ID: 534010
Sample Name: E196fncR4E.exe
Cookbook: default.jbs
Time: 00:07:37
Date: 05/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

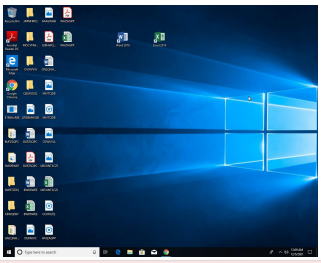
Windows Analysis Report E196fncR4E.exe

Overview

General Information

Sample Name:	E196fncR4E.exe
Analysis ID:	534010
MD5:	a15f089ed04672a.
SHA1:	8761c4ac67f6faa..
SHA256:	79682758e1c5e1..
Tags:	exe RedLineStealer
Infos:	

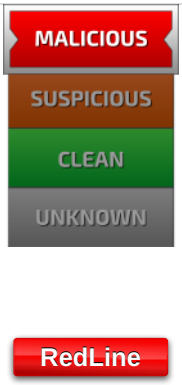
Most interesting Screenshot:



Errors

- Sigma runtime error: Invalid condition: all of selection* Rule: Conti Backup Database
- Sigma runtime error: Invalid condition: all of selection* Rule: Stop Or Remove Antivirus Service
- Sigma runtime error: Invalid condition: all of selection* Rule: Conti Volume Shadow Listing
- Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With 7-ZIP
- Sigma runtime error: Invalid condition: all of selection* Rule: Disable or Delete Windows Eventlog
- Sigma runtime error: Invalid condition: all of selection* Rule: PowerShell Web Request
- Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With WINZIP

Detection

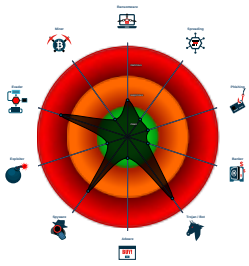


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Antivirus / Scanner detection for sub…
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Tries to steal Crypto Currency Wallets
- Connects to many ports of the same…
- Contains functionality to hide user a…
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Queries sensitive video device inform…
- Queries sensitive disk information (v…
- Sigma detected: Microsoft Workflow…
- Tries to harvest and steal browser in…
- PE file contains section with special…
- Uses 32bit PE files
- Queries the volume information (nam…
- May sleep (evasive loops) to hinder …
- Checks if Antivirus/Antispyware/Fire…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Internet Provider seen in connection…

Classification



Process Tree

- System is w10x64
- E196fncR4E.exe (PID: 2224 cmdline: "C:\Users\user\Desktop\E196fncR4E.exe" MD5: A15F089ED04672A843DBE2FA9CA3C69A)
  - RegSvcs.exe (PID: 4240 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
  - dfsvc.exe (PID: 6628 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\dfsvc.exe MD5: 48FD4DD682051712E3E7757C525DED71)
  - Microsoft.Workflow.Compiler.exe (PID: 6604 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\Microsoft.Workflow.Compiler.exe MD5: D91462AE31562E241AF5595BA5E1A3C4)
  - InstallUtil.exe (PID: 6692 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- cleanup

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "87.251.73.109:37261"
  ],
  "Bot Id": "@"
}
```

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.674383078.00000000061D0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000005.00000000.659360737.0000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000005.00000002.721305659.0000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000002.674103198.0000000003C6A000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000002.668694127.00000000028C0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.E196fncR4E.exe.28c0000.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.2.E196fncR4E.exe.61d0000.9.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.2.E196fncR4E.exe.3a35530.6.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.2.E196fncR4E.exe.3a55550.7.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.2.E196fncR4E.exe.6240000.11.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 13 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Microsoft Workflow Compiler

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking:

Networking:

Connects to many ports of the same IP (likely port scanning)

System Summary:

PE file contains section with special chars

Hooking and other Techniques for Hiding and Protection:

Contains functionality to hide user accounts

Malware Analysis System Evasion:

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

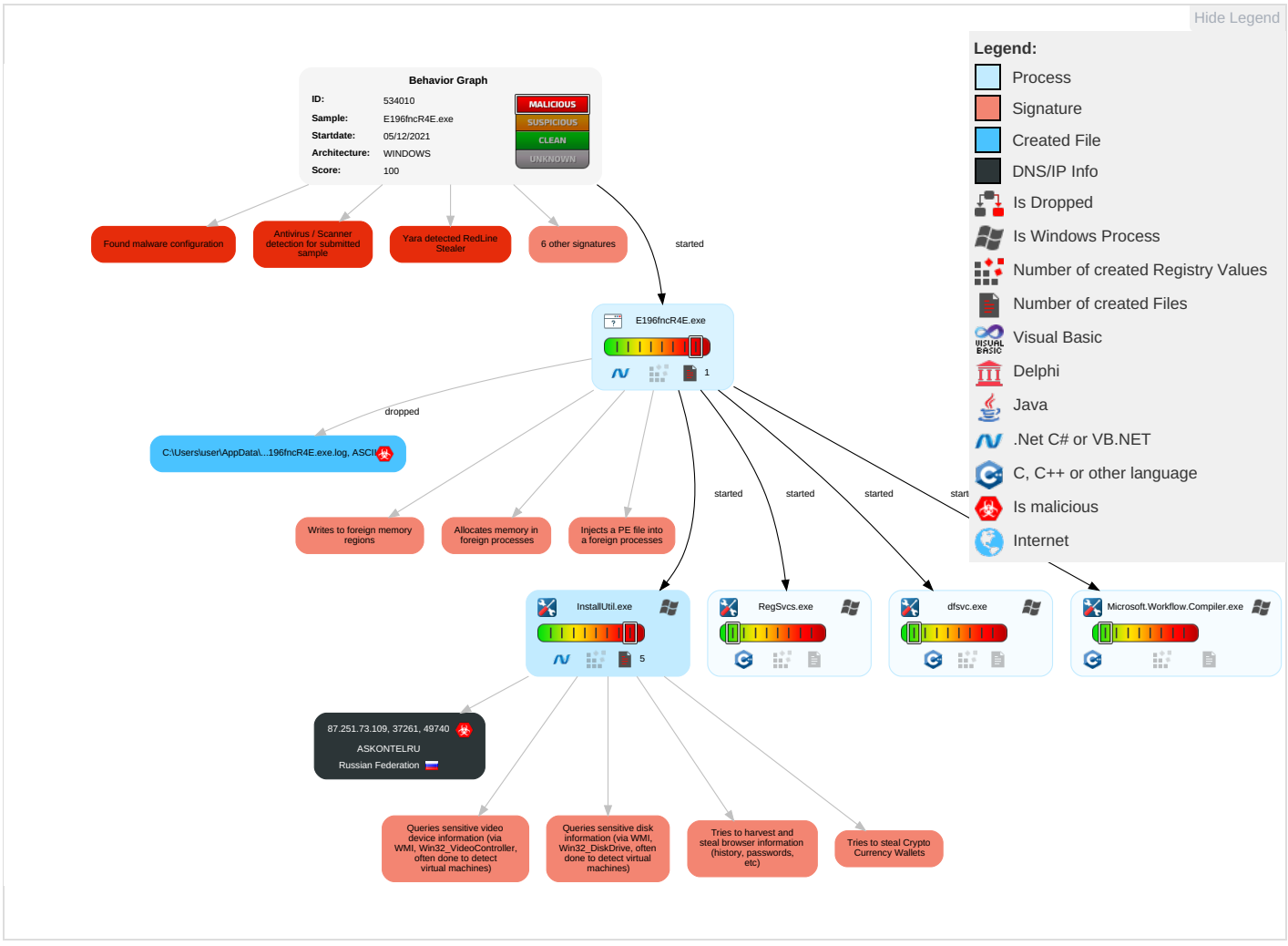
Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Process Injection 3 1 1	Masquerading 1	OS Credential Dumping 1	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 3 1	Security Account Manager	Process Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 1	NTDS	Virtualization/Sandbox Evasion 2 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Users 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

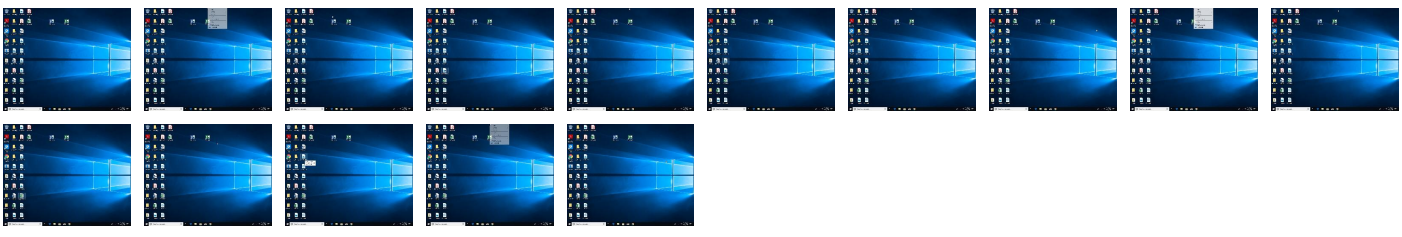
Behavior Graph



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
E196fncR4E.exe	100%	Avira	HEUR/AGEN.1133806	
E196fncR4E.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.E196fncR4E.exe.6f0000.0.unpack	100%	Avira	HEUR/AGEN.1133806		Download File
1.0.E196fncR4E.exe.6f0000.0.unpack	100%	Avira	HEUR/AGEN.1133806		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.251.73.109	unknown	Russian Federation		204490	ASKONTELRU	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	534010
Start date:	05.12.2021
Start time:	00:07:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	E196fncR4E.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:	11
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.spyw.evad.winEXE@9/2@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 83% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 93% • 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 • Stop behavior analysis, all processes terminated
Warnings:	Show All
Errors:	• Sigma runtime error: Invalid condition: all of selection* Rule: Conti Backup Database • Sigma runtime error: Invalid condition: all of selection* Rule: Stop Or Remove Antivirus Service • Sigma runtime error: Invalid condition: all of selection* Rule: Conti Volume Shadow Listing • Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With 7-ZIP • Sigma runtime error: Invalid condition: all of selection* Rule: Disable or Delete Windows Eventlog • Sigma runtime error: Invalid condition: all of selection* Rule: PowerShell SAM Copy • Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With WINZIP

Simulations

Behavior and APIs

Time	Type	Description
00:08:55	API Interceptor	37x Sleep call for process: InstallUtil.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
87.251.73.109	466c4a9f01e7b04499eafee7a9283df00ed06c00134cc.exe	Get hash	malicious	Browse	
	EV49Im3Lnd.exe	Get hash	malicious	Browse	
	9820500aae4c3b3b5ab38a63f9776a75cfb2203a20798.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASKONTELRU	466c4a9f01e7b04499eafee7a9283df00ed06c00134cc.exe	Get hash	malicious	Browse	• 87.251.73.109
	Kq8hjfiv87.exe	Get hash	malicious	Browse	• 185.186.142.166
	pgOVV6yBlF.exe	Get hash	malicious	Browse	• 185.186.142.166
	jvclBMP1vW.exe	Get hash	malicious	Browse	• 185.186.142.166
	9wHCL2s0mn.exe	Get hash	malicious	Browse	• 185.186.142.166
	lqzq58DLHP.exe	Get hash	malicious	Browse	• 185.186.142.166
	ZU7aA39iRz.exe	Get hash	malicious	Browse	• 185.186.142.166
	OTYlygnSWX.exe	Get hash	malicious	Browse	• 185.186.142.166
	KQ9j4VJ0f8.exe	Get hash	malicious	Browse	• 185.186.142.166
	r3vhW8dfrr.exe	Get hash	malicious	Browse	• 185.186.142.166
	70h2dF8m45.exe	Get hash	malicious	Browse	• 185.186.142.166
	mGRHBSEOZW.exe	Get hash	malicious	Browse	• 185.186.142.166
	lnlJCR9JVn.exe	Get hash	malicious	Browse	• 185.186.142.166
	EOGcyVU7U3.exe	Get hash	malicious	Browse	• 185.186.142.166
	VF78jGjtCG.exe	Get hash	malicious	Browse	• 185.186.142.166
	EV49Im3Lnd.exe	Get hash	malicious	Browse	• 87.251.73.109
	9820500aae4c3b3b5ab38a63f9776a75cfb2203a20798.exe	Get hash	malicious	Browse	• 87.251.73.109
	6093384421389c5a04411fe0807a20ec283ef9bbb248b.exe	Get hash	malicious	Browse	• 185.186.143.241
	swift_mt103.xlsx	Get hash	malicious	Browse	• 185.186.142.132
	outstanding_remit111921.xlsx	Get hash	malicious	Browse	• 185.186.142.132

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\E196fncR4E.exe.log

Process:	C:\Users\user\Desktop\E196fncR4E.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.347301286976015
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat92n4MqmI+DLI4M9s:ML9E4Ks2wKDE4KhK3VZ9pKhg84xmIeEw
MD5:	5D8E90786245BC9A124C0F045E69D4B0
SHA1:	C318D99F7C812F42D811BD70B37B682101785028
SHA-256:	83920340DA936F72DF8B5876526B01675916AF7DEA377613808985220CC9432E
SHA-512:	77AB06E1741F94B4E356775E846DBA4BC5F178F5F972A8494A320C251E739C2DE267D947E1867795F901CE26C6A53A14EAB7CD454C23CE0CB1B8AAAB3145467
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\E196fncR4E.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Workflow.Compiler, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InstallUtil.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKoLHG1qHjHKdHAHDJn:vq5qXAqLqdqUqzcGYqhQnoPtlxHbqoL1
MD5:	B8B968C6C5994E11C0AEF299F6CC13DF
SHA1:	60351148A0D29E39DF51AE7F8D6DA7653E31BCF9
SHA-256:	DD53198266985E5C23239DCDDE91B25CF1FC1F4266B239533C11DDF0EF0F958D
SHA-512:	CFBCFCB650EF8C84A4BA005404E90ECAC9E77BDB618F53CD5948C085E44D099183C97C1D818A905B16C5E495FF167BD47347B14670A6E68801B0C01BC264F1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.70800225309473
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	E196fncR4E.exe
File size:	223744
MD5:	a15f089ed04672a843dbe2fa9ca3c69a
SHA1:	8761c4ac67f6faa8b6e05a6844f3b24d33a35fe2
SHA256:	79682758e1c5e1b4796f6882bd35890e84d3f6de23c445e79d7df25de67721c8
SHA512:	2f25c7854a2bf66c4c6f40e6eac9a143b33f4607d747696d60262da071a8f7d9cf4044f4f595db9129d9027e703fb0b78053b5a8d3eabe821e654ef3908c4167
SSDEEP:	6144:yOyJYFq1ye0vCY839its1L+MXytKCaDEJw:F/F62FQ6SLzXQKCagw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...).d.....0..:...,.....>....`.. ....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x43983e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0xC564A029 [Mon Dec 10 22:22:33 2074 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
A(!@(!	0x2000	0x22e4	0x2400	False	1.00119357639	data	7.9791679085	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x6000	0x33844	0x33a00	False	0.591059132869	data	6.6573114894	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x3a000	0x5c6	0x600	False	0.419270833333	data	4.14050513885	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Behavior

Click to jump to process

System Behavior

Analysis Process: E196fncR4E.exe PID: 2224 Parent PID: 5516

General

Start time:	00:08:26
Start date:	05/12/2021
Path:	C:\Users\user\Desktop\E196fncR4E.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\E196fncR4E.exe"
Imagebase:	0x6f0000
File size:	223744 bytes
MD5 hash:	A15F089ED04672A843DBE2FA9CA3C69A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.674383078.00000000061D0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.674103198.0000000003C6A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.668694127.00000000028C0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.673461133.0000000003A55000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.674538239.0000000006240000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.673366720.0000000003A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.668653404.00000000028A0000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 4240 Parent PID: 2224

General

Start time:	00:08:27
Start date:	05/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x110000

File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dfsvc.exe PID: 6628 Parent PID: 2224

General

Start time:	00:08:28
Start date:	05/12/2021
Path:	C:\Windows\Microsoft.NET\assembly\GAC_MSIL\dfsvc\v4.0_4.0.0.0__b03f5f7f11d50a3a\dfsvc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\dfsvc.exe
Imagebase:	0x2509cd90000
File size:	24160 bytes
MD5 hash:	48FD4DD682051712E3E7757C525DED71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: Microsoft.Workflow.Compiler.exe PID: 6604 Parent PID: 2224

General

Start time:	00:08:29
Start date:	05/12/2021
Path:	C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.Workflow.Compiler\v4.0_4.0.0.0__31bf3856ad364e35\Microsoft.Workflow.Compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Microsoft.Workflow.Compiler.exe
Imagebase:	0x23f26ad0000
File size:	32872 bytes
MD5 hash:	D91462AE31562E241AF5595BA5E1A3C4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: InstallUtil.exe PID: 6692 Parent PID: 2224

General

Start time:	00:08:30
Start date:	05/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0xbe0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000005.00000000.659360737.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000005.00000002.721305659.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000005.00000000.660068047.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000005.00000000.660369622.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000005.00000000.659685845.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis