	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:20.493740082 CEST	192.168.2.3	8.8.8.8	0xf4fa	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:21.071223021 CEST	192.168.2.3	8.8.8.8	0x9cf0	Standard query (0)	vt8dlg.bn. files.1drv.com	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:21.249716043 CEST	192.168.2.3	37.235.1.174	0xdcf7	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:22.332037926 CEST	192.168.2.3	37.235.1.174	0xdcf7	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:24.343555927 CEST	192.168.2.3	37.235.1.174	0xdcf7	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:26.367660046 CEST	192.168.2.3	8.8.8.8	0xc35e	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:27.067500114 CEST	192.168.2.3	8.8.8.8	0xaab6	Standard query (0)	vt8dlg.bn. files.1drv.com	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:28.393822908 CEST	192.168.2.3	37.235.1.174	0xdcf7	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:32.611684084 CEST	192.168.2.3	37.235.1.177	0xb62f	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:33.625143051 CEST	192.168.2.3	37.235.1.177	0xb62f	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:34.676656008 CEST	192.168.2.3	37.235.1.177	0xb62f	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 14:49:36.722357988 CEST	192.168.2.3	37.235.1.177	0xb62f	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:40.736180067 CEST	192.168.2.3	37.235.1.177	0xb62f	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:44.786421061 CEST	192.168.2.3	8.8.8.8	0x582e	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:50.041579962 CEST	192.168.2.3	37.235.1.174	0xcab9	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:51.064291000 CEST	192.168.2.3	37.235.1.174	0xcab9	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:52.095896006 CEST	192.168.2.3	37.235.1.174	0xcab9	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:54.142237902 CEST	192.168.2.3	37.235.1.174	0xcab9	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:58.158940077 CEST	192.168.2.3	37.235.1.174	0xcab9	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:02.238451004 CEST	192.168.2.3	37.235.1.177	0xe0ed	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:03.310316086 CEST	192.168.2.3	37.235.1.177	0xe0ed	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:04.346719027 CEST	192.168.2.3	37.235.1.177	0xe0ed	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:07.050962925 CEST	192.168.2.3	37.235.1.177	0xe0ed	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:11.049787998 CEST	192.168.2.3	37.235.1.177	0xe0ed	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:15.121032953 CEST	192.168.2.3	8.8.8.8	0xf0ba	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:20.361833096 CEST	192.168.2.3	37.235.1.174	0x1a01	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:21.348215103 CEST	192.168.2.3	37.235.1.174	0x1a01	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:22.395008087 CEST	192.168.2.3	37.235.1.174	0x1a01	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:24.441831112 CEST	192.168.2.3	37.235.1.174	0x1a01	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:28.489753962 CEST	192.168.2.3	37.235.1.174	0x1a01	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:32.527599096 CEST	192.168.2.3	37.235.1.177	0xe7d4	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:33.551763058 CEST	192.168.2.3	37.235.1.177	0xe7d4	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:34.567779064 CEST	192.168.2.3	37.235.1.177	0xe7d4	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:36.599262953 CEST	192.168.2.3	37.235.1.177	0xe7d4	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:41.068483114 CEST	192.168.2.3	37.235.1.177	0xe7d4	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:45.186182022 CEST	192.168.2.3	8.8.8.8	0xa59b	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:05.606369019 CEST	192.168.2.3	37.235.1.174	0x1573	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:06.648612022 CEST	192.168.2.3	37.235.1.174	0x1573	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:07.649360895 CEST	192.168.2.3	37.235.1.174	0x1573	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:09.664884090 CEST	192.168.2.3	37.235.1.174	0x1573	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:14.306473970 CEST	192.168.2.3	37.235.1.174	0x1573	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:18.394648075 CEST	192.168.2.3	37.235.1.177	0xb62b	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:19.399610043 CEST	192.168.2.3	37.235.1.177	0xb62b	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:20.399944067 CEST	192.168.2.3	37.235.1.177	0xb62b	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:22.415865898 CEST	192.168.2.3	37.235.1.177	0xb62b	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:26.447141886 CEST	192.168.2.3	37.235.1.177	0xb62b	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:30.542591095 CEST	192.168.2.3	8.8.8.8	0x8660	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:35.773979902 CEST	192.168.2.3	37.235.1.174	0xa2f0	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 14:51:36.807101965 CEST	192.168.2.3	37.235.1.174	0xa2f0	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:37.808396101 CEST	192.168.2.3	37.235.1.174	0xa2f0	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:39.807629108 CEST	192.168.2.3	37.235.1.174	0xa2f0	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:43.854691982 CEST	192.168.2.3	37.235.1.174	0xa2f0	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:47.896253109 CEST	192.168.2.3	37.235.1.177	0x486f	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:48.886442900 CEST	192.168.2.3	37.235.1.177	0x486f	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:49.917701006 CEST	192.168.2.3	37.235.1.177	0x486f	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:51.965085983 CEST	192.168.2.3	37.235.1.177	0x486f	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:55.998029947 CEST	192.168.2.3	37.235.1.177	0x486f	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:00.522680044 CEST	192.168.2.3	8.8.8.8	0x1d1	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:06.244844913 CEST	192.168.2.3	37.235.1.174	0x69f0	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:07.232276917 CEST	192.168.2.3	37.235.1.174	0x69f0	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:08.251035929 CEST	192.168.2.3	37.235.1.174	0x69f0	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:10.247987032 CEST	192.168.2.3	37.235.1.174	0x69f0	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:14.295309067 CEST	192.168.2.3	37.235.1.174	0x69f0	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:18.359519005 CEST	192.168.2.3	37.235.1.177	0xae39	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:19.404599905 CEST	192.168.2.3	37.235.1.177	0xae39	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:20.420696020 CEST	192.168.2.3	37.235.1.177	0xae39	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:22.467644930 CEST	192.168.2.3	37.235.1.177	0xae39	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:26.468364000 CEST	192.168.2.3	37.235.1.177	0xae39	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:30.553715944 CEST	192.168.2.3	8.8.8.8	0x169	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:50.889255047 CEST	192.168.2.3	37.235.1.174	0xc6f4	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:51.907280922 CEST	192.168.2.3	37.235.1.174	0xc6f4	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:52.907313108 CEST	192.168.2.3	37.235.1.174	0xc6f4	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:54.923268080 CEST	192.168.2.3	37.235.1.174	0xc6f4	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:58.954516888 CEST	192.168.2.3	37.235.1.174	0xc6f4	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:03.039676905 CEST	192.168.2.3	37.235.1.177	0xeef9	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:04.064625978 CEST	192.168.2.3	37.235.1.177	0xeef9	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:05.097647905 CEST	192.168.2.3	37.235.1.177	0xeef9	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:07.111944914 CEST	192.168.2.3	37.235.1.177	0xeef9	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:11.128269911 CEST	192.168.2.3	37.235.1.177	0xeef9	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:15.209213972 CEST	192.168.2.3	8.8.8.8	0xf3cb	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:20.518920898 CEST	192.168.2.3	37.235.1.174	0xb4a	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:21.519411087 CEST	192.168.2.3	37.235.1.174	0xb4a	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:22.566785097 CEST	192.168.2.3	37.235.1.174	0xb4a	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:24.597949028 CEST	192.168.2.3	37.235.1.174	0xb4a	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:28.645020008 CEST	192.168.2.3	37.235.1.174	0xb4a	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 14:53:32.718887091 CEST	192.168.2.3	37.235.1.177	0xb966	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:33.754573107 CEST	192.168.2.3	37.235.1.177	0xb966	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:34.754681110 CEST	192.168.2.3	37.235.1.177	0xb966	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:36.770991087 CEST	192.168.2.3	37.235.1.177	0xb966	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:40.786465883 CEST	192.168.2.3	37.235.1.177	0xb966	Standard query (0)	mexi11.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 14:46:59.405335903 CEST	8.8.8.8	192.168.2.3	0xb6c2	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 14:47:00.252003908 CEST	8.8.8.8	192.168.2.3	0x1de6	No error (0)	vt8dlg.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 14:47:00.252003908 CEST	8.8.8.8	192.168.2.3	0x1de6	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 14:47:35.656497002 CEST	8.8.8.8	192.168.2.3	0x1eda	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:14.257884979 CEST	8.8.8.8	192.168.2.3	0x6b09	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)
Aug 3, 2021 14:48:59.267369032 CEST	8.8.8.8	192.168.2.3	0x5594	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:20.526868105 CEST	8.8.8.8	192.168.2.3	0xf4fa	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 14:49:21.136039019 CEST	8.8.8.8	192.168.2.3	0x9cf0	No error (0)	vt8dlg.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 14:49:21.136039019 CEST	8.8.8.8	192.168.2.3	0x9cf0	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 14:49:26.403091908 CEST	8.8.8.8	192.168.2.3	0xc35e	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 14:49:27.103094101 CEST	8.8.8.8	192.168.2.3	0xaab6	No error (0)	vt8dlg.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 14:49:27.103094101 CEST	8.8.8.8	192.168.2.3	0xaab6	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 14:49:44.821619034 CEST	8.8.8.8	192.168.2.3	0x582e	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)
Aug 3, 2021 14:49:56.672193050 CEST	8.8.8.8	192.168.2.3	0xcd5b	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 14:50:15.156367064 CEST	8.8.8.8	192.168.2.3	0xf0ba	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:24.716253042 CEST	37.235.1.177	192.168.2.3	0xe0ed	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)
Aug 3, 2021 14:50:45.220398903 CEST	8.8.8.8	192.168.2.3	0xa59b	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)
Aug 3, 2021 14:51:30.574955940 CEST	8.8.8.8	192.168.2.3	0x8660	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:00.558269024 CEST	8.8.8.8	192.168.2.3	0x1d1	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)
Aug 3, 2021 14:52:30.590955973 CEST	8.8.8.8	192.168.2.3	0x169	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)
Aug 3, 2021 14:53:15.244764090 CEST	8.8.8.8	192.168.2.3	0xf3cb	No error (0)	mexi11.ddns.net		194.5.98.74	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 7keerHhHvn.exe PID: 1056 Parent PID: 5604

General

Start time:	14:45:09
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\7keerHhHvn.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\7keerHhHvn.exe'
Imagebase:	0x400000
File size:	143360 bytes
MD5 hash:	782783574D2D4B67666B77B686C2E673
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: RegAsm.exe PID: 2476 Parent PID: 1056

General

Start time:	14:46:05
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\7keerHhHvn.exe'
Imagebase:	0xd50000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 3596 Parent PID: 2476

General

Start time:	14:46:05
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: filename1.exe PID: 2344 Parent PID: 3388

General

Start time:	14:47:08
Start date:	03/08/2021
Path:	C:\Users\user\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x400000
File size:	143360 bytes
MD5 hash:	782783574D2D4B67666B77B686C2E673
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 31%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: filename1.exe PID: 5512 Parent PID: 3388

General

Start time:	14:47:16
Start date:	03/08/2021
Path:	C:\Users\user\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x400000
File size:	143360 bytes
MD5 hash:	782783574D2D4B67666B77B686C2E673

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities Show Windows behavior

Analysis Process: RegAsm.exe PID: 4168 Parent PID: 2344

General

Start time:	14:48:18
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0xd0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 3448 Parent PID: 2344

General

Start time:	14:48:18
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x130000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 5904 Parent PID: 2344

General

Start time:	14:48:19
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0xea0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000026.00000002.767234010.000000001F1D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000026.00000002.767234010.000000001F1D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000026.00000002.767134795.000000001E1D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000026.00000002.767134795.000000001E1D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000026.00000002.762525078.0000000000FD0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 4792 Parent PID: 5904

General

Start time:	14:48:19
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: RegAsm.exe PID: 5376 Parent PID: 5512

General

Start time:	14:48:25
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x520000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 4736 Parent PID: 5512

General

Start time:	14:48:25
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x8c0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000029.00000002.780177556.000000001EBB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000029.00000002.780177556.000000001EBB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000029.00000002.780062745.000000001DBB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000029.00000002.780062745.000000001DBB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000029.00000002.774677046.00000000009F0000.00000004.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: conhost.exe PID: 5028 Parent PID: 4736

General

Start time:	14:48:26
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis