ID: 533997
Sample Name:
y3LE4c6D5u.exe
Cookbook: default.jbs
Time: 22:41:10
Date: 04/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

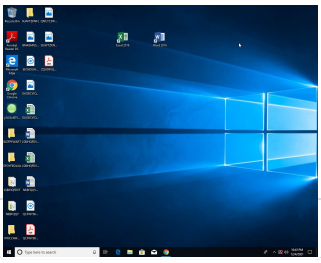
Windows Analysis Report y3LE4c6D5u.exe

Overview

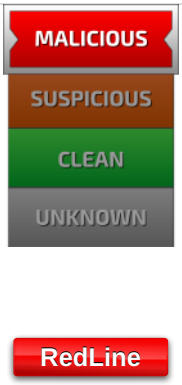
General Information

Sample Name:	y3LE4c6D5u.exe
Analysis ID:	533997
MD5:	3e8cc35ca6575d…
SHA1:	ef6d17e7d00a933.
SHA256:	cf91e3f791e5a6e..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

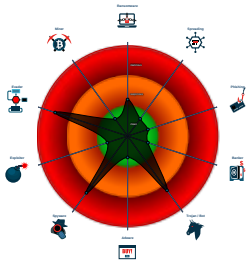


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Detected unpacking (overwrites its o…
- Tries to steal Crypto Currency Wallets
- Machine Learning detection for samp…
- Queries sensitive video device inform…
- Queries sensitive disk information (v…
- Found many strings related to Crypt…
- Tries to harvest and steal browser in…
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- y3LE4c6D5u.exe (PID: 4028 cmdline: "C:\Users\user\Desktop\y3LE4c6D5u.exe" MD5: 3E8CC35CA6575D200A33026A43D97E93)
- **cleanup**

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "185.215.113.67:30242"
  ],
  "Bot Id": "Palpa"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.338351783.00000000021D5000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.338910699.0000000002674000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.341341615.0000000004A20000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.340525187.0000000003624A000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.338491858.0000000002350000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 3 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.y3LE4c6D5u.exe.50a660.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.y3LE4c6D5u.exe.2350ee8.4.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.y3LE4c6D5u.exe.221563e.2.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.y3LE4c6D5u.exe.221563e.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.y3LE4c6D5u.exe.2350ee8.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

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)

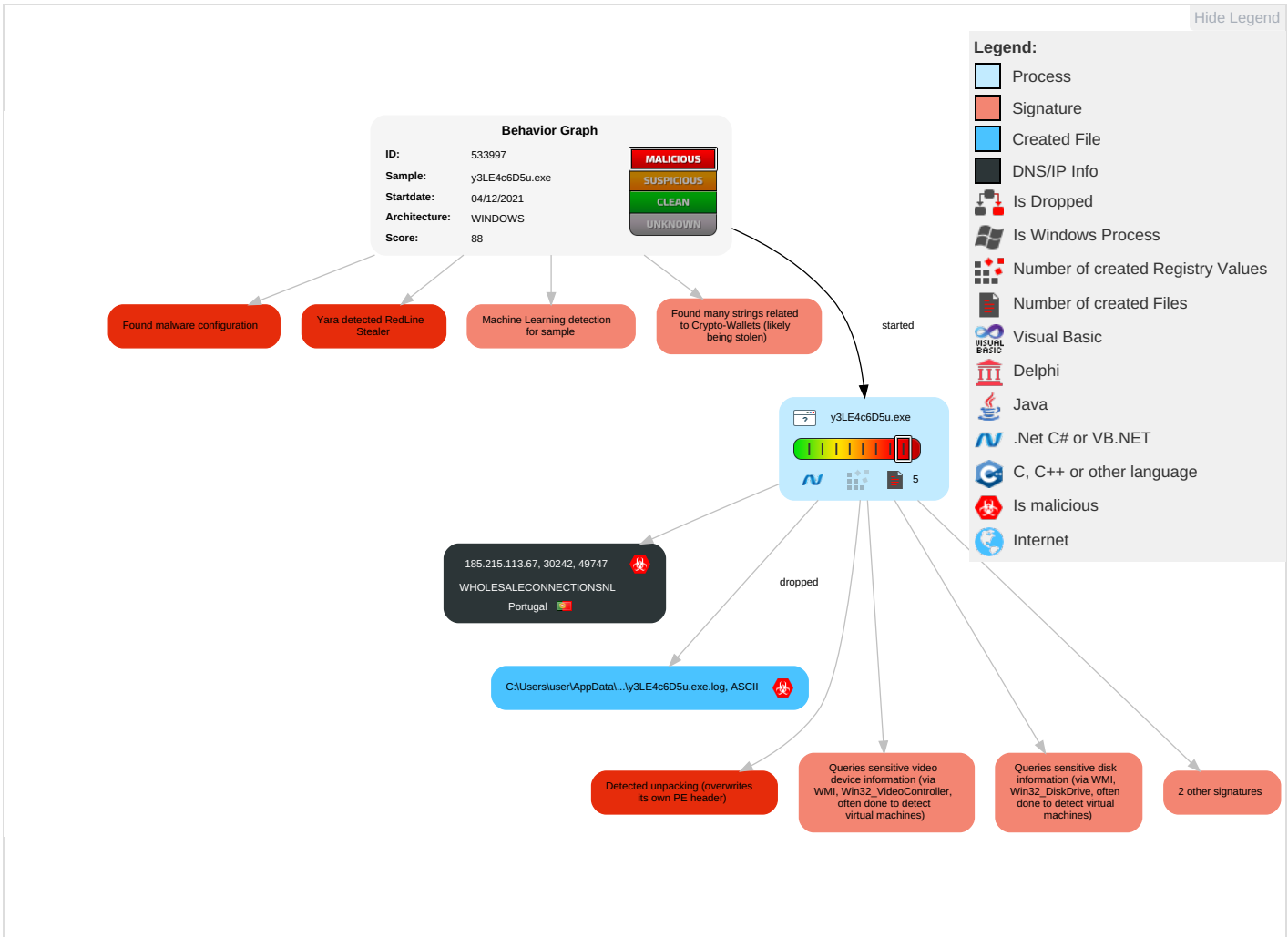
Remote Access Functionality:

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	Netw Effec
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comn
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 6 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls/
Domain Accounts	Native API 1	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	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comn
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 2	Cached Domain Credentials	System Information Discovery 1 3 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic

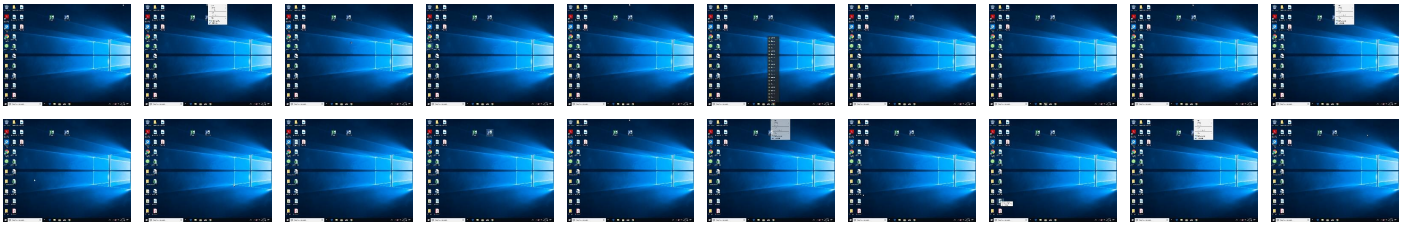
Behavior Graph



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
y3LE4c6D5u.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

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://ns.adobe.c/g	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

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.215.113.67	unknown	Portugal		206894	WHOLESALECONNECTIONSNL	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	533997
Start date:	04.12.2021
Start time:	22:41:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	y3LE4c6D5u.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:	22
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:	mal88.troj.spyw.evad.winEXE@1/1@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 38.3% (good quality ratio 36.7%) • Quality average: 84.6% • Quality standard deviation: 25.2%
HCA Information:	• Successful, ratio: 100% • 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
22:42:21	API Interceptor	62x Sleep call for process: y3LE4c6D5u.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.215.113.67	oMHveSc3hh.exe	Get hash	malicious	Browse	• 185.215.113.67/4dcYcWsw3/index.php
	0KuDEDABFO.exe	Get hash	malicious	Browse	• 185.215.113.67/4dcYcWsw3/index.php
	miOnrvnXK0.exe	Get hash	malicious	Browse	• 185.215.113.67/4dcYcWsw3/index.php
	Rh74sODsWE.exe	Get hash	malicious	Browse	• 185.215.113.67/4dcYcWsw3/index.php
	dSQUdo6EjO.exe	Get hash	malicious	Browse	• 185.215.113.67/4dcYcWsw3/index.php
	usVhwck8lN.exe	Get hash	malicious	Browse	• 185.215.113.67/4dcYcWsw3/index.php
	SecuriteInfo.com.W32.AIDetect.malware1.20102.exe	Get hash	malicious	Browse	• 185.215.113.67/4dcYcWsw3/index.php
	MR98F1zzeo.exe	Get hash	malicious	Browse	• 185.215.113.67/4dcYcWsw3/index.php
	8f5718a6042061b23a4e42ee5cd8112946c135dc9d0c2.exe	Get hash	malicious	Browse	• 185.215.113.67/4dcYcWsw3/index.php
	fC4T1vVs24.exe	Get hash	malicious	Browse	• umbrelladdownload.uno/gp6GbqVce/index.php
	Yw1JP5EYQJ.exe	Get hash	malicious	Browse	• umbrelladdownload.uno/gp6GbqVce/index.php

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WHOLESALECONNECTIONSNL	780426DE24AE46F300FDAF9CBF597C8F2164F7B6C525C.exe	Get hash	malicious	Browse	• 185.215.113.208
	10645f6f4e270d6a9181b7c04c11e5b251caabfe7a204.exe	Get hash	malicious	Browse	• 185.215.113.67
	W88QoyCyC7.exe	Get hash	malicious	Browse	• 185.215.113.208
	mB7g5qi5hg.exe	Get hash	malicious	Browse	• 185.215.113.67
	C7304FF0966068D305DA031F9DA60C5B0EBE32AC43533.exe	Get hash	malicious	Browse	• 185.215.113.208
	l6l10z8wKV.exe	Get hash	malicious	Browse	• 185.215.113.208
	2FCmNeQzct.exe	Get hash	malicious	Browse	• 185.215.113.67
	qwEMaieh4k.exe	Get hash	malicious	Browse	• 185.215.113.208
	FKdsgnUjpn.exe	Get hash	malicious	Browse	• 185.215.113.208
	y8xn6l2hY0.exe	Get hash	malicious	Browse	• 185.215.113.208
	mixshop_20211204-142046(1).exe	Get hash	malicious	Browse	• 185.215.113.15
	2ywvPFqvsp.exe	Get hash	malicious	Browse	• 185.215.113.67
	9i54LrAWDa.exe	Get hash	malicious	Browse	• 185.215.113.67
	jA0D6OjNRa.exe	Get hash	malicious	Browse	• 185.215.113.44
	AAH2imJVoV.exe	Get hash	malicious	Browse	• 185.215.113.67
	xajsmKqcFk.exe	Get hash	malicious	Browse	• 185.215.113.208

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4L2BCPJRuk.exe	Get hash	malicious	Browse	• 185.215.113.208
	XPCIJGAZa6.exe	Get hash	malicious	Browse	• 185.215.113.44
	r3rKPk6RDO.exe	Get hash	malicious	Browse	• 185.215.113.208
	pquHvJLDFX.exe	Get hash	malicious	Browse	• 185.215.113.208

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\y3LE4c6D5u.exe.log

Process:	C:\Users\user\Desktop\y3LE4c6D5u.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHK5HKXRfHK7HKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKoLHG1qHqHAH5HX:Pq5qXdq7qLqdqUqzcGYqhQnoPtlxHbq4
MD5:	924DEA6470CAC502B24442CF377CE6A7
SHA1:	133C304912A1DF4AF62F6EDCA3EA21F3E0CE7F4F
SHA-256:	2B2572C7D0134EEF12644AF90D61302A50E7B550FFB4629666F8C566F34BED0D
SHA-512:	34C817F3F4D87AAD5F6902BB80522B59FE8F9935C86819B575B6139EBDEF3026866ED802DB1D36765CF7ECCF323692705DCA3D799FC7CFF7C0114B08CBE9F7A
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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.Runtimeb92aa12#\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\b219d4630d26b88041b

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.114668063596944
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	y3LE4c6D5u.exe
File size:	421376
MD5:	3e8cc35ca6575d200a33026a43d97e93
SHA1:	ef6d17e7d00a933e06fe712ed89ef519da1ca650
SHA256:	cf91e3f791e5a6e9ce4cf4c1765ffdaf0fd8a61382071c2ef7e32e84f7b854ef
SHA512:	76c6b973546f3cbf586e172757bc617b71050fb5e16b233c511566bbe22ea5c91fd4793b9d30616abf5b7dffb237595504a1c925f513922b4cd2e27b07aa30b4
SSDEEP:	6144:A0CtUfY3icsOj7eJMTu1MOO50GHseggomDoelkXmP6rRu0:A00w/SeSwMOO50GRymMeOGit

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.kD!...!...!...?...;...?.....?.....n~.&...!.....?... ...?... ...?... ...Rich!.....PE..L...[5Z_.....d.

File Icon

Icon Hash:	dab1e4d4e4b9c7b8

Static PE Info

General

Entrypoint:	0x40373d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5F5A355B [Thu Sep 10 14:16:59 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	ace494ecc2c2c2c7ecf836ae6aa78574

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5634d	0x56400	False	0.769964334239	data	7.58350051554	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x58000	0x4934	0x4a00	False	0.375527871622	data	5.33905171138	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5d000	0xe5c8	0xa400	False	0.0572599085366	data	0.737558606312	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x6c000	0x1740	0x1800	False	0.680989583333	data	5.86466086019	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
Nepali	Nepal	

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: y3LE4c6D5u.exe PID: 4028 Parent PID: 1376

General

Start time:	22:41:58
Start date:	04/12/2021
Path:	C:\Users\user\Desktop\y3LE4c6D5u.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\y3LE4c6D5u.exe"
Imagebase:	0x400000
File size:	421376 bytes
MD5 hash:	3E8CC35CA6575D200A33026A43D97E93
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: 00000000.00000002.338351783.00000000021D5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.338910699.0000000002674000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.341341615.0000000004A20000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.340525187.000000000362A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.338491858.0000000002350000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.273143458.000000000050A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis