

JOeSandbox Cloud BASIC



ID: 553367

Sample Name: xD2TnigEaY

Cookbook: default.jbs

Time: 19:07:32

Date: 14/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report xD2TnigEaY	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: RedLine	3
Yara Overview	3
Initial Sample	3
PCAP (Network Traffic)	3
Memory Dumps	4
Unpacked PEs	4
Sigma Overview	4
Jbx Signature Overview	4
AV Detection:	4
Malware Analysis System Evasion:	4
Stealing of Sensitive Information:	4
Remote Access Functionality:	4
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	5
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	7
Contacted Domains	7
URLs from Memory and Binaries	7
Contacted IPs	8
Public	8
General Information	8
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	9
General	9
File Icon	10
Static PE Info	10
General	10
Entrypoint Preview	10
Data Directories	10
Sections	10
Resources	10
Imports	10
Version Infos	10
Network Behavior	10
Network Port Distribution	10
TCP Packets	11
Code Manipulations	11
Statistics	11
System Behavior	11
Analysis Process: xD2TnigEaY.exe PID: 5128 Parent PID: 5772	11
General	11
File Activities	11
File Created	11
File Written	11
File Read	11
Disassembly	11
Code Analysis	11

Windows Analysis Report xD2TnigEaY

Overview

General Information

Sample Name:	xD2TnigEaY (renamed file extension from none to exe)
Analysis ID:	553367
MD5:	07dd723a06bb89..
SHA1:	d36a56e3aa33c6..
SHA256:	d56f880cb8c35e6..
Tags:	32 exe RedLineStealer
Infos:	
Most interesting Screenshot:	

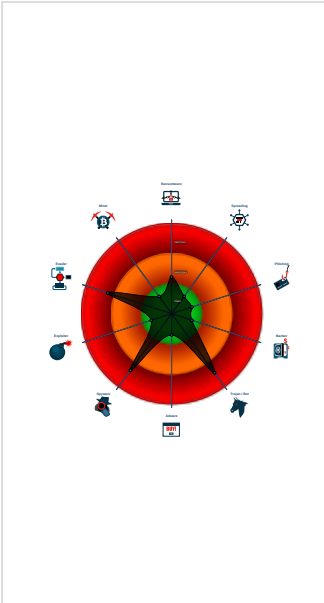
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN RedLine	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Yara detected RedLine Stealer
Antivirus / Scanner detection for sub...
Found malware configuration
Multi AV Scanner detection for subm...
Antivirus detection for URL or domain
Queries sensitive video device inform...
Tries to steal Crypto Currency Wallets
Queries sensitive disk information (v...
Found many strings related to Crypt...
Machine Learning detection for samp...
Tries to harvest and steal browser in...
Is looking for software installed on th...
Uses 32bit PE files
Found a high number of Window / Us...

Classification



Process Tree

- System is w10x64
- xD2TnigEaY.exe (PID: 5128 cmdline: "C:\Users\user\Desktop\xD2TnigEaY.exe" MD5: 07DD723A06BB89DC1BDCE3CC56F1CF20)
- cleanup

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "208.167.249.72:2943"
  ],
  "Bot Id": "Result"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
xD2TnigEaY.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

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
00000000.00000000.341469282.00000000001E2000.00000002.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.397709229.00000000001E2000.00000002.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.398592673.00000000026F0000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.398592673.00000000026F0000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: xD2TnigEaY.exe PID: 5128	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 1 entries

Unpacked PE's

Source	Rule	Description	Author	Strings
0.2.xD2TnigEaY.exe.1e0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.0.xD2TnigEaY.exe.1e0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview



Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

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)

Stealing of Sensitive Information:



Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Found many strings related to Crypto-Wallets (likely being stolen)

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

Remote Access Functionality:

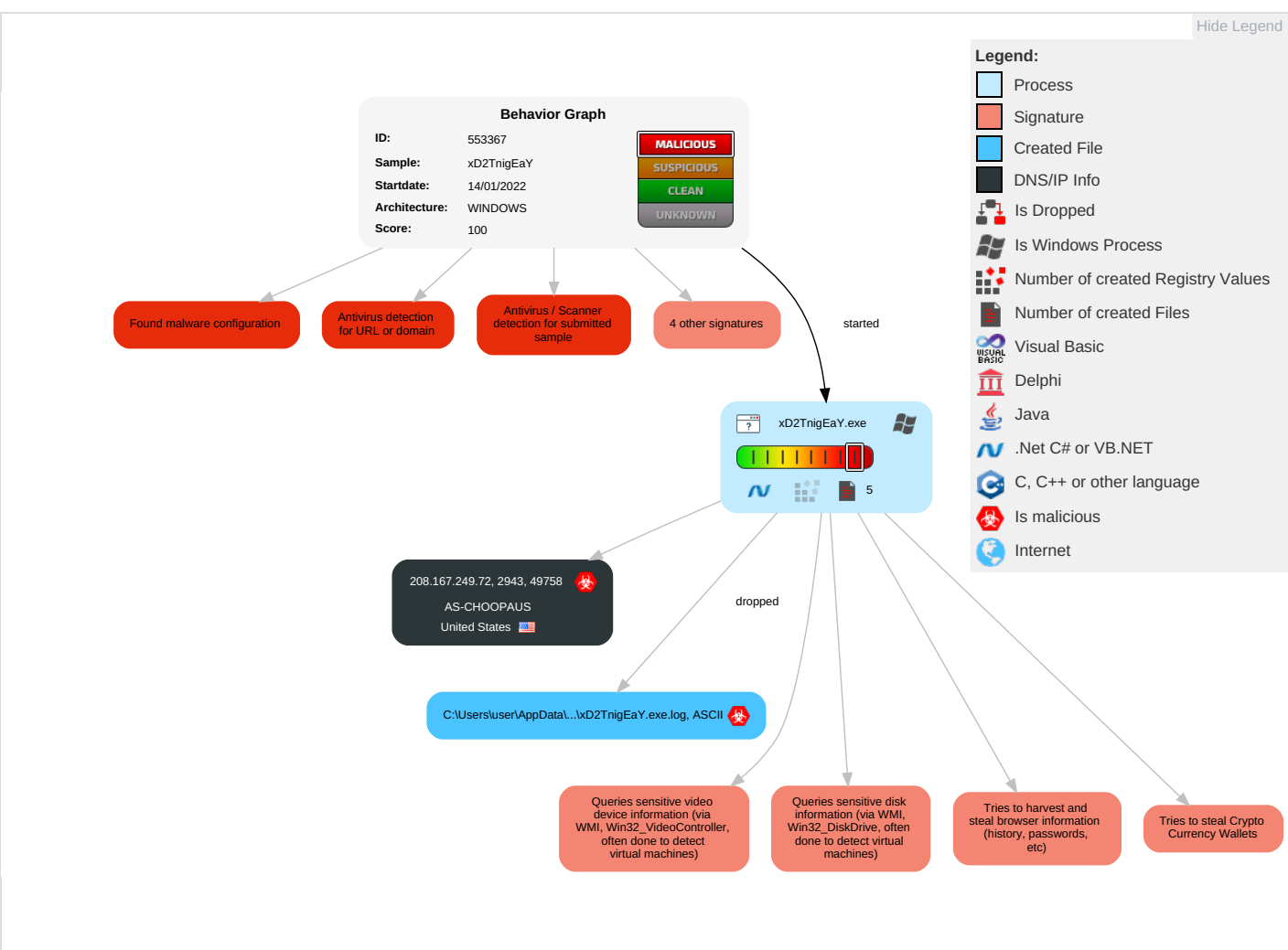


Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 2 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdropping, Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Scripts, Redirected Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	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	Steganography	Exploit Scripts, Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	System Information Discovery 1 2 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulation of Device Communication

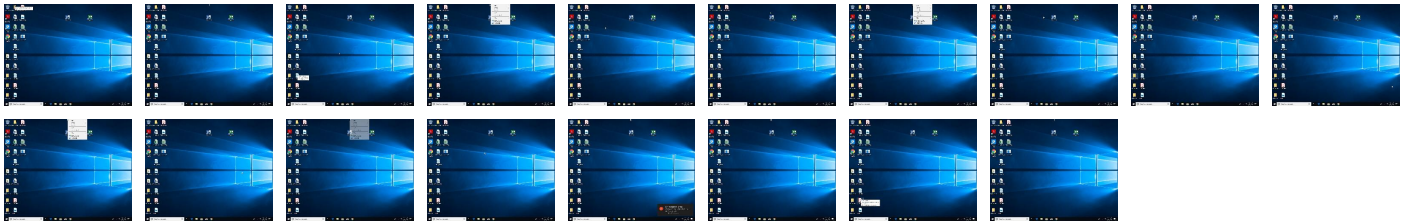
Behavior Graph



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
xD2TnigEaY.exe	65%	Virustotal		Browse
xD2TnigEaY.exe	84%	ReversingLabs	ByteCode-MSIL.InfoStealer.RedLine	
xD2TnigEaY.exe	100%	Avira	HEUR/AGEN.1145065	
xD2TnigEaY.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.xD2TnigEaY.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
0.0.xD2TnigEaY.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1145065		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
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/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/Id22ResponseH0f	100%	Avira URL Cloud	phishing	
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
208.167.249.72	unknown	United States		20473	AS-CHOOPAUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553367
Start date:	14.01.2022
Start time:	19:07:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xD2TnigEaY (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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@1/1@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.1%) • Quality average: 24.2% • Quality standard deviation: 35.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:08:54	API Interceptor	21x Sleep call for process: xD2TnigEaY.exe modified

Joe Sandbox View / Context

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogslxD2TnigEaY.exe.log	
Process:	C:\Users\user\Desktop\lxD2TnigEaY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MOFHK5HKXAHKhBHKdHKB1AHKzVqThmYHKhQnoPtHoxHlImHKOHLHG1qHjHKdHAHDJn:vg5qXAqLqdqUqzcGYqhQnoPtIxHbqoL1
MD5:	B8B968C6C5994E11C0AEF299F6CC13DF
SHA1:	60351148A0D29E39DF51AE7F8D6DA7653E31BCF9
SHA-256:	DD53198266985E5C23239DCDDE91B25CF1FC1F4266B239533C11DDF0EF0F958D
SHA-512:	CFBFCFB650EF8C8A4BA005404E90ECAC9E77BDB618F53CD5948C085E44D099183C97C1D818A905B16C5E495FF167BD47347B14670A6E68801B0C01BC264F1
Malicious:	true
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.Runtb92aa12#\34957343ad5d84dae97a1affda91665\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):	5.771488269227702
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.79% - Win32 Executable (generic) a (10002005/4) 49.75% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Windows Screen Saver (13104/52) 0.07% - Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	xD2TnigEaY.exe
File size:	106496
MD5:	07dd723a06bb89dc1bdce3cc56f1cf20
SHA1:	d36a56e3aa33c602cbb405dc6dd7425e17cf4672

General	
SHA256:	d56f880cb8c35e66750faa6ae9284f0eb2383cec287e8cef4f85122fe90d4305
SHA512:	0d031e01c6f19357db61df8801971de597ad50a8a3822232f97b186aada2d7f2e9758d5d6d120b510f8e5eef61cb08020c5d308094a3ccee9364b9c51e8d60ed
SSDEEP:	1536:bUVrU5RhoBuHDZATQWxUYITiF/YuXUrsbYpf8MeRToPvsS800s:bUVIfpHDi0WxVJiHerKz5TRZu
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......PE..L..., S.....0.....@.. .@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4191ae
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
Time Stamp:	0xB1F9532C [Thu Aug 14 02:36:28 2064 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
.text	0x2000	0x18d84	0x19000	False	0.43318359375	data	5.87919002445	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1c000	0x4dc	0x800	False	0.2841796875	data	2.99852033217	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1e000	0xc	0x400	False	0.025390625	data	0.0558553080537	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

System Behavior

Analysis Process: xD2TnigEaY.exe PID: 5128 Parent PID: 5772

General

Start time:	19:08:30
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\xD2TnigEaY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\xD2TnigEaY.exe"
Imagebase:	0x1e0000
File size:	106496 bytes
MD5 hash:	07DD723A06BB89DC1BDCE3CC56F1CF20
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: 00000000.00000000.341469282.00000000001E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.397709229.00000000001E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.398592673.00000000026F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.398592673.00000000026F0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis

