ID: 510140
Sample Name: IfakQb9U15.exe
Cookbook: default.jbs
Time: 14:07:11
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

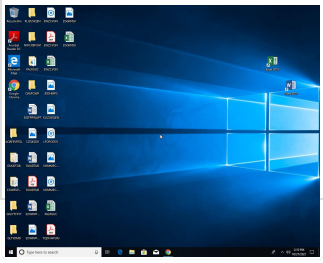
Windows Analysis Report IfakQb9U15.exe

Overview

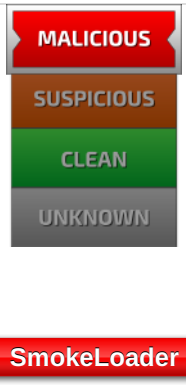
General Information

Sample Name:	IfakQb9U15.exe
Analysis ID:	510140
MD5:	36f662b3c9a54c0..
SHA1:	7e46615097282a..
SHA256:	d836a03e0b7eea..
Tags:	exe SmokeLoader
Infos:	

Most interesting Screenshot:



Detection

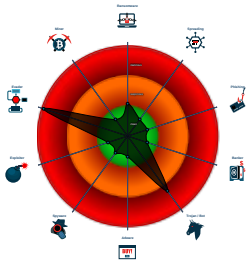


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Antivirus / Scanner detection for sub…
- Yara detected SmokeLoader
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- IfakQb9U15.exe (PID: 4748 cmdline: 'C:\Users\user\Desktop\IfakQb9U15.exe' MD5: 36F662B3C9A54C0C2427602F1463EB69)
  - IfakQb9U15.exe (PID: 2456 cmdline: 'C:\Users\user\Desktop\IfakQb9U15.exe' MD5: 36F662B3C9A54C0C2427602F1463EB69)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- jjevwiw (PID: 6372 cmdline: C:\Users\user\AppData\Roaming\jjevwiw MD5: 36F662B3C9A54C0C2427602F1463EB69)
  - jjevwiw (PID: 6404 cmdline: C:\Users\user\AppData\Roaming\jjevwiw MD5: 36F662B3C9A54C0C2427602F1463EB69)
- jjevwiw (PID: 5852 cmdline: C:\Users\user\AppData\Roaming\jjevwiw MD5: 36F662B3C9A54C0C2427602F1463EB69)
  - jjevwiw (PID: 5868 cmdline: C:\Users\user\AppData\Roaming\jjevwiw MD5: 36F662B3C9A54C0C2427602F1463EB69)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader

```
{
  "C2 list": [
    "http://gejajoo7.top/",
    "http://sysaheu9.top/"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.376750362.000000000460000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000003.00000002.314233218.000000000680000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000003.00000002.314273302.00000000006A1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.296784154.00000000030C1000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000E.00000002.376904228.0000000001F51000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
28.0.jjevwiw.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
28.2.jjevwiw.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
28.1.jjevwiw.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
14.1.jjevwiw.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
27.2.jjevwiw.30815a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	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

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:

Yara detected SmokeLoader

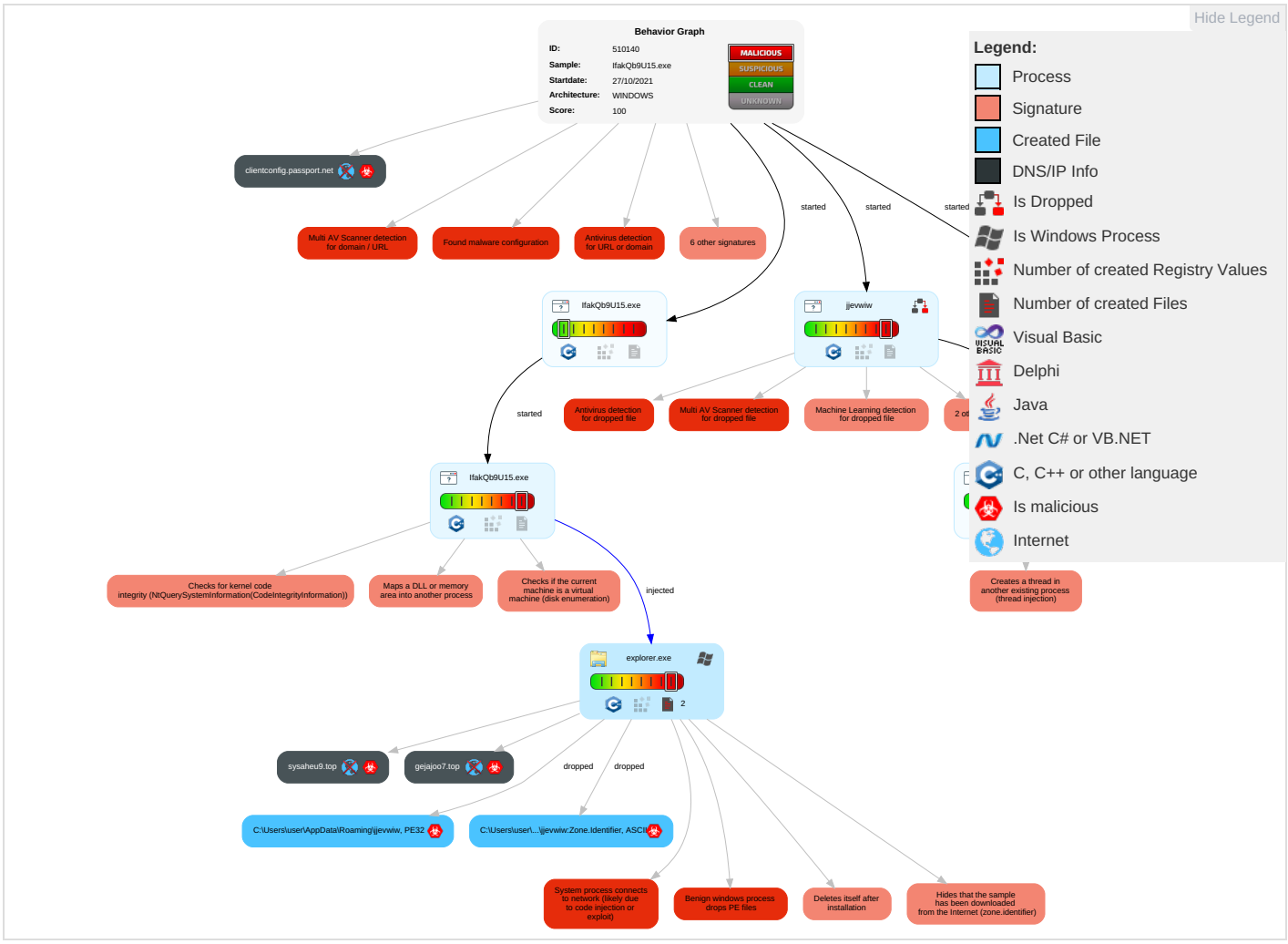
Remote Access Functionality:

Yara detected SmokeLoader

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	Exploitation for Client Execution 1	DLL Side-Loading 1	Process Injection 5 1 2	Masquerading 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Security Software Discovery 4 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Hidden Files and Directories 1	NTDS	Virtualization/Sandbox Evasion 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-I Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

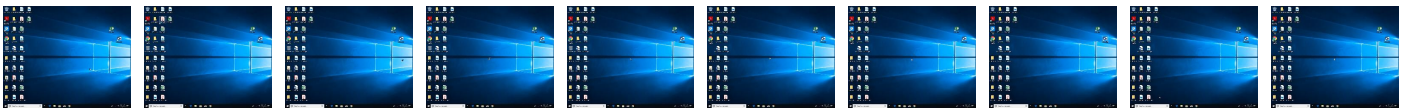
Behavior Graph



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
IfakQb9U15.exe	38%	Virustotal		Browse
IfakQb9U15.exe	75%	ReversingLabs	Win32.Ransomware.StopCrypt	
IfakQb9U15.exe	100%	Avira	TR/Redcap.yyhtm	
IfakQb9U15.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\jjevwiw	100%	Avira	TR/Redcap.yyhtm	
C:\Users\user\AppData\Roaming\jjevwiw	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\jjevwiw	75%	ReversingLabs	Win32.Ransomware.StopCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
28.2.jjevwiw.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.IfakQb9U15.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.jjevwiw.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.jjevwiw.400000.1.unpack	100%	Avira	TR/Redcap.yyhtm		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.IfakQb9U15.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.jjevwiw.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.jjevwiw.400000.0.unpack	100%	Avira	HEUR/AGEN.1124573		Download File
14.0.jjevwiw.400000.2.unpack	100%	Avira	TR/Redcap.yyhtm		Download File
14.2.jjevwiw.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.IfakQb9U15.exe.400000.0.unpack	100%	Avira	TR/Redcap.yyhtm		Download File
28.0.jjevwiw.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.jjevwiw.400000.0.unpack	100%	Avira	HEUR/AGEN.1124573		Download File
1.2.IfakQb9U15.exe.31415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.jjevwiw.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.jjevwiw.400000.3.unpack	100%	Avira	TR/Redcap.yyhtm		Download File
3.0.IfakQb9U15.exe.400000.1.unpack	100%	Avira	TR/Redcap.yyhtm		Download File
28.1.jjevwiw.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.jjevwiw.400000.0.unpack	100%	Avira	TR/Redcap.yyhtm		Download File
14.1.jjevwiw.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.jjevwiw.400000.0.unpack	100%	Avira	TR/Redcap.yyhtm		Download File
28.0.jjevwiw.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.jjevwiw.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.jjevwiw.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.IfakQb9U15.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1124573		Download File
3.0.IfakQb9U15.exe.400000.2.unpack	100%	Avira	TR/Redcap.yyhtm		Download File
3.0.IfakQb9U15.exe.400000.0.unpack	100%	Avira	TR/Redcap.yyhtm		Download File
3.0.IfakQb9U15.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.IfakQb9U15.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.jjevwiw.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.IfakQb9U15.exe.400000.3.unpack	100%	Avira	TR/Redcap.yyhtm		Download File
1.1.IfakQb9U15.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.1.jjevwiw.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.1.IfakQb9U15.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.1.jjevwiw.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.jjevwiw.4b215a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.jjevwiw.400000.0.unpack	100%	Avira	TR/Redcap.yyhtm		Download File
27.2.jjevwiw.30815a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.jjevwiw.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.jjevwiw.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
clientconfig.passport.net	0%	Virustotal		Browse
gejajoo7.top	10%	Virustotal		Browse
sysaheu9.top	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://gejajoo7.top/	0%	Avira URL Cloud	safe	
http://sysaheu9.top/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
clientconfig.passport.net	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
gejajoo7.top	unknown	unknown	true	• 10%, Virustotal, Browse	unknown
sysaheu9.top	unknown	unknown	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gejajoo7.top/	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://sysaheu9.top/	true	• Avira URL Cloud: malware	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510140
Start date:	27.10.2021
Start time:	14:07:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IfakQb9U15.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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/2@3/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 80.2% (good quality ratio 62.1%) • Quality average: 43.3% • Quality standard deviation: 31%
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
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:08:57	Task Scheduler	Run new task: Firefox Default Browser Agent 7A4EC823D5D4514B path: C:\Users\user\AppData\Roaming\jjevwiw

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\jjevwiw	cx6hZvW5HV.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Roaming\jjevwiw

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	189952
Entropy (8bit):	6.772121581791356
Encrypted:	false
SSDEEP:	3072:5+d4MmCHgQlJeblXMLQPAkilxUj3RMsOEd7lj/CrzeuVMO6P2+BwvHJ3/Rg:Ad4aHgaulXyQ4kicim9/C+ynVP
MD5:	36F662B3C9A54C0C2427602F1463EB69
SHA1:	7E46615097282AC51EF08D3E4AC7D65CE6684A07
SHA-256:	D836A03E0B7EEABBC971DE7D3E6FCC11BF06E13E633D11118C7429B3ABB3C4ED
SHA-512:	35B60C6DA50B94484A77F40C3446BEB1D5562128F5585731A09328140C68C7B57F1727CC0783B439DAFB5660C93CA1BD4E1C3F443261545AAA9B22C0DE9A1599
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 75%
Joe Sandbox View:	• Filename: cx6hZvW5HV.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L...b.u_.....p.....8'.....0....@.....@.....E.....m..<.....xi.....1.....0T..@.....0..x..... .....text...U..... ..`.rdata...E...0...F.....@..@.data....<.....d.....@....befifupr.....x.....@..@.rsrc...xi.....j...|.....@..@..... ....

C:\Users\user\AppData\Roaming\jjevwiw:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.772121581791356
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	IfakQb9U15.exe
File size:	189952
MD5:	36f662b3c9a54c0c2427602f1463eb69
SHA1:	7e46615097282ac51ef08d3e4ac7d65ce6684a07
SHA256:	d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed
SHA512:	35b60c6da50b94484a77f40c3446beb1d5562128f5585731a09328140c68c7b57f1727cc0783b439dafb5660c93ca1bd4e1c3f443261545aaa9b22c0de9a1599
SSDEEP:	3072:5+d4MmCHgQlJeblXMLQPAkilxUj3RMsOEd7lj/CrzeuVMO6P2+BwvHJ3/Rg:Ad4aHgaulXyQ4kicim9/C+ynVP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....PE..L...b.u_...

File Icon

Icon Hash:	b4fc36b6b694c6e2

Static PE Info

General

Entrypoint:	0x402738
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:	0x5F75D462 [Thu Oct 1 13:06:42 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
Subsystem Version Minor:	1
Import Hash:	fa148d0c70a978454538a9c9c0513fc1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x11955	0x11a00	False	0.791264960106	data	7.47772772393	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

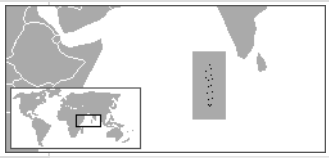
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x13000	0x45f8	0x4600	False	0.281026785714	data	4.05856795989	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x18000	0x2ac3cd0	0x1400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.befifup	0x2adc000	0x272	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2add000	0x16978	0x16a00	False	0.672792213398	data	6.40537973684	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
Divehi; Dhivehi; Maldivian	Maldives	
Bulgarian	Bulgaria	

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 27, 2021 14:08:02.449810028 CEST	192.168.2.5	8.8.8.8	0xc0dd	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)
Oct 27, 2021 14:08:56.076786041 CEST	192.168.2.5	8.8.8.8	0x5b0d	Standard query (0)	gejajoo7.top	A (IP address)	IN (0x0001)
Oct 27, 2021 14:08:56.113085985 CEST	192.168.2.5	8.8.8.8	0x93dc	Standard query (0)	sysaheu9.top	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 27, 2021 14:08:02.471621037 CEST	8.8.8.8	192.168.2.5	0xc0dd	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 14:08:56.096251965 CEST	8.8.8.8	192.168.2.5	0x5b0d	Name error (3)	gejajoo7.top	none	none	A (IP address)	IN (0x0001)
Oct 27, 2021 14:08:56.130479097 CEST	8.8.8.8	192.168.2.5	0x93dc	Name error (3)	sysaheu9.top	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: IfakQb9U15.exe PID: 4748 Parent PID: 5236

General

Start time:	14:08:06
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\IfakQb9U15.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IfakQb9U15.exe'
Imagebase:	0x400000
File size:	189952 bytes
MD5 hash:	36F662B3C9A54C0C2427602F1463EB69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: IfakQb9U15.exe PID: 2456 Parent PID: 4748

General

Start time:	14:08:12
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\IfakQb9U15.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IfakQb9U15.exe'
Imagebase:	0x400000
File size:	189952 bytes
MD5 hash:	36F662B3C9A54C0C2427602F1463EB69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.314233218.0000000000680000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.314273302.00000000006A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3472 Parent PID: 2456

General

Start time:	14:08:19
Start date:	27/10/2021

Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000005.00000000.296784154.00000000030C1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: jjevwiw PID: 6372 Parent PID: 904

General

Start time:	14:08:57
Start date:	27/10/2021
Path:	C:\Users\user\AppData\Roaming\jjevwiw
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jjevwiw
Imagebase:	0x400000
File size:	189952 bytes
MD5 hash:	36F662B3C9A54C0C2427602F1463EB69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 75%, ReversingLabs
Reputation:	low

Analysis Process: jjevwiw PID: 6404 Parent PID: 6372

General

Start time:	14:09:04
Start date:	27/10/2021
Path:	C:\Users\user\AppData\Roaming\jjevwiw
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jjevwiw
Imagebase:	0x400000
File size:	189952 bytes
MD5 hash:	36F662B3C9A54C0C2427602F1463EB69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000E.00000002.376750362.0000000000460000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000E.00000002.376904228.0000000001F51000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: jjevwiw PID: 5852 Parent PID: 904

General

Start time:	14:10:01
Start date:	27/10/2021
Path:	C:\Users\user\AppData\Roaming\jjevwiw
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jjevwiw
Imagebase:	0x400000
File size:	189952 bytes
MD5 hash:	36F662B3C9A54C0C2427602F1463EB69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: jjevwiw PID: 5868 Parent PID: 5852

General

Start time:	14:10:08
Start date:	27/10/2021
Path:	C:\Users\user\AppData\Roaming\jjevwiw
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jjevwiw
Imagebase:	0x400000
File size:	189952 bytes
MD5 hash:	36F662B3C9A54C0C2427602F1463EB69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis