ID: 411858
Sample Name: shipping Document and Bill Of Landing.exe
Cookbook: default.jbs
Time: 08:00:38
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Analysis Report shipping Document and Bill Of Landing…

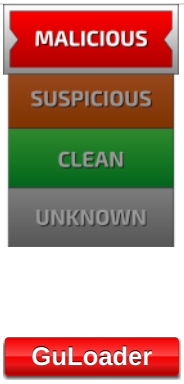
Overview

General Information

Sample Name:	shipping Document and Bill Of Landing.exe
Analysis ID:	411858
MD5:	7196e6e67a3922..
SHA1:	c0da8d54393e93..
SHA256:	4d5e7bff4f749a4…
Tags:	GuLoader
Infos:	

Most interesting Screenshot:

Detection

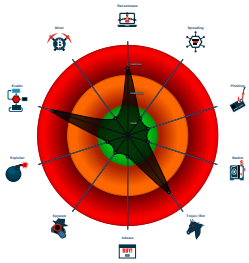


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Executable has a suspicious name (…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Tries to detect Any.run

Classification



Startup

- **System is w10x64**
- shipping Document and Bill Of Landing.exe (PID: 672 cmdline: 'C:\Users\user\Desktop\shipping Document and Bill Of Landing.exe' MD5: 7196E6E67A39225A9B73AF0C6F6B5B0E)
  - shipping Document and Bill Of Landing.exe (PID: 204 cmdline: 'C:\Users\user\Desktop\shipping Document and Bill Of Landing.exe' MD5: 7196E6E67A39225A9B73AF0C6F6B5B0E)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://reachglobal-in.com/fdeb/bin_dXfiGRj156.bin"
}
```


Yara Overview

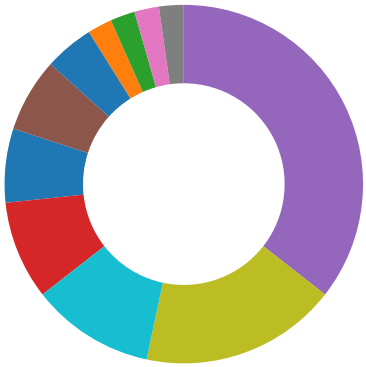
Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.469283991.000000000056 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000002.296439672.000000000229 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

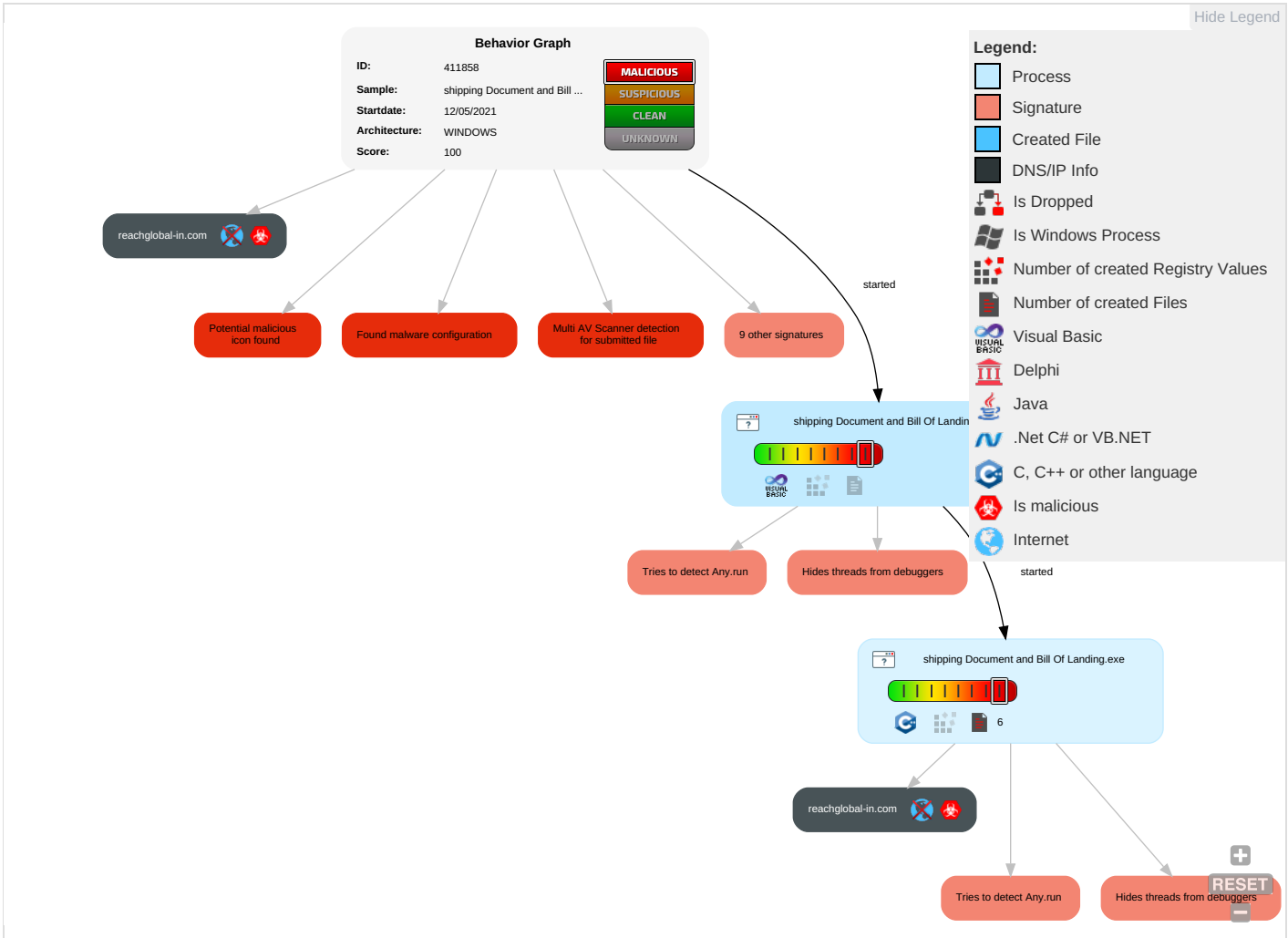
Anti Debugging:

Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Virtualization/Sandbox Evasion 2 1	OS Credential Dumping	Security Software Discovery 6 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
shipping Document and Bill Of Landing.exe	52%	Virustotal		Browse
shipping Document and Bill Of Landing.exe	30%	ReversingLabs	Win32.Trojan.Vebzenpak	
shipping Document and Bill Of Landing.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://https://reachglobal-in.com/fdeb/bin_dXfiGRj156.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
reachglobal-in.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://reachglobal-in.com/fdeb/bin_dXfiGRj156.bin	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411858
Start date:	12.05.2021
Start time:	08:00:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	shipping Document and Bill Of Landing.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:	33
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.rans.troj.evad.winEXE@3/0@43/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7% (good quality ratio 3.2%) • Quality average: 26.4% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 73% • 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 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 92.122.145.220, 104.43.193.48, 168.61.161.212, 13.64.90.137, 23.218.208.56, 20.82.209.183, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.954249338916242
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	shipping Document and Bill Of Landing.exe
File size:	192512
MD5:	7196e6e67a39225a9b73af0c6f6b5b0e
SHA1:	c0da8d54393e9365d1fa0f0a88cf4b52496992b1
SHA256:	4d5e7bff4f749a4f1a357c61098c19c345246b142308f4048aebc6dfdaf4fc73
SHA512:	d977f3ef74715984e3d1f536975a8ab0a361724f2303305abcf6e14895461ef2288096c0f05be69c84656c9cb8eebc51b586e5f38119bae0507102fc1c7209f7
SSDEEP:	3072:OTqw9SpYljV4Swtm3hdcIYZKZEXaXk/L:OTqw9PSukCKZKaU/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....M.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401ccc
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4DE4F581 [Tue May 31 14:04:49 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	3af66fbc6abd133270fa3848991f9c33

Entrypoint Preview

Instruction
push 0041222Ch
call 00007FDABCAC72C3h
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ebx], al
pushad
in eax, dx
fcom dword ptr [ecx-64B32A36h]
test dword ptr [edi+3Ah], eax
mov edx, esi
and eax, 0000000Fh
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edx+00h], al
push es
push eax
add dword ptr [ecx], 41h
insd
je 00007FDABCAC734Ch
jnc 00007FDABCAC7346h
jc 00007FDABCAC7307h
add byte ptr [eax], al
mov ah, 28h
or eax, 00000003h
add bh, bh
int3
xor dword ptr [eax], eax
or al, FDh
salc
cmp eax, ebx
call 00007FDA3DEF2BDDh
sbb dh, ch
jmp far 1A55h : 7BB8AF0Bh
cld
mov edx, 44E62D63h
mov ebp, BC1E9B46h
dec ebp
and byte ptr [edx], al
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
pop esp
add al, 01h
add byte ptr [edx+02h], ch
add dword ptr [eax], eax
add byte ptr [ecx], cl
add byte ptr [edi+68h], dh
insb
jc 00007FDABCAC7346h
add byte ptr [43000501h], cl
outsd
outsd
jo 00007FDABCAC7307h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2bc74	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2f000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x140	.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	0x2b200	0x2c000	False	0.31094082919	data	6.14682442454	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2d000	0x11f4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2f000	0x900	0x1000	False	0.16650390625	data	1.96156765674	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2f7d0	0x130	data		
RT_ICON	0x2f4e8	0x2e8	data		
RT_ICON	0x2f3c0	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x2f390	0x30	data		
RT_VERSION	0x2f150	0x240	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaStrCat, __vbaSetSystemError, __vbaRecDestruct, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRecUniToAnsi, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaStrToAnsi, __vbaFpI4, __vbaRecDestructAnsi, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	The
FileVersion	1.00
CompanyName	Origin! CAD
ProductName	Origin! CAD
ProductVersion	1.00
FileDescription	Origin!
OriginalFilename	The.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-08:02:35.204329	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:02:36.222464	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:02:37.240826	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:02:40.491414	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:02:41.527466	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:02:46.372764	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:02:50.638500	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:02:51.639741	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:02:55.687460	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:02:56.734923	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:00.783150	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:02.811944	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:05.906613	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:06.938617	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:11.031996	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:12.079577	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:16.126441	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:17.141343	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:19.140188	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:22.289451	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:23.327932	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-08:03:25.321499	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:27.403886	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:28.393190	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:33.424666	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-08:03:34.472475	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 08:01:19.031388044 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:19.080117941 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 08:01:20.157840967 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:20.225888968 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 08:01:22.002157927 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:22.053714037 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 08:01:22.813426971 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:22.865047932 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 08:01:24.007102966 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:24.055876970 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 08:01:25.481729031 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:25.539752007 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 08:01:26.385723114 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:26.437232018 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 08:01:27.526230097 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:27.575057030 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 08:01:28.726255894 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:28.778234005 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 08:01:30.069235086 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:30.118036032 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 08:01:31.603904009 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:31.655699968 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 08:01:34.786555052 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:34.841972113 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 08:01:35.618351936 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:35.667068005 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 08:01:36.700438976 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:36.749245882 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 08:01:37.594563961 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:37.643485069 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 08:01:38.529011011 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:38.577831984 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 08:01:39.541491032 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:39.590857983 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 08:01:44.314141989 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:44.365715981 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 08:01:45.483055115 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:45.531965971 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 08:01:55.487745047 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 08:01:55.559851885 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 08:02:29.154186964 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:30.151031017 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:31.166793108 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:32.352262974 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:32.424287081 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 08:02:33.167016029 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:34.206736088 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 08:02:35.203108072 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 08:02:35.250248909 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:36.219311953 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 08:02:36.419112921 CEST	57762	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 08:02:37.240662098 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 08:02:37.461003065 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:39.314114094 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 08:02:40.333544970 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:40.487884045 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 08:02:41.323945045 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:41.524218082 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 08:02:42.370624065 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:44.397491932 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 08:02:45.529561043 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:46.372621059 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 08:02:46.434206009 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 08:02:46.574399948 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:47.574556112 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:49.593126059 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 08:02:49.597605944 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:49.658670902 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 08:02:50.613149881 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:50.638376951 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 08:02:51.621308088 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:51.639637947 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 08:02:52.668411970 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:54.678493023 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 08:02:55.687346935 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 08:02:55.696567059 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:56.718844891 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:56.734673023 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 08:02:57.762463093 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:58.541511059 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 08:02:58.606501102 CEST	53	60633	8.8.8.8	192.168.2.3
May 12, 2021 08:02:59.762057066 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 08:03:00.782874107 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 08:03:00.853844881 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:01.841365099 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:02.811834097 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 08:03:02.872667074 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:04.917594910 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 08:03:05.906464100 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 08:03:05.970653057 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:06.937756062 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 08:03:06.966382980 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:08.013849020 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:10.035644054 CEST	53	63619	8.8.8.8	192.168.2.3
May 12, 2021 08:03:11.031840086 CEST	53	63619	8.8.8.8	192.168.2.3
May 12, 2021 08:03:11.059521914 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:12.060440063 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:12.079459906 CEST	53	63619	8.8.8.8	192.168.2.3
May 12, 2021 08:03:13.076947927 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:13.364254951 CEST	61946	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:13.421365976 CEST	53	61946	8.8.8.8	192.168.2.3
May 12, 2021 08:03:15.076543093 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:16.107876062 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 08:03:16.125893116 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 08:03:17.141036034 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 08:03:17.201738119 CEST	64910	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:17.604834080 CEST	52123	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:17.666291952 CEST	53	52123	8.8.8.8	192.168.2.3
May 12, 2021 08:03:18.217997074 CEST	64910	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:19.140124083 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 08:03:19.264046907 CEST	64910	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:21.264622927 CEST	64910	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:21.267046928 CEST	53	64910	8.8.8.8	192.168.2.3
May 12, 2021 08:03:22.285006046 CEST	53	64910	8.8.8.8	192.168.2.3
May 12, 2021 08:03:22.291197062 CEST	56130	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 08:03:23.327791929 CEST	53	64910	8.8.8.8	192.168.2.3
May 12, 2021 08:03:23.341129065 CEST	56130	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:24.327455997 CEST	56130	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:25.321345091 CEST	53	64910	8.8.8.8	192.168.2.3
May 12, 2021 08:03:26.345091105 CEST	53	56130	8.8.8.8	192.168.2.3
May 12, 2021 08:03:27.366398096 CEST	56338	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:27.403759003 CEST	53	56130	8.8.8.8	192.168.2.3
May 12, 2021 08:03:28.375382900 CEST	56338	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:28.393043995 CEST	53	56130	8.8.8.8	192.168.2.3
May 12, 2021 08:03:29.421453953 CEST	56338	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:31.420943975 CEST	53	56338	8.8.8.8	192.168.2.3
May 12, 2021 08:03:32.444873095 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:33.424427986 CEST	53	56338	8.8.8.8	192.168.2.3
May 12, 2021 08:03:33.437156916 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:34.437467098 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 08:03:34.472316980 CEST	53	56338	8.8.8.8	192.168.2.3
May 12, 2021 08:03:36.453270912 CEST	59420	53	192.168.2.3	8.8.8.8

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 12, 2021 08:02:35.204329014 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:02:36.222464085 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:02:37.240825891 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:02:40.491414070 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:02:41.527466059 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:02:46.372764111 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:02:50.638499975 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:02:51.639740944 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:02:55.687459946 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:02:56.734922886 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:00.783149958 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:02.811944008 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:05.906613111 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:06.938616991 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:11.031996012 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:12.079576969 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:16.126441002 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:17.141343117 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:19.140187979 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:22.289450884 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:23.327931881 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:25.321499109 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:27.403886080 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:28.393189907 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable
May 12, 2021 08:03:33.424665928 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 12, 2021 08:03:34.472475052 CEST	192.168.2.3	8.8.8.8	cff5	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 08:02:29.154186964 CEST	192.168.2.3	8.8.8.8	0x5a7c	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:30.151031017 CEST	192.168.2.3	8.8.8.8	0x5a7c	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:31.166793108 CEST	192.168.2.3	8.8.8.8	0x5a7c	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:33.167016029 CEST	192.168.2.3	8.8.8.8	0x5a7c	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:35.250248909 CEST	192.168.2.3	8.8.8.8	0x681c	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:36.419112921 CEST	192.168.2.3	8.8.8.8	0x681c	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:37.461003065 CEST	192.168.2.3	8.8.8.8	0x681c	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:40.333544970 CEST	192.168.2.3	8.8.8.8	0x9ec5	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:41.323945045 CEST	192.168.2.3	8.8.8.8	0x9ec5	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:42.370624065 CEST	192.168.2.3	8.8.8.8	0x9ec5	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:45.529561043 CEST	192.168.2.3	8.8.8.8	0x6936	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:46.574399948 CEST	192.168.2.3	8.8.8.8	0x6936	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:47.574556112 CEST	192.168.2.3	8.8.8.8	0x6936	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:50.613149881 CEST	192.168.2.3	8.8.8.8	0x214c	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:51.621308088 CEST	192.168.2.3	8.8.8.8	0x214c	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:52.668411970 CEST	192.168.2.3	8.8.8.8	0x214c	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:55.696567059 CEST	192.168.2.3	8.8.8.8	0x72d7	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:56.718844891 CEST	192.168.2.3	8.8.8.8	0x72d7	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:02:57.762463093 CEST	192.168.2.3	8.8.8.8	0x72d7	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:00.853844881 CEST	192.168.2.3	8.8.8.8	0xf2a4	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:01.841365099 CEST	192.168.2.3	8.8.8.8	0xf2a4	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:02.872667074 CEST	192.168.2.3	8.8.8.8	0xf2a4	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:05.970653057 CEST	192.168.2.3	8.8.8.8	0xf19	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:06.966382980 CEST	192.168.2.3	8.8.8.8	0xf19	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:08.013849020 CEST	192.168.2.3	8.8.8.8	0xf19	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:11.059521914 CEST	192.168.2.3	8.8.8.8	0xa27b	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:12.060440063 CEST	192.168.2.3	8.8.8.8	0xa27b	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:13.076947927 CEST	192.168.2.3	8.8.8.8	0xa27b	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:15.076543093 CEST	192.168.2.3	8.8.8.8	0xa27b	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:17.201738119 CEST	192.168.2.3	8.8.8.8	0x2838	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:18.217997074 CEST	192.168.2.3	8.8.8.8	0x2838	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:19.264046907 CEST	192.168.2.3	8.8.8.8	0x2838	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:21.264622927 CEST	192.168.2.3	8.8.8.8	0x2838	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:22.291197062 CEST	192.168.2.3	8.8.8.8	0x48c9	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 08:03:23.341129065 CEST	192.168.2.3	8.8.8.8	0x48c9	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:24.327455997 CEST	192.168.2.3	8.8.8.8	0x48c9	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:27.366398096 CEST	192.168.2.3	8.8.8.8	0x9d40	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:28.375382900 CEST	192.168.2.3	8.8.8.8	0x9d40	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:29.421453953 CEST	192.168.2.3	8.8.8.8	0x9d40	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:32.444873095 CEST	192.168.2.3	8.8.8.8	0x89c0	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:33.437156916 CEST	192.168.2.3	8.8.8.8	0x89c0	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:34.437467098 CEST	192.168.2.3	8.8.8.8	0x89c0	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)
May 12, 2021 08:03:36.453270912 CEST	192.168.2.3	8.8.8.8	0x89c0	Standard query (0)	reachglobal-in.com	A (IP address)	IN (0x0001)

DNS Answers

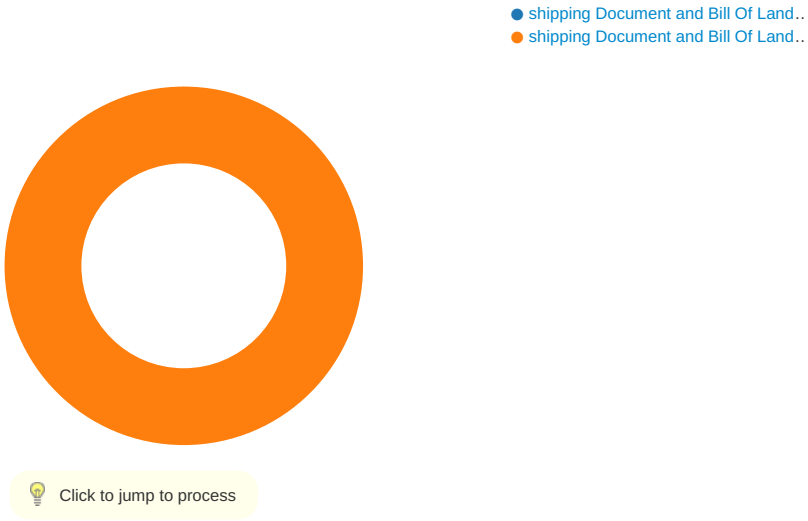
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 08:02:34.206736088 CEST	8.8.8.8	192.168.2.3	0x5a7c	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:35.203108072 CEST	8.8.8.8	192.168.2.3	0x5a7c	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:36.219311953 CEST	8.8.8.8	192.168.2.3	0x5a7c	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:37.240662098 CEST	8.8.8.8	192.168.2.3	0x5a7c	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:39.314114094 CEST	8.8.8.8	192.168.2.3	0x681c	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:40.487884045 CEST	8.8.8.8	192.168.2.3	0x681c	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:41.524218082 CEST	8.8.8.8	192.168.2.3	0x681c	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:44.397491932 CEST	8.8.8.8	192.168.2.3	0x9ec5	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:46.372621059 CEST	8.8.8.8	192.168.2.3	0x9ec5	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:46.434206009 CEST	8.8.8.8	192.168.2.3	0x9ec5	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:49.593126059 CEST	8.8.8.8	192.168.2.3	0x6936	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:50.638376951 CEST	8.8.8.8	192.168.2.3	0x6936	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:51.639637947 CEST	8.8.8.8	192.168.2.3	0x6936	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:54.678493023 CEST	8.8.8.8	192.168.2.3	0x214c	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:55.687346935 CEST	8.8.8.8	192.168.2.3	0x214c	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:56.734673023 CEST	8.8.8.8	192.168.2.3	0x214c	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:02:59.762057066 CEST	8.8.8.8	192.168.2.3	0x72d7	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:00.782874107 CEST	8.8.8.8	192.168.2.3	0x72d7	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 08:03:02.811834097 CEST	8.8.8.8	192.168.2.3	0x72d7	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:04.917594910 CEST	8.8.8.8	192.168.2.3	0xf2a4	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:05.906464100 CEST	8.8.8.8	192.168.2.3	0xf2a4	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:06.937756062 CEST	8.8.8.8	192.168.2.3	0xf2a4	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:10.035644054 CEST	8.8.8.8	192.168.2.3	0xf19	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:11.031840086 CEST	8.8.8.8	192.168.2.3	0xf19	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:12.079459906 CEST	8.8.8.8	192.168.2.3	0xf19	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:16.107876062 CEST	8.8.8.8	192.168.2.3	0xa27b	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:16.125893116 CEST	8.8.8.8	192.168.2.3	0xa27b	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:17.141036034 CEST	8.8.8.8	192.168.2.3	0xa27b	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:19.140124083 CEST	8.8.8.8	192.168.2.3	0xa27b	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:21.267046928 CEST	8.8.8.8	192.168.2.3	0x2838	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:22.285006046 CEST	8.8.8.8	192.168.2.3	0x2838	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:23.327791929 CEST	8.8.8.8	192.168.2.3	0x2838	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:25.321345091 CEST	8.8.8.8	192.168.2.3	0x2838	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:26.345091105 CEST	8.8.8.8	192.168.2.3	0x48c9	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:27.403759003 CEST	8.8.8.8	192.168.2.3	0x48c9	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:28.393043995 CEST	8.8.8.8	192.168.2.3	0x48c9	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:31.420943975 CEST	8.8.8.8	192.168.2.3	0x9d40	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:33.424427986 CEST	8.8.8.8	192.168.2.3	0x9d40	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 08:03:34.472316980 CEST	8.8.8.8	192.168.2.3	0x9d40	Server failure (2)	reachglobal-in.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: shipping Document and Bill Of Landing.exe PID: 672 Parent PID: 5588

General

Start time:	08:01:26
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\shipping Document and Bill Of Landing.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\shipping Document and Bill Of Landing.exe'
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	7196E6E67A39225A9B73AF0C6F6B5B0E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.296439672.0000000002290000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: shipping Document and Bill Of Landing.exe PID: 204 Parent PID: 672

General

Start time:	08:02:09
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\shipping Document and Bill Of Landing.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\shipping Document and Bill Of Landing.exe'
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	7196E6E67A39225A9B73AF0C6F6B5B0E

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000D.00000002.469283991.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	563A70	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	563A70	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	563A70	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	563A70	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	563A70	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	563A70	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis