



ID: 756298
Sample Name: file.exe
Cookbook: default.jbs
Time: 00:10:30
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: SmokeLoader 4
Yara Signatures 4
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
E-Banking Fraud 6
System Summary 6
Data Obfuscation 6
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
Anti Debugging 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 11
General Information 12
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Roaming\dwgvcre 13
C:\Users\user\AppData\Roaming\jdggfai 13
C:\Users\user\AppData\Roaming\jdggfai:Zone.Identifier 13
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 15
Rich Headers 16
Data Directories 16
Sections 16
Resources 16
Imports 17
Possible Origin 17
Network Behavior 17
Network Port Distribution 17

TCP Packets 18
UDP Packets 20
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 23
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: file.exePID: 6100, Parent PID: 3320 25
General 25
Analysis Process: explorer.exePID: 3320, Parent PID: 6100 25
General 25
File Activities 26
File Created 26
File Deleted 26
File Written 26
File Read 27
Analysis Process: jdggfaiPID: 5952, Parent PID: 1100 27
General 27
Analysis Process: explorer.exePID: 1372, Parent PID: 3320 27
General 27
Analysis Process: explorer.exePID: 4452, Parent PID: 3320 28
General 28
Analysis Process: explorer.exePID: 1836, Parent PID: 3320 28
General 28
Analysis Process: explorer.exePID: 4584, Parent PID: 3320 28
General 28
Analysis Process: explorer.exePID: 3852, Parent PID: 3320 29
General 29
Analysis Process: explorer.exePID: 2088, Parent PID: 3320 29
General 29
Analysis Process: explorer.exePID: 4800, Parent PID: 3320 29
General 29
Analysis Process: explorer.exePID: 1776, Parent PID: 3320 30
General 30
Analysis Process: explorer.exePID: 2464, Parent PID: 3320 30
General 30
Disassembly 30

Copyright Joe Security LLC 2022

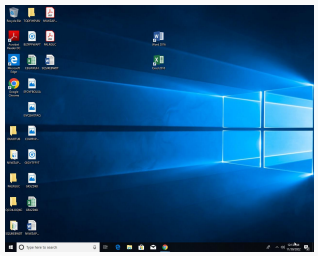
Windows Analysis Report

file.exe

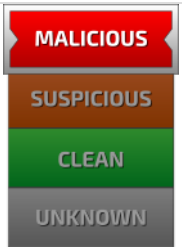
Overview

General Information

Sample Name:	file.exe
Analysis ID:	756298
MD5:	f39dbbcdcaac9c…
SHA1:	ab36da0a55feab..
SHA256:	12675d0f7c4a8d..
Tags:	exe
Infos:	



Detection



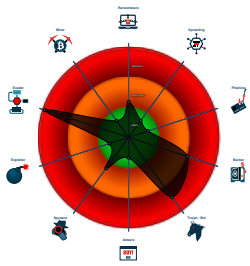
SmokeLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Maps a DLL or memory area into an…
- Found evasive API chain (may stop…
- Writes to foreign memory regions
- Checks if browser processes are run…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 6100 cmdline: C:\Users\user\Desktop\file.exe MD5: F39DBBCDCAAC9C8D2039B855C752C214)
  - explorer.exe (PID: 3320 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 1372 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 4452 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 1836 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 4584 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 3852 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 2088 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 4800 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 1776 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 2464 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- jdggfai (PID: 5952 cmdline: C:\Users\user\AppData\Roaming\jdggfai MD5: F39DBBCDCAAC9C8D2039B855C752C214)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://s2scomm20.com/",
    "http://c2csosi228d.com/",
    "http://xdd42sdfsdf.com/"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.407040058.0000000000748000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x4a28:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
0000000D.00000002.507736401.0000000000F41000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader	Yara detected SmokeLoader	Joe Security	
00000000.00000002.347095759.00000000020A1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000000.00000002.347095759.00000000020A1000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x374:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
0000000C.00000000.411589845.00000000009E0000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x34:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0

Click to see the 21 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.jdggfai.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
9.3.jdggfai.6f0000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.file.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.3.file.exe.5e0000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.file.exe.5d0e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Click to see the 1 entries

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

⊘ **No Snort rule has matched**

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

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

E-Banking Fraud



Checks if browser processes are running

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



Detected unpacking (changes PE section rights)

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



Found evasive API chain (may stop execution after checking mutex)

Contains functionality to compare user and computer (likely to detect sandboxes)

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

Writes to foreign memory regions

Injects code into the Windows Explorer (explorer.exe)

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information



Yara detected SmokeLoader

Remote Access Functionality



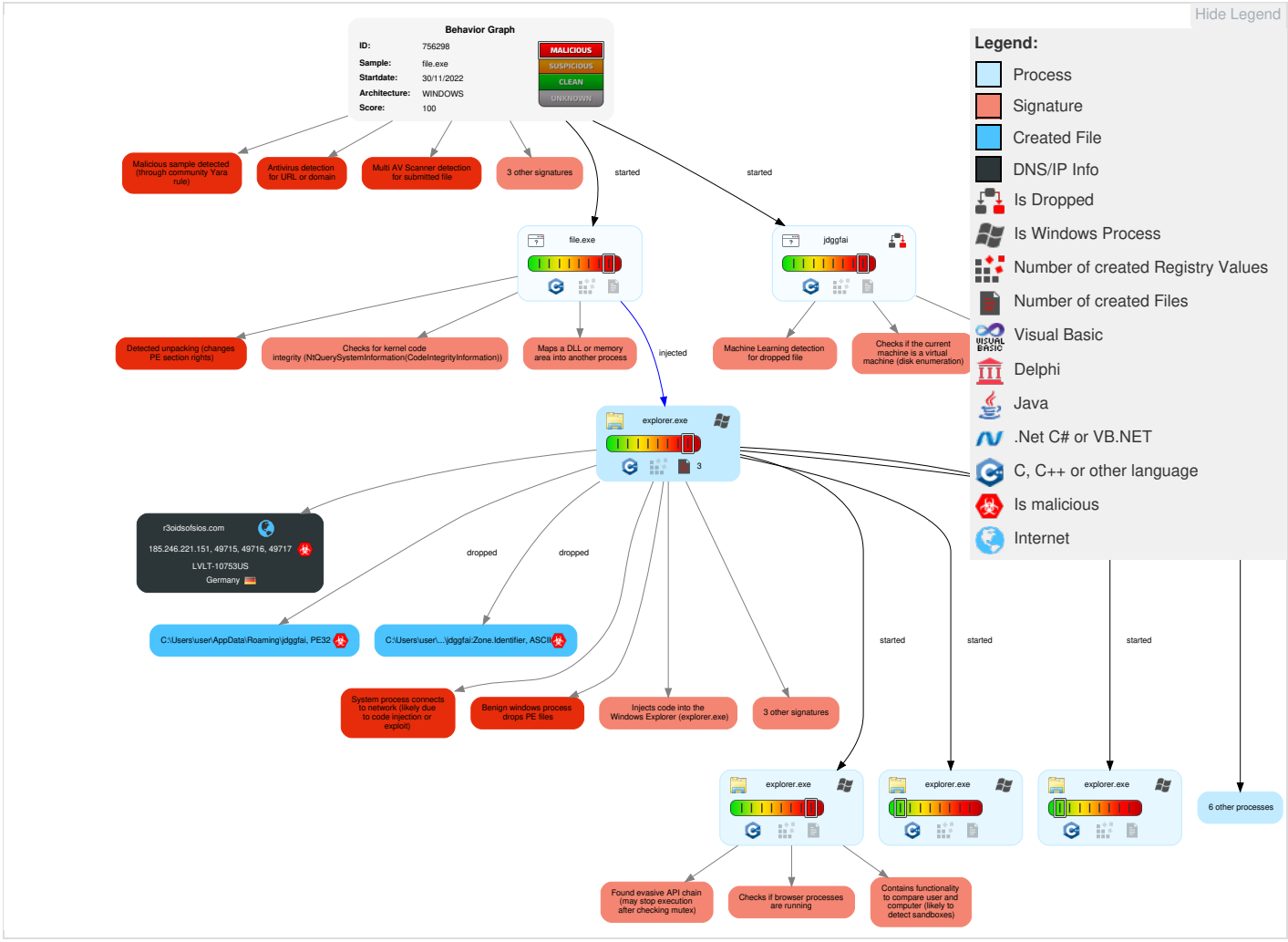
Yara detected SmokeLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	1 Exploitation for Client Execution	1 Create Account	5 1 3 Process Injection	2 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	1 5 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	3 5 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Masquerading	Cached Domain Credentials	1 3 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	5 1 3 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

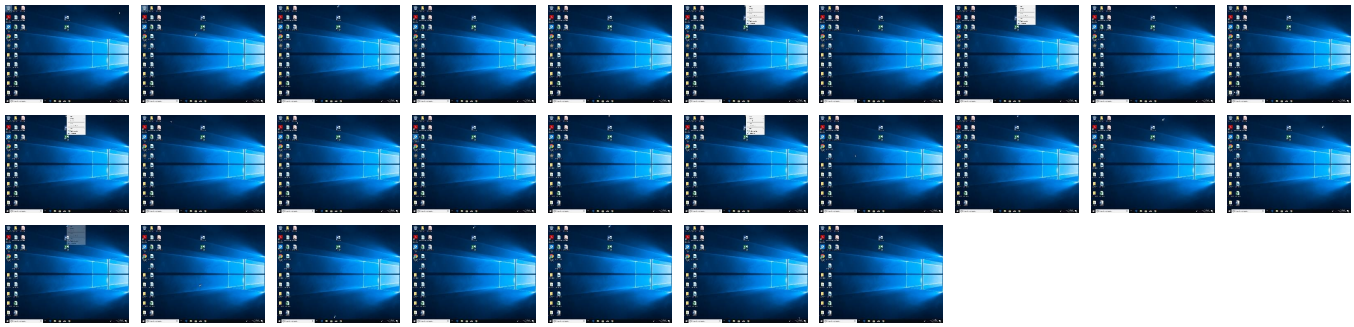
Behavior Graph



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
file.exe	34%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\jdggfai	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.file.exe.5d0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.jdggfai.6f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.jdggfai.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.file.exe.5e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
9.2.jdggfai.6d0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
r3oidsofsios.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://xdd42sdfsdf.com/	1%	Virustotal		Browse
http://s2scomm20.com/	1%	Virustotal		Browse
http://c2csosi228d.com/	1%	Virustotal		Browse
http://xdd42sdfsdf.com/	0%	Avira URL Cloud	safe	
http://s2scomm20.com/	0%	Avira URL Cloud	safe	
http://c2csosi228d.com/	100%	Avira URL Cloud	malware	
http://r3oidsofsios.com/Mozilla/5.0	0%	Avira URL Cloud	safe	
http://r3oidsofsios.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
r3oidsofsios.com	185.246.221.151	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

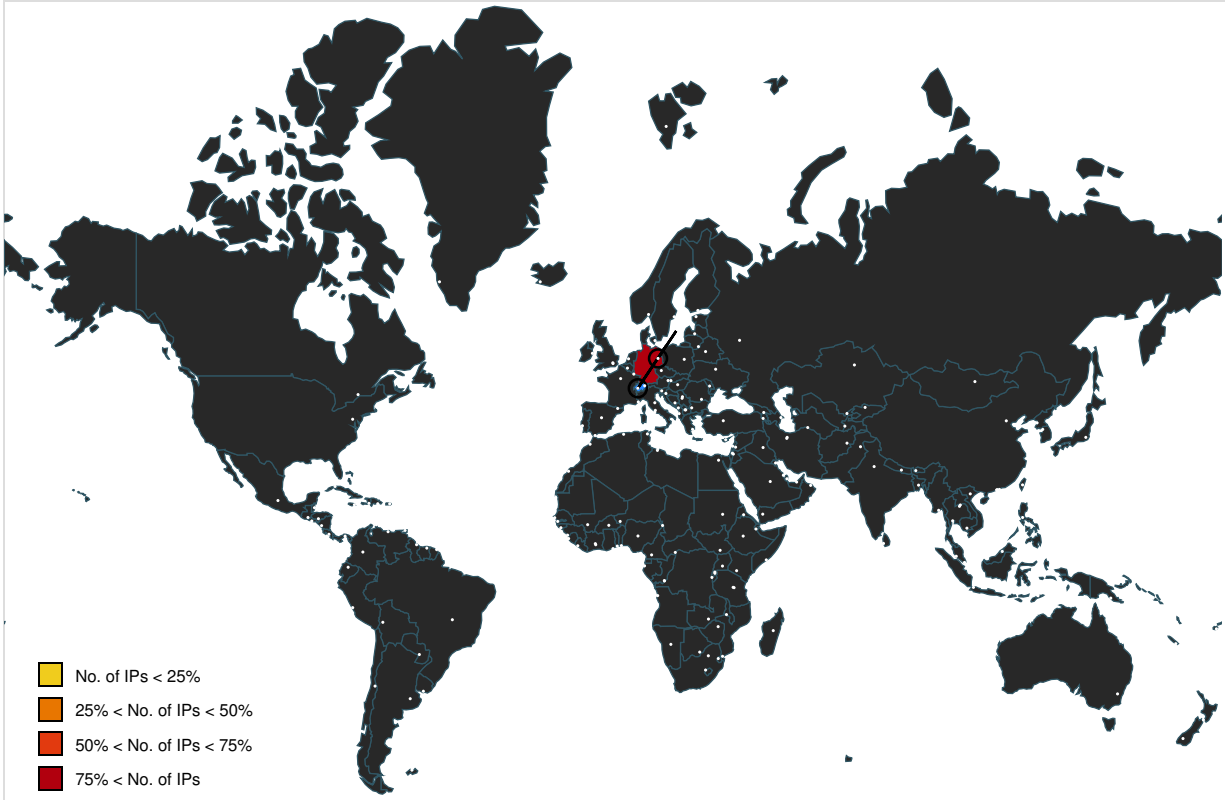
Name	Malicious	Antivirus Detection	Reputation
http://s2scomm20.com/	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://c2csosi228d.com/	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://xdd42sdfsdf.com/	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://r3oidsofsios.com/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://go.mail.ru/search	explorer.exe, explorer.exe, 0000000F.00000002.5078 50080.00000000031D1000.00000040.80000000 .00040000.00000000.sdmp	false		high
http://search.yahoo.com/search	explorer.exe, explorer.exe, 0000000F.00000002.5078 50080.00000000031D1000.00000040.80000000 .00040000.00000000.sdmp	false		high
http://www.google.com/search	explorer.exe, explorer.exe, 0000000F.00000002.5078 50080.00000000031D1000.00000040.80000000 .00040000.00000000.sdmp	false		high
http://nova.rambler.ru/search	explorer.exe, explorer.exe, 0000000F.00000002.5078 50080.00000000031D1000.00000040.80000000 .00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://r3oidsofsios.com/Mozilla/5.0	explorer.exe, 0000000A.00000000.40563187 4.0000000000CF0000.00000040.80000000.000 40000.00000000.sdmp, explorer.exe, 00000 00B.00000000.408629568.0000000000D20000. 00000040.80000000.00040000.00000000.sdmp, explorer.exe, 0000000B.00000002.508519891.000000 0001039000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000000C.0000 0000.411589845.00000000009E0000.00000040 .80000000.00040000.00000000.sdmp, explorer.exe, 0000000C.00000002.509151416.00000000032B70 00.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000D.00000000.414672467.000 0000000F50000.00000040.80000000.00040000 .00000000.sdmp, explorer.exe, 0000000D.0 0000002.508405258.0000000001268000.00000 004.00000020.00020000.00000000.sdmp, exp lorer.exe, 0000000F.00000000.420288650.0 0000000031E0000.00000040.80000000.000400 00.00000000.sdmp, explorer.exe, 00000010 .00000000.423035885.00000000007E0000.000 00040.80000000.00040000.00000000.sdmp, e xplorer.exe, 00000010.00000002.509492375 .0000000000C83000.00000004.00000020.0002 0000.00000000.sdmp, explorer.exe, 000000 11.00000002.508629995.0000000000CE8000.0 0000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000011.00000000.4258755 13.0000000000AE0000.00000040.80000000.00 040000.00000000.sdmp, explorer.exe, 0000 0014.00000000.428749130.0000000000580000 .00000040.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.aol.com/aol/search	explorer.exe, explorer.exe, 0000000F.00000002.5078 50080.00000000031D1000.00000040.80000000 .00040000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.246.221.151	r3oidsofsios.com	Germany		10753	LVLT-10753US	true

Copyright Joe Security LLC 2022

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756298
Start date and time:	2022-11-30 00:10:30 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
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.bank.troj.evad.winEXE@20/3@29/1
EGA Information:	• Successful, ratio: 90.9%
HDC Information:	• Successful, ratio: 40.1% (good quality ratio 29.4%) • Quality average: 41% • Quality standard deviation: 31.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target jdggfai, PID 5952 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
00:12:31	Task Scheduler	Run new task: Firefox Default Browser Agent 3F6E2A49B5A2019A path: C:\Users\user\AppData\Roaming\jdggfai
00:12:48	API Interceptor	329x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\dwgvcre

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	modified
Size (bytes):	160970
Entropy (8bit):	**7.998679399911187**
Encrypted:	**true**
SSDEEP:	3072:Ot6MQNn3XKprOPX+1zMkg7BWTHnMs18vGyMYzZQunMwvY:nN3XMrOv+1zMkg7BWTH1uNZQunbY
MD5:	3BCD6D6CA7F3787FB48CE0A6ACB9AC0F
SHA1:	99CC47E2A3229CC1F727AF36607932B562B8EC50
SHA-256:	39AB690FF5A0633B24065AF986D1DAE4995B57F056776B8BB638833A62FF5B06
SHA-512:	3CC89A6D55BF632283B2245B288500EFAA9FC75881AC005628971D0C691AA38A2D37F9F343EDC047794A3FD8EA843BF64E1F9302616DBD918BF2D79AF9D44AAD
Malicious:	false
Preview:	.2...%.....(.`..."........A~.g.....-.....|.-....S.R6g...zow?.-.,yE.....X..%....lJT.....~..M.Y..r....Qq.....s...`.....e....U.E.uSl..&WD..2...S.d&x...?#D.a...t...B.O<.....Y.}.'.A..N.A.{#I*A.yz...s.....M..1m.z.7~.u..*+.....&T.x...t....d$..0..x=.(x..It.n....K..*...>15....].G..I.n)+....[%..{:.D....j.].y.U../..i...r.x....h.....y.o.K??z.[v.....?l.0..q61..C...O..X.m..+...0.L.9!.N...G...J..`.\|..C>Y....W._-.^kY.K(....Y..h.F.0.0.d..\P**..{.p.=M,c,..%.}.F.....B.G..Q_24.a.y-.7{7@.Tq.X...,".F....[..HB.*....P.J....O;.....C....O.q.....7.+..._.....O\|.v.\.....&T..2.u..B..E..I.V.K.....8..+:.C..Y...m..O}..!E.D..g.....IVmv.y...3J....#.4I.W6..r.....;.X.H....jA..W..8F.$.0.dP..C.u..S.(wq....z..G.....F.6..R.Pa..0x.8."..VT|.....,[.]..a%*....ZB>B.^.(.....&...jpQ..m.+;T...E..b.7.&....U..=....Nxl#..u.!.Fe..Q.(.H.E`..&.y.".1.!ci.....Z.q....enB.....F.u^/.L..O<w..hQ...y.x..8.f.....rW?w.]..........n.L..'..WIR$+p.c....

C:\Users\user\AppData\Roaming\jdggfai

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	148992
Entropy (8bit):	7.085071601621051
Encrypted:	false
SSDEEP:	3072:MDxDtsHGGH2wUp5zjLf0+p+4vrtWhqyXV5G0pbCA:atuH2/jLfM4vr0quk0p/
MD5:	F39DBBCDCAAC9C8D2039B855C752C214
SHA1:	AB36DA0A55FEAB685587C52BCE5268FCA7EF0E23
SHA-256:	12675D0F7C4A8D729EDA453AD01697B0790F2921258E9BEFC54CF9327156AA10
SHA-512:	44419723FFBDF3CAF47FC0902AFD36BCCFE66AD60C150333FDA1EA62DA6410FBEBB805CCF61278CD95FD48F7BA23EDD06857050AB24D069AB6F3D2A8D1854BB0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.'.5.I.5.I.5.I....4.I.+...$.I.+...].I..]2.2.I.5.H.I.+.....I.+...4.I.+...4.I.Rich5.I.....PE..L.....a.....L..... ....@.....G>.....P....`..P0.....@.....<.....text..... ..`.data....?... .....@....rsrc...P0...`...2.....@..@.....

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

Process:	C:\Windows\explorer.exe

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.085071601621051
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:	file.exe
File size:	148992
MD5:	f39dbbcdcaac9c8d2039b855c752c214
SHA1:	ab36da0a55feab685587c52bce5268fca7ef0e23
SHA256:	12675d0f7c4a8d729eda453ad01697b0790f2921258e9befc54cf9327156aa10
SHA512:	44419723ffbdf3caf47fc0902afd36bccfe66ad60c150333fda1ea62da6410fbebb805ccf61278cd95fd48f7ba23edd06857050ab24d069ab6f3d2a8d1854bb0
SSDEEP:	3072:MDxDtsHGGH2wUp5zjLf0+p+4vrtWhqyXV5G0pbCA:atuH2/jLfM4vr0quk0p/
TLSH:	40E3DF157291D033E79794315925C3A26BFAF93228B4C94BB7480B7E4FB12D1BA2B307
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.'.5.I.5.I.5.I.....4.I.+...$.I.+...].I..]2.2.I.5.H...I.+.....I.+...4.I.+...4.I.Rich5.I.....PE..L.....a.....

File Icon



Icon Hash:	d4b4b0e8e0eaf0c0

Static PE Info

General

Entrypoint:	0x404c97
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x6183E2E1 [Thu Nov 4 13:40:49 2021 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:	2ac0f7085258eff31142b9f87cb0f218

Entrypoint Preview
Instruction
call 00007FF368B207BCh
jmp 00007FF368B1A99Dh
sub eax, 000003A4h
je 00007FF368B1AB44h
sub eax, 04h
je 00007FF368B1AB39h
sub eax, 0Dh
je 00007FF368B1AB2Eh
dec eax
je 00007FF368B1AB25h
xor eax, eax
ret
mov eax, 00000404h
ret
mov eax, 00000412h
ret
mov eax, 00000804h
ret
mov eax, 00000411h
ret
mov edi, edi
push esi
push edi
mov esi, eax
push 00000101h
xor edi, edi
lea eax, dword ptr [esi+1Ch]
push edi
push eax
call 00007FF368B1BD2Eh
xor eax, eax
movzx ecx, ax
mov eax, ecx
mov dword ptr [esi+04h], edi
mov dword ptr [esi+08h], edi
mov dword ptr [esi+0Ch], edi
shl ecx, 10h
or eax, ecx
lea edi, dword ptr [esi+10h]
stosd
stosd
stosd
mov ecx, 00421658h
add esp, 0Ch
lea eax, dword ptr [esi+1Ch]
sub ecx, esi
mov edi, 00000101h
mov dl, byte ptr [ecx+eax]
mov byte ptr [eax], dl
inc eax
dec edi
jne 00007FF368B1AB19h
lea eax, dword ptr [esi+0000011Dh]
mov esi, 00000100h
mov dl, byte ptr [eax+ecx]
mov byte ptr [eax], dl

Instruction
inc eax
dec esi
jne 00007FF368B1AB19h
pop edi
pop esi
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 0000051Ch
mov eax, dword ptr [00422260h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
push edi
lea eax, dword ptr [ebp-00000518h]
push eax
push dword ptr [esi+04h]
call dword ptr [00401170h]
mov edi, 00000100h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10a9c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x56000	0x3050	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1280	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2cd8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x23c	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x107d4	0x10800	False	0.511911103219697	data	6.098461593221709	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x12000	0x43f08	0x10800	False	0.9390536221590909	data	7.820995800308699	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x56000	0x3050	0x3200	False	0.62859375	data	5.655023153247635	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
JEBOPOZUSUHARAFA	0x58430	0x55f	ASCII text, with very long lines (1375), with no line terminators	Raeto-Romance	Switzerland
RT_ICON	0x562b0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x56978	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x56ee0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x57f88	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Raeto-Romance	Switzerland
RT_STRING	0x58b78	0x2d8	data	Raeto-Romance	Switzerland
RT_STRING	0x58e50	0x1fc	data	Raeto-Romance	Switzerland
RT_ACCELERATOR	0x58990	0xa0	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0x583f0	0x3e	data	Raeto-Romance	Switzerland
RT_VERSION	0x58a30	0x148	x86 executable not stripped		

Imports

DLL	Import
KERNEL32.dll	OpenMutexW, GetConsoleAliasExesLengthA, CopyFileExA, ReadConsoleOutputCharacterW, CompareStringW, SetVolumeLabelA, FillConsoleOutputAttribute, GetConsoleTitleA, QueryDosDeviceW, EnumCalendarInfoExA, GetProcessPriorityBoost, IsProcessInJob, AddConsoleAliasW, CreateFileW, SetMailslotInfo, GetWindowsDirectoryW, GetModuleHandleA, GlobalLock, CreateDirectoryExW, GetLogicalDriveStringsA, ReadConsoleInputA, FindNextVolumeMountPointW, OpenWaitableTimerA, GetVersionExA, SearchPathA, MoveFileExW, CallNamedPipeW, GetCurrentDirectoryW, GetDriveTypeA, CreateMailslotA, BuildCommDCBAndTimeoutsA, GetProcAddress, LoadLibraryA, LocalAlloc, GetBinaryTypeA, GetCPInfoExW, WriteConsoleOutputA, GetCommandLineA, EnumDateFormatsW, CancelTimerQueueTimer, GetHandleInformation, FindResourceA, CreateJobObjectA, FindFirstVolumeA, GlobalFlags, CreateNamedPipeW, InterlockedIncrement, CloseHandle, CopyFileW, GetComputerNameExA, GetShortPathNameA, FlushFileBuffers, GetLogicalDriveStringsW, InterlockedCompareExchange, EnumCalendarInfoW, GetConsoleAliasExesLengthW, InterlockedExchange, GetNamedPipeHandleStateW, GetModuleHandleW, GetCurrentActCtx, GenerateConsoleCtrlEvent, MoveFileW, AddAtomA, SetThreadPriority, FreeEnvironmentStringsW, SetConsoleTitleW, SetVolumeMountPointW, VirtualAlloc, _hread, EnumResourceLanguagesW, ClearCommBreak, QueryMemoryResourceNotification, GlobalFindAtomA, HeapWalk, SetFilePointer, GetTickCount, EnumSystemCodePagesW, VerifyVersionInfoA, LoadLibraryW, CreateFileA, GetLastError, WideCharToMultiByte, HeapReAlloc, HeapAlloc, HeapFree, UnhandledExceptionFilter, SetUnhandledExceptionFilter, DeleteFileA, GetStartupInfoA, GetCPInfo, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, TerminateProcess, GetCurrentProcess, IsDebuggerPresent, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, HeapCreate, VirtualFree, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, SetStdHandle, GetConsoleCP, GetConsoleMode, RtlUnwind, InitializeCriticalSectionAndSpinCount, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, HeapSize, ReadFile
GDI32.dll	GetCharWidthA, GetCharABCWidthsA
WINHTTP.dll	WinHttpSetOption

Possible Origin

Language of compilation system	Country where language is spoken	Map
Raeto-Romance	Switzerland	

Network Behavior

Network Port Distribution

Total Packets: 62

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:12:31.871395111 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:31.898896933 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:31.899008989 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:31.899173021 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:31.899214029 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:31.927711964 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.019617081 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.019654036 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.019699097 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.019731998 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.019763947 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.019814014 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.019828081 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.019865036 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.019881010 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.019922972 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.019973040 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.020023108 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.020193100 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.020194054 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.020194054 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.049228907 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.049278021 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.049432039 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.063112974 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063162088 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063194990 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063226938 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063270092 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063287973 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.063287973 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.063322067 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063375950 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063420057 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063424110 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.063476086 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063510895 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.063527107 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063576937 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.063594103 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.077265978 CET	80	49715	185.246.221.151	192.168.2.7

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:12:32.077397108 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.103285074 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.103332996 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.103414059 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.103981018 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.104018927 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.104049921 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.104083061 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.104089022 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.104115009 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.104135990 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.104149103 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.104181051 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.104212999 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.104257107 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.104283094 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.104289055 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.104435921 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.105029106 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.153188944 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.167846918 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.167993069 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168015003 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168034077 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168060064 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168078899 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168123960 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.168191910 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.168214083 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168236017 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168257952 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168283939 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168302059 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168308973 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.168322086 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.168344021 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.168376923 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.183612108 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.187916040 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.187942982 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.187997103 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.188143015 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.188165903 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.188286066 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.189188957 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.189212084 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.189233065 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.189255953 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.189276934 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.189282894 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.189299107 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.189321995 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.189342976 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.189347029 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.189364910 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.189372063 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.189450026 CET	49715	80	192.168.2.7	185.246.221.151
Nov 30, 2022 00:12:32.195622921 CET	80	49715	185.246.221.151	192.168.2.7
Nov 30, 2022 00:12:32.238928080 CET	80	49715	185.246.221.151	192.168.2.7

Copyright Joe Security LLC 2022

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:12:31.576731920 CET	51007	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:31.867197037 CET	53	51007	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:32.519501925 CET	50513	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:32.811173916 CET	53	50513	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:33.003753901 CET	60765	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:33.028825998 CET	53	60765	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:33.193178892 CET	58283	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:33.212548971 CET	53	58283	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:33.470622063 CET	50024	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:33.821990967 CET	53	50024	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:34.020052910 CET	49516	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:34.036792994 CET	53	49516	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:34.196407080 CET	62679	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:34.488857985 CET	53	62679	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:34.650456905 CET	61392	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:34.669634104 CET	53	61392	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:34.832746983 CET	52104	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:34.851197958 CET	53	52104	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:35.027832985 CET	65356	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:35.319250107 CET	53	65356	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:35.475203037 CET	59006	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:35.494378090 CET	53	59006	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:35.653045893 CET	51526	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:35.672054052 CET	53	51526	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:35.851425886 CET	51139	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:35.871113062 CET	53	51139	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:36.038981915 CET	58784	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:36.067956924 CET	53	58784	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:36.250511885 CET	57970	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:36.359834909 CET	53	57970	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:36.525525093 CET	64608	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:36.543272018 CET	53	64608	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:36.705869913 CET	58746	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:36.996306896 CET	53	58746	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:37.164571047 CET	62433	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:37.183329105 CET	53	62433	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:37.352591038 CET	61248	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:37.373538971 CET	53	61248	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:37.531023026 CET	52750	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:37.549065113 CET	53	52750	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:37.720558882 CET	64078	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:37.750535965 CET	53	64078	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:37.949290991 CET	50231	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:37.969152927 CET	53	50231	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:38.138925076 CET	58514	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:38.158756018 CET	53	58514	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:38.340357065 CET	51436	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:38.360474110 CET	53	51436	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:38.756226063 CET	59053	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:38.774048090 CET	53	59053	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:38.983336926 CET	51945	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:39.002141953 CET	53	51945	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:39.224884987 CET	63187	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:39.242450953 CET	53	63187	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:39.508954048 CET	64760	53	192.168.2.7	8.8.8.8
Nov 30, 2022 00:12:39.526495934 CET	53	64760	8.8.8.8	192.168.2.7
Nov 30, 2022 00:12:40.331233978 CET	53637	53	192.168.2.7	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:12:40.349824905 CET	53	53637	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:12:31.576731920 CET	192.168.2.7	8.8.8.8	0xe620	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:32.519501925 CET	192.168.2.7	8.8.8.8	0x9a00	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:33.003753901 CET	192.168.2.7	8.8.8.8	0xcb73	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:33.193178892 CET	192.168.2.7	8.8.8.8	0xd2b9	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:33.470622063 CET	192.168.2.7	8.8.8.8	0xd702	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:34.020052910 CET	192.168.2.7	8.8.8.8	0xde7c	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:34.196407080 CET	192.168.2.7	8.8.8.8	0x80e4	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:34.650456905 CET	192.168.2.7	8.8.8.8	0x2609	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:34.832746983 CET	192.168.2.7	8.8.8.8	0xbf35	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:35.027832985 CET	192.168.2.7	8.8.8.8	0x883f	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:35.475203037 CET	192.168.2.7	8.8.8.8	0xef7	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:35.653045893 CET	192.168.2.7	8.8.8.8	0x7e44	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:35.851425886 CET	192.168.2.7	8.8.8.8	0xb4f1	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:36.038981915 CET	192.168.2.7	8.8.8.8	0x6dd1	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:36.250511885 CET	192.168.2.7	8.8.8.8	0x8b45	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:36.525525093 CET	192.168.2.7	8.8.8.8	0x7568	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:36.705869913 CET	192.168.2.7	8.8.8.8	0x4443	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:37.164571047 CET	192.168.2.7	8.8.8.8	0xc6d7	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:37.352591038 CET	192.168.2.7	8.8.8.8	0x2915	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:37.531023026 CET	192.168.2.7	8.8.8.8	0x8766	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:37.720558882 CET	192.168.2.7	8.8.8.8	0xdb37	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:37.949290991 CET	192.168.2.7	8.8.8.8	0x67f0	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:38.138925076 CET	192.168.2.7	8.8.8.8	0xebc7	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:38.340357065 CET	192.168.2.7	8.8.8.8	0xb147	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:38.756226063 CET	192.168.2.7	8.8.8.8	0x39bd	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:38.983336926 CET	192.168.2.7	8.8.8.8	0xccea	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:39.224884987 CET	192.168.2.7	8.8.8.8	0x2155	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:39.508954048 CET	192.168.2.7	8.8.8.8	0xa014	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:40.331233978 CET	192.168.2.7	8.8.8.8	0xec7a	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false

DNS Answers

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:12:31.867197037 CET	8.8.8.8	192.168.2.7	0xe620	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:32.811173916 CET	8.8.8.8	192.168.2.7	0x9a00	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:33.028825998 CET	8.8.8.8	192.168.2.7	0xcb73	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:33.212548971 CET	8.8.8.8	192.168.2.7	0xd2b9	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:33.821990967 CET	8.8.8.8	192.168.2.7	0xd702	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:34.036792994 CET	8.8.8.8	192.168.2.7	0xde7c	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:34.488857985 CET	8.8.8.8	192.168.2.7	0x80e4	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:34.669634104 CET	8.8.8.8	192.168.2.7	0x2609	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:34.851197958 CET	8.8.8.8	192.168.2.7	0xbf35	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:35.319250107 CET	8.8.8.8	192.168.2.7	0x883f	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:35.494378090 CET	8.8.8.8	192.168.2.7	0xef7	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:35.672054052 CET	8.8.8.8	192.168.2.7	0x7e44	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:35.871113062 CET	8.8.8.8	192.168.2.7	0xb4f1	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:36.067956924 CET	8.8.8.8	192.168.2.7	0x6dd1	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:36.359834909 CET	8.8.8.8	192.168.2.7	0x8b45	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:36.543272018 CET	8.8.8.8	192.168.2.7	0x7568	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:36.996306896 CET	8.8.8.8	192.168.2.7	0x4443	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:37.183329105 CET	8.8.8.8	192.168.2.7	0xc6d7	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:37.373538971 CET	8.8.8.8	192.168.2.7	0x2915	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:37.549065113 CET	8.8.8.8	192.168.2.7	0x8766	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:37.750535965 CET	8.8.8.8	192.168.2.7	0xdb37	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:37.969152927 CET	8.8.8.8	192.168.2.7	0x67f0	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:38.158756018 CET	8.8.8.8	192.168.2.7	0xebc7	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:38.360474110 CET	8.8.8.8	192.168.2.7	0xb147	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:38.774048090 CET	8.8.8.8	192.168.2.7	0x39bd	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:12:39.002141953 CET	8.8.8.8	192.168.2.7	0xccea	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:39.242450953 CET	8.8.8.8	192.168.2.7	0x2155	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:39.526495934 CET	8.8.8.8	192.168.2.7	0xa014	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:40.349824905 CET	8.8.8.8	192.168.2.7	0xec7a	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- kqgkblakc.com
  - r3oidsofsios.com
- ryjwkat.net
- ewfonmrybp.org
- hraesy.net
- vqnwxa.org
- sqyiaue.net
- cygghp.com
- dtxwodx.net
- wypuksbjb.org
- qgjuekrsef.net
- rlovsbdvn.net
- ugjjaam.net
- poflgkd.org
- vshacsl.org
- kabjenh.com
- vyukg.com
- xnfwjbsuvp.com
- nvftibg.com
- okade.org
- iungf.org
- bhqtkqlvvb.org
- whvkq.com
- rspyhp.net
- jvjyarecuw.net
- hrxqxa.net
- uwoxt.net
- bqruytosp.com
- lclth.com
- vreqndf.com

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **6100**, Parent PID: **3320**

General

Target ID:	0
Start time:	00:11:25
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	148992 bytes
MD5 hash:	F39DBBCDCAAC9C8D2039B855C752C214
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: 00000000.00000002.347095759.00000000020A1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.347095759.00000000020A1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.346601770.00000000005D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.346812958.000000000060A000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.346666685.00000000005E0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.346666685.00000000005E0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000003.245341240.00000000005E0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: **3320**, Parent PID: **6100**

General

Target ID:	1
Start time:	00:11:32

Copyright Joe Security LLC 2022

Start date:	30/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff75ed40000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000000.338708718.0000000002661000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.338708718.0000000002661000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jdggfai	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device | compressed	sequential only | non directory file	success or wait	1	266204A	CopyFileW
C:\Users\user\AppData\Roaming\jdggfai\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device | compressed	sequential only | synchronous io non alert	success or wait	1	266204A	CopyFileW
C:\Users\user\AppData\Roaming\dwgvcre	read attributes | synchronize | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	26625C9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	success or wait	1	266205B	DeleteFileW
C:\Users\user\AppData\Roaming\jdggfai:Zone.Identifier	success or wait	1	26620A6	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jdggfai	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jdggfai:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	266204A	CopyFileW
C:\Users\user\AppData\Roaming\dwgvcre	0	160970	16 32 fd 0c fd 25 fd fd e9 f8 fd 28 fd 60 09 fd fd 22 fd fd fd fd 14 39 fd fd 41 7e fd 67 fd fd fd 0f fd fd 2d fd fd 1f fd fd fd fd 7c fd 2d 0d fd 13 19 53 8c 52 36 67 fd fd 0b 7a 6f 77 3f fd 2d fd 2c 79 45 fd fd fd fd fd 1f 58 0a fd 25 58 fd fd fd 49 4a 54 fd 19 bd fd fd 7e 1d fd 4d fd 59 fd fd 72 a9 fd fd 2e 51 71 fd fd fd fd 0f 73 fd fd fd 60 fd fd fd fd fd 65 fd fd 09 fd 55 fd 45 fd 75 53 6c fd 1a 26 57 44 fd fd 32 fd fd 2a 53 fd 64 26 78 fd fd fd 3f 23 44 fd 61 fd fd fd 74 fd fd fd 42 fd 4f 3c fd fd fd ae 04 fd 59 1e 7d fd 27 fd 41 1b fd 4e 0f 41 fd 7b 23 49 2a 41 fd 79 7a fd fd fd 73 06 fd fd fd 4d 06 7f 31 6d fd 7a fd 37 7e 02 75 fd fd 2a 2b fd fd fd fd 11 fd 26 54 1b 78 fd fd fd 74 10	2%(`"A~g-|-SR6gzow?-,yEX%lJT~M YrQqs`eUEuSl&WD2Sd& x?#DatBO<Y} 'ANA{#I*AyzsM1mz7~u*+ &Txt	success or wait	1	266262A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dwgvcre	unknown	160970	success or wait	1	26634E3	ReadFile

Analysis Process: jdggfai PID: **5952**, Parent PID: **1100**

General

Target ID:	9
Start time:	00:12:31
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Roaming\jdggfai
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jdggfai
Imagebase:	0x400000
File size:	148992 bytes
MD5 hash:	F39DBBCDCAAC9C8D2039B855C752C214
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000009.00000002.407040058.0000000000748000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000009.00000002.406829127.0000000000700000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000009.00000002.406829127.0000000000700000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000009.00000003.388354905.00000000006F0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000009.00000002.406779661.00000000006D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000009.00000002.407192385.00000000020D1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000009.00000002.407192385.00000000020D1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: explorer.exe PID: **1372**, Parent PID: **3320**

General

Target ID:	10
Start time:	00:12:40
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xd70000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000A.00000000.405631874.0000000000CF0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

Analysis Process: explorer.exe PID: **4452**, Parent PID: **3320**

General

Target ID:	11
Start time:	00:12:43
Start date:	30/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff75ed40000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **1836**, Parent PID: **3320**

General

Target ID:	12
Start time:	00:12:44
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xd70000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000C.00000000.411589845.00000000009E0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 0000000C.00000002.507826700.00000000009D1000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: explorer.exe PID: **4584**, Parent PID: **3320**

General

Target ID:	13
Start time:	00:12:46
Start date:	30/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff75ed40000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.507736401.0000000000F41000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: explorer.exe PID: **3852**, Parent PID: **3320**

General

Target ID:	14
Start time:	00:12:47
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xd70000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000E.00000000.417608043.00000000003D0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

Analysis Process: explorer.exe PID: **2088**, Parent PID: **3320**

General

Target ID:	15
Start time:	00:12:49
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xd70000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000F.00000000.420288650.00000000031E0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: explorer.exe PID: **4800**, Parent PID: **3320**

General

Target ID:	16

Start time:	00:12:50
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xd70000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000010.00000000.423035885.00000000007E0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: explorer.exe PID: **1776**, Parent PID: **3320**

General	
Target ID:	17
Start time:	00:12:51
Start date:	30/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff75ed40000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **2464**, Parent PID: **3320**

General	
Target ID:	20
Start time:	00:12:52
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xd70000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000014.00000000.428749130.0000000000580000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Disassembly

No disassembly