ID: 1502445
Sample Name:
WaveInstaller.exe
Cookbook: default.jbs
Time: 16:20:05
Date: 01/09/2024
Version: 40.0.0 Tourmaline

Table of Contents

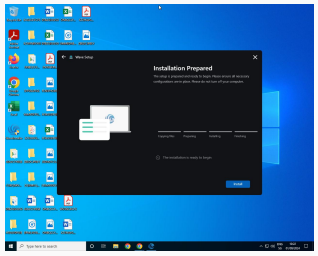
Windows Analysis Report

WaveInstaller.exe

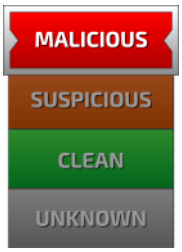
Overview

General Information

Sample name:	WaveInstaller.exe
Analysis ID:	1502445
MD5:	215d509bc217…
SHA1:	bfe0a2580d54c..
SHA256:	984dfc64c10f9…
Tags:	exe
Infos:	



Detection

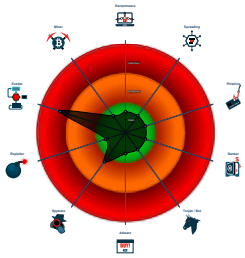


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for subm…
- .NET source code contains potentia…
- Uses Windows timers to delay exec…
- Yara detected Costura Assembly Lo…
- Allocates memory with a write watch…
- Binary contains a suspicious time s…
- Potential time zone aware malware
- Program does not show much activi…
- Queries the volume information (nam…
- Sample file is different than original …

Classification



Process Tree

- **System is w10x64**
- WaveInstaller.exe (PID: 7464 cmdline: "C:\Users\user\Desktop\WaveInstaller.exe" MD5: 215D509BC217F7878270C161763B471E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
WaveInstaller.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.1637430102.0000000000B82000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000002.2895806482.00000000031A1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: WaveInstaller.exe PID: 7464	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.WaveInstaller.exe.b80000.0.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Suricata Signatures

No Suricata rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Data Obfuscation

.NET source code contains potential unpacker

Yara detected Costura Assembly Loader

Malware Analysis System Evasion

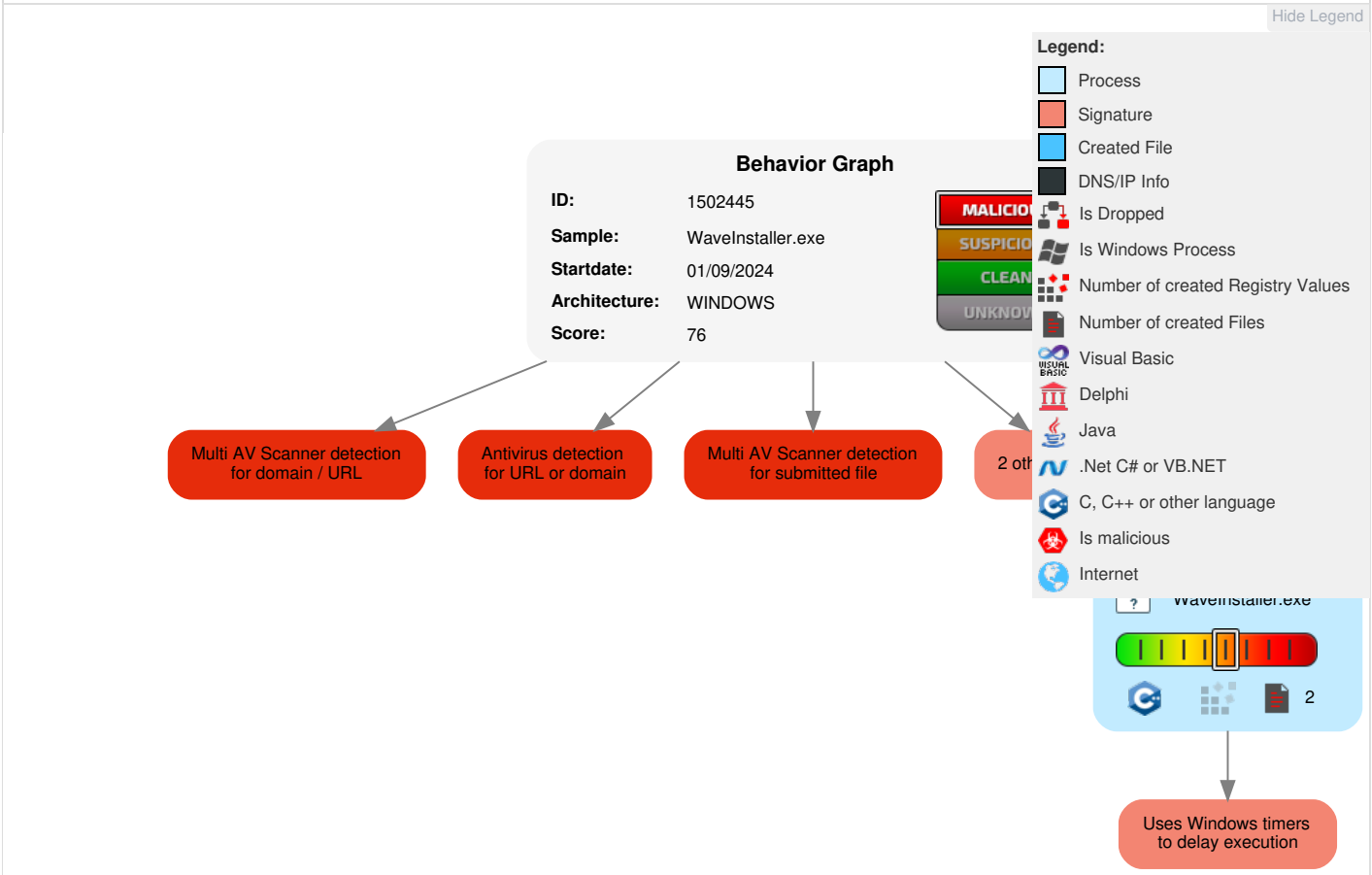
Uses Windows timers to delay execution

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	2 Command and Scripting Interpreter	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Junk Data	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	1 2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Steganography	Automated Exfiltration	Data Encrypted for Impact

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 Timestomp	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	Internet Connection Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Obfuscated Files or Information	Cached Domain Credentials	Wi-Fi Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

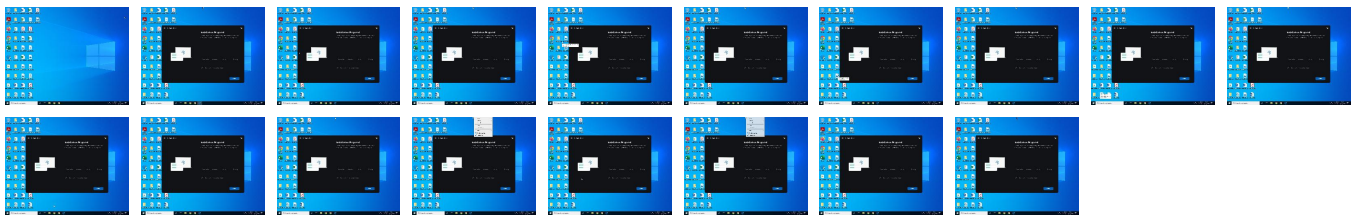
Behavior Graph

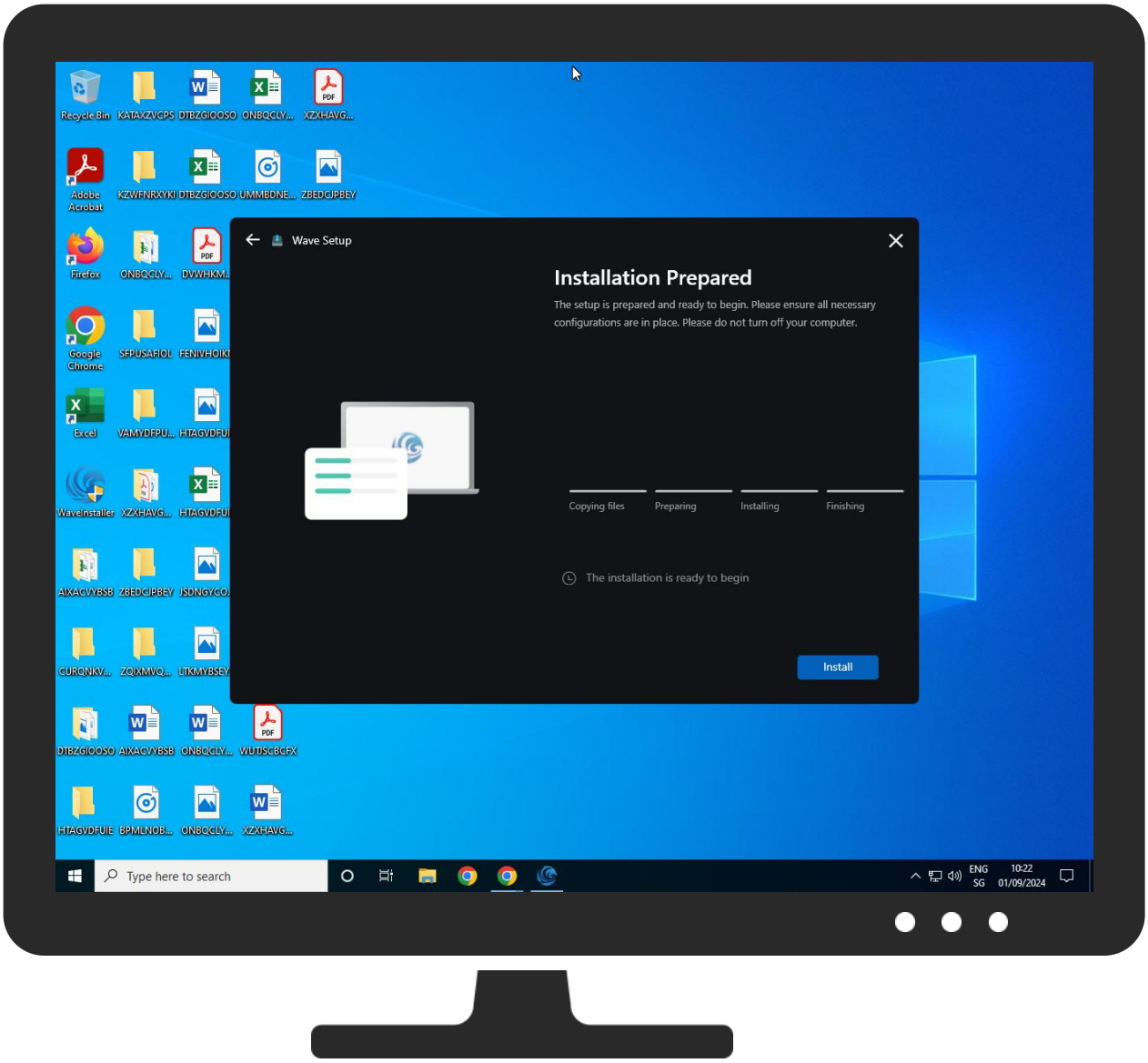


Screenshots

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
WaveInstaller.exe	32%	ReversingLabs	Win32.Trojan.Generic	
WaveInstaller.exe	45%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://github.com/dxgi/wave-binaries/raw/main/CefSharp.Common.124.3.8.rar	0%	Avira URL Cloud	safe	
http://https://github.com/dxgi/wave-binaries/raw/main/CefSharp.Wpf.124.3.8.rar	0%	Avira URL Cloud	safe	
http://https://www.nuget.org/api/v2/package/chromiumembeddedframework.runtime.win-x86/124.3.8	0%	Avira URL Cloud	safe	
http://https://www.nuget.org/api/v2/package/chromiumembeddedframework.runtime.win-x86/124.3.87CefSharp.Comm	0%	Avira URL Cloud	safe	
http://https://cdn.getwave.gg/bootstrapper/WaveWindows.exe-Wave	100%	Avira URL Cloud	malware	
http://https://github.com/dxgi/wave-binaries/raw/main/Wave-x64.rar	0%	Avira URL Cloud	safe	
http://https://github.com/dxgi/wave-binaries/raw/main/Luau-x64.rar	0%	Avira URL Cloud	safe	
http://https://github.com/dxgi/wave-binaries/raw/main/CefSharp.Wpf.124.3.8.rar	0%	Virustotal		Browse
http://https://www.nuget.org/api/v2/package/chromiumembeddedframework.runtime.win-x86/124.3.8	0%	Virustotal		Browse
http://https://cdn.getwave.gg/bootstrapper/WaveWindows.exeio	100%	Avira URL Cloud	malware	
http://https://github.com/dxgi/wave-binaries/raw/main/CefSharp.Common.124.3.8.rar1CefSharp.Wpf.124.3.8.rar	0%	Avira URL Cloud	safe	
http://https://github.com/dxgi/wave-binaries/raw/main/CefSharp.Common.124.3.8.rar	0%	Virustotal		Browse
http://https://github.com/dxgi/wave-binaries/raw/main/Luau-x64.rar	0%	Virustotal		Browse
http://https://github.com/dxgi/wave-binaries/raw/main/Wave-x64.rar	0%	Virustotal		Browse
http://https://github.com/dxgi/wave-binaries/raw/main/CefSharp.Common.124.3.8.rar1CefSharp.Wpf.124.3.8.rar	0%	Virustotal		Browse
http://https://cdn.getwave.gg/bootstrapper/WaveWindows.exe-Wave	11%	Virustotal		Browse
http://https://www.nuget.org/api/v2/package/chromiumembeddedframework.runtime.win-x86/124.3.87CefSharp.Comm	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.getwave.gg/bootstrapper/WaveWindows.exe-Wave	WaveInstaller.exe	false	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://github.com/dxgi/wave-binaries/raw/main/CefSharp.Wpf.124.3.8.rar	WaveInstaller.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.nuget.org/api/v2/package/chromiumembeddedframework.runtime.win-x86/124.3.8	WaveInstaller.exe, 00000000.00000002.2895806482.00000000031A1000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.nuget.org/api/v2/package/chromiumembeddedframework.runtime.win-x86/124.3.87CefSharp.Comm	WaveInstaller.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://github.com/dxgi/wave-binaries/raw/main/CefSharp.Common.124.3.8.rar	WaveInstaller.exe, 00000000.00000002.2895806482.00000000031A1000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://github.com/dxgi/wave-binaries/raw/main/Luau-x64.rar	WaveInstaller.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://github.com/dxgi/wave-binaries/raw/main/Wave-x64.rar	WaveInstaller.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://cdn.getwave.gg/bootstrapper/WaveWindows.exeio	WaveInstaller.exe, 00000000.00000002.2895806482.00000000031A1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://github.com/dxgi/wave-binaries/raw/main/CefSharp.Common.124.3.8.rar1CefSharp.Wpf.124.3.8.rar	WaveInstaller.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1502445
Start date and time:	2024-09-01 16:20:05 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 3m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	7
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	WaveInstaller.exe
Detection:	MAL
Classification:	mal76.evad.winEXE@1/0@0/0
EGA Information:	Failed
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- Execution Graph export aborted for target WaveInstaller.exe, PID 7464 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.874597413262029
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	WaveInstaller.exe
File size:	2'377'216 bytes
MD5:	215d509bc217f7878270c161763b471e
SHA1:	bfe0a2580d54cfa28d3ff5ef8dc754fdc73adcd9
SHA256:	984dfc64c10f96c5350d6d9216a5d7abfece1658dfc93925f7a6b0c80817c886
SHA512:	68e615dfcb1b7770ad64175438a913744c14bdd3af93b339c2b526271bdd0d23334e78d049fdae8ca9fe66672a8cf252ebf891be9ab6c46a3d8f1fb00fa8c83b
SSDEEP:	49152:LinbT3qpTDQSmanAmwJAaDMg33U2pLOiniT:LinKpTJmWAmmAMP8in
TLSH:	6DB512192A3CC8CBEC3907B15AFAE15A7B39317782490748ECCCC14C62F9E56F5B6529
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...v.4.....".0...!..8.....N+!.. .....@.. .....$.....`.....

File Icon

Icon Hash:	2340020b0bbf733f

Static PE Info

General

Entrypoint:	0x612b4e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x8C34F576 [Sat Jul 16 11:22:30 2044 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:	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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x212af4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x214000	0x33568	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x248000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x212a60	0x38	.text
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	

Name	Virtual Address	Virtual Size	Is in Section
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	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x210b54	0x210c00	41e0a54accebca40bf945a207af8a88f	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x214000	0x33568	0x33600	32ec3b22a5cf4afe774f17b0bc6fcb20	False	0.5065579379562044	data	6.519047836554647	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x248000	0xc	0x200	b8becffedd18a9b187b1a5d4a2499a67	False	0.044921875	MacBinary, Mon Feb 6 07:28:16 2040 INVALID date, modified Mon Feb 6 07:28:16 2040 "!"	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x214200	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024, resolution 5669 x 5669 px/m			0.875
RT_ICON	0x214678	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304, resolution 5669 x 5669 px/m			0.7729508196721312
RT_ICON	0x215010	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096, resolution 5669 x 5669 px/m			0.6744840525328331
RT_ICON	0x2160c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216, resolution 5669 x 5669 px/m			0.5504149377593361
RT_ICON	0x218680	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384, resolution 5669 x 5669 px/m			0.4750236183278224
RT_ICON	0x21c8b8	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736, resolution 5669 x 5669 px/m			0.4406192236598891
RT_ICON	0x221d50	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864, resolution 5669 x 5669 px/m			0.36519865461425266
RT_ICON	0x22b208	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536, resolution 5669 x 5669 px/m			0.2990949958594582
RT_ICON	0x23ba40	0xa9e7	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced			0.9990343717668697
RT_GROUP_ICON	0x246438	0x84	data			0.7272727272727273
RT_VERSION	0x2464cc	0x33c	data			0.41304347826086957
RT_MANIFEST	0x246818	0xd4c	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators			0.38689776733254994

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WaveInstaller.exe PID: 7464, Parent PID: 2580

General

Target ID:	0
Start time:	10:20:51
Start date:	01/09/2024
Path:	C:\Users\user\Desktop\WaveInstaller.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\WaveInstaller.exe"
Imagebase:	0xb80000
File size:	2'377'216 bytes
MD5 hash:	215D509BC217F7878270C161763B471E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000000.1637430102.0000000000B82000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.2895806482.00000000031A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	false

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	72BBF4C3	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	72BBF4C3	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C: \Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BBCBDB	unknown
C: \Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	72B60842	ReadFile
C: \Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BD738A	ReadFile
C: \Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BD738A	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\38481df3886f4bbd3cc20bcb84e0ed73\PresentationFramework.ni.dll.aux	0	2436	success or wait	1	72B60842	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\4d760e3e4675c4a4c66b64205fb0d001\WindowsBase.ni.dll.aux	0	1348	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\17470ef0c7a174f38bdcadacc3e310ad\PresentationCore.ni.dll.aux	0	1832	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\4a6b3689887244ce68a20c5d8154ca54\System.Xaml.ni.dll.aux	0	572	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	72B60842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	72BBCBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71A89B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71A89B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\bb5812ab3cec92427da8c5c696e5f731\System.Net.Http.ni.dll.aux	0	536	success or wait	1	72B60842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatioaec034ca#\cbe8cd16089e77a8a17d8292a6a5e943\PresentationFramework.Aero2.ni.dll.aux	0	1252	success or wait	1	72B60842	ReadFile

Disassembly

No disassembly