ID: 528741
Sample Name:
d32Z71Q0wT.exe
Cookbook: default.jbs
Time: 18:21:16
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

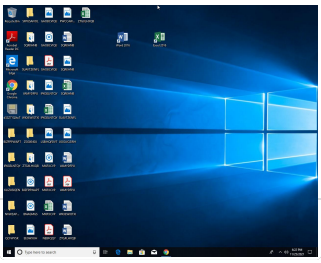
Windows Analysis Report d32Z71Q0wT.exe

Overview

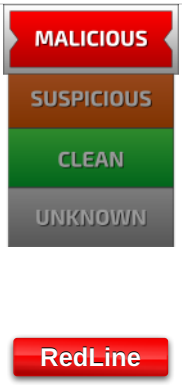
General Information

Sample Name:	d32Z71Q0wT.exe
Analysis ID:	528741
MD5:	22881f3c6d61c70..
SHA1:	90d344108bb0ba..
SHA256:	a2b6c4286d9de9..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

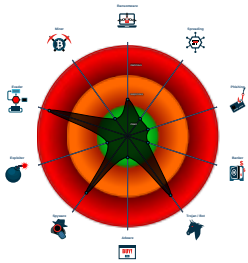


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Detected unpacking (overwrites its o…
- Detected unpacking (changes PE se…
- 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…

Classification



Process Tree

- **System is w10x64**
- d32Z71Q0wT.exe (PID: 3280 cmdline: "C:\Users\user\Desktop\d32Z71Q0wT.exe" MD5: 22881F3C6D61C70B25FF28654B6961E5)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "193.56.146.64:65441"
  ],
  "Bot Id": "udptest"
}
```


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
00000000.00000002.725147062.0000000003C50000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.724710900.0000000003990000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.671477605.0000000001E87000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.727344652.0000000004F1A000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.725068988.0000000003B65000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.d32Z71Q0wT.exe.3c50000.6.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.d32Z71Q0wT.exe.3ba60c6.5.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.d32Z71Q0wT.exe.3990000.2.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.d32Z71Q0wT.exe.3ba51de.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.d32Z71Q0wT.exe.3c50000.6.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)

Detected unpacking (changes PE section rights)

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)

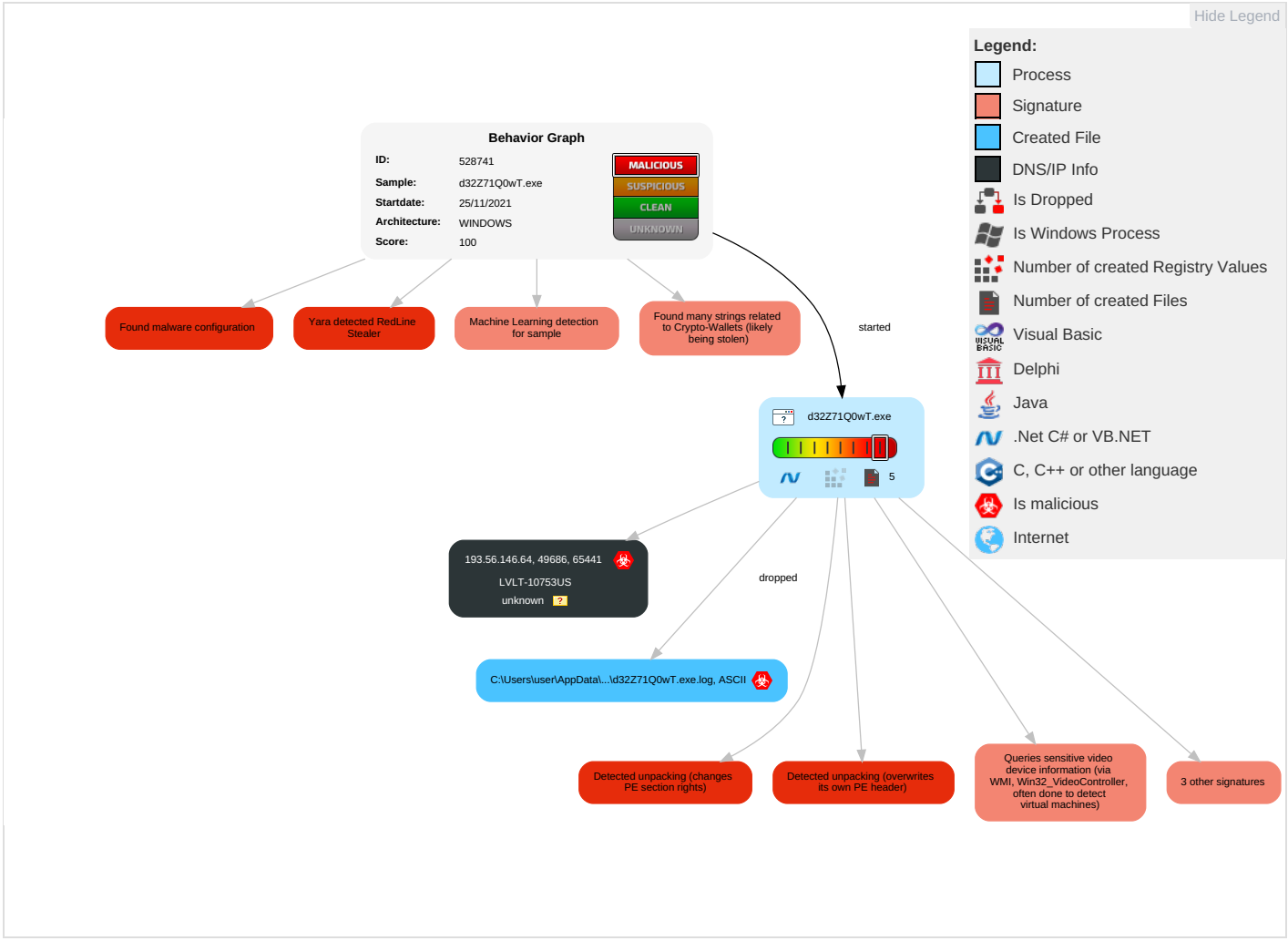
Remote Access Functionality:

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 1	Remote Services	Input Capture 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	Input Capture 1	Security Software Discovery 2 6 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redire 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 Local System 3	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 1	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 2 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
d32Z71Q0wT.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	

Source	Detection	Scanner	Label	Link
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://www.interoperabilitybridges.com/wmp-extension-for-chromex	0%	Avira URL Cloud	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
193.56.146.64	unknown	unknown	?	10753	LVLT-10753US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal

Analysis ID:	528741
Start date:	25.11.2021
Start time:	18:21:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	d32Z71Q0wT.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:	1
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: 11.4% (good quality ratio 11%) • Quality average: 84.5% • Quality standard deviation: 23.5%
HCA Information:	• Successful, ratio: 67% • 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

Simulations

Behavior and APIs

Time	Type	Description
18:22:41	API Interceptor	10x Sleep call for process: d32Z71Q0wT.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
193.56.146.64	n3ZB11gmgx.exe	Get hash	malicious	Browse	
	lUutlamdAP.exe	Get hash	malicious	Browse	
	JVOevQSmez.exe	Get hash	malicious	Browse	
	tgrnZru3Ux.exe	Get hash	malicious	Browse	
	kWe1P2w4cy.exe	Get hash	malicious	Browse	
	9qifkNvPb8.exe	Get hash	malicious	Browse	
	AOE3ZrAHCZ.exe	Get hash	malicious	Browse	
	7ux5Q0EZQH.exe	Get hash	malicious	Browse	
	QVRDRyonIY.exe	Get hash	malicious	Browse	
	pLKSFlouAv.exe	Get hash	malicious	Browse	
	uzViZJ5hxU.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	aebCfcwHy0.exe	Get hash	malicious	Browse	
	5o2bRAvHx9.exe	Get hash	malicious	Browse	
	2ce1WYKMsA.exe	Get hash	malicious	Browse	
	Kod7jprn7K.exe	Get hash	malicious	Browse	
	2LG87UfOTH.exe	Get hash	malicious	Browse	
	4Lkdxnkt9M.exe	Get hash	malicious	Browse	
	t2E05q13ox.exe	Get hash	malicious	Browse	
	I3O28Z5uqy.exe	Get hash	malicious	Browse	
	Hf34l6qunJ.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LVLT-10753US	n3ZB11gmgx.exe	Get hash	malicious	Browse	• 193.56.146.64
	OPKyR75fJn.exe	Get hash	malicious	Browse	• 193.56.146.36
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	• 193.56.146.36
	23062BA932165210EBB3FFCD15474E79F19E6AD74869F.exe	Get hash	malicious	Browse	• 193.56.146.36
	lUutlamdAP.exe	Get hash	malicious	Browse	• 193.56.146.64
	44E401AAF0B52528AA033257C1A1B8A09A2B10EDF26ED.exe	Get hash	malicious	Browse	• 193.56.146.36
	77012C024869BA2639B54B959FAB1E10EBAAF8EBB9BFC.exe	Get hash	malicious	Browse	• 193.56.146.36
	22BA4262D93379DE524029DAFC7528E431E56A22CB293.exe	Get hash	malicious	Browse	• 193.56.146.36
	zMvP34LhcZ.exe	Get hash	malicious	Browse	• 193.56.146.36
	JVOevQSmez.exe	Get hash	malicious	Browse	• 193.56.146.64
	wmwL0AmWha.exe	Get hash	malicious	Browse	• 193.56.146.36
	BPjUXSEwuL.exe	Get hash	malicious	Browse	• 193.56.146.36
	734C31431B89B7501B984AF35A2D61BDCE27BA87CA484.exe	Get hash	malicious	Browse	• 193.56.146.36
	utKWcb6Hzs.exe	Get hash	malicious	Browse	• 193.56.146.36
	6ZYg7h0ynL.exe	Get hash	malicious	Browse	• 193.56.146.36
	CVfKJhwYQW.exe	Get hash	malicious	Browse	• 193.56.146.36
	1baYVecsju.exe	Get hash	malicious	Browse	• 193.56.146.36
	tgrnZru3Ux.exe	Get hash	malicious	Browse	• 193.56.146.64
	F2433DFBA69148A0C3A5A5951D360B6C3C045090DE06F.exe	Get hash	malicious	Browse	• 193.56.146.36
	kWe1P2w4cy.exe	Get hash	malicious	Browse	• 193.56.146.64

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\d32Z71Q0wT.exe.log

Process:	C:\Users\user\Desktop\d32Z71Q0wT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHK5HKXRfHK7HKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHK1HxLHG1qHqH5HX:Pq5qXdq7qLqdqUqzcGYqhQnoPtlxHbqG
MD5:	B480B5E2E0D8EB6CC658782575F52F35

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\d32Z71Q0wT.exe.log	
SHA1:	5E0440E4E0005F9084A7061FF942618083DD400A
SHA-256:	1A8388CF5706484514C6358BCA4DFFE463A1AE1A1BEAB38DB480B3CB262EE14E
SHA-512:	DEADF1B8FB8DC8AC7E4AC8D2E36E48CDB20E3B6E6431C465BF81C9B26731CAFFB85537F7AA5762B9479528092209B29FAC84317A3AAF3EEE1D9E0E8617786732
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.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\b219d4630d26b88041b

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.593386354237363
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:	d32Z71Q0wT.exe
File size:	414208
MD5:	22881f3c6d61c70b25ff28654b6961e5
SHA1:	90d344108bb0ba41e068080443a4bd42c25bdf54
SHA256:	a2b6c4286d9de9cded676840936ce2446a5244d5e415613404eae6430efc8c58
SHA512:	aa57847eb66727fd72fd66ed5cfbeb46e14bdf1c03a17ed9fa9137d864de0aadd80036ef1d806e81b714ccfe0661d9e1831e3c4355b85ecf9523fedc6bf9d889
SSDEEP:	6144:os/8DawW7XxngvaXXAHBIRM0ff/SzpIsLsX:X8DaqaXXA+i0ff/STLs
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...p...p...p..Wp...p..bp...p..Vp...p..op...p...pa..p..Sp...p..fp...p..ap...pRich...p.....PE..L...R.&_.....

File Icon

Icon Hash:	a2e8e8e8aaa2a488

Static PE Info

General

Entrypoint:	0x433040
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5F26C552 [Sun Aug 2 13:53:22 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5

General

Subsystem Version Minor:	1
Import Hash:	ee6524c22cc0cf74d4c47508c44cd3e2

Entrypoint Preview

Rich Headers

Data Directories

Sections

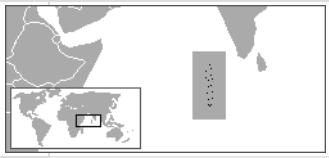
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4ba02	0x4bc00	False	0.748359503919	data	7.51602349785	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x4d000	0x17b41c0	0x1400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1802000	0x67f8	0x6800	False	0.53662109375	data	5.52301875313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1809000	0x1143c	0x11600	False	0.0749494154676	data	0.972181558947	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Divehi; Dhivehi; Maldivian	Maldives	
Spanish	Panama	

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: d32Z71Q0wT.exe PID: 3280 Parent PID: 5408

General

Start time:	18:22:11
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\d32Z71Q0wT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\d32Z71Q0wT.exe"
Imagebase:	0x400000
File size:	414208 bytes
MD5 hash:	22881F3C6D61C70B25FF28654B6961E5
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: 00000000.00000002.725147062.0000000003C50000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.724710900.0000000003990000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.671477605.0000000001E87000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.727344652.0000000004F1A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.725068988.0000000003B65000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis