ID: 356046
Sample Name:
QuotationInvoices.exe
Cookbook: default.jbs
Time: 13:56:47
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

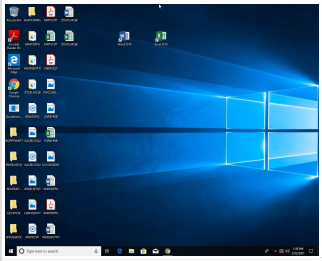
Analysis Report QuotationInvoices.exe

Overview

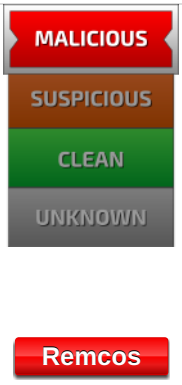
General Information

Sample Name:	QuotationInvoices.exe
Analysis ID:	356046
MD5:	9c51e2991c6c97…
SHA1:	64accc9e3f84e73…
SHA256:	572a6a6fa5277c2…
Tags:	exe RAT RemcosRAT

Most interesting Screenshot:



Detection



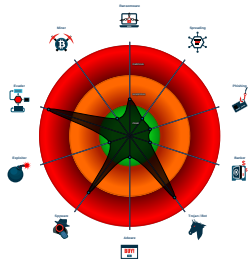
Remcos

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

Signatures

- Detected Remcos RAT
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: Remcos
- Yara detected Remcos RAT
- C2 URLs / IPs found in malware con…
- Contains functionality to capture and…
- Contains functionality to inject code …
- Contains functionality to steal Chrom…
- Contains functionality to steal Firefo…
- Delayed program exit found

Classification



Startup

- **System is w10x64**
- QuotationInvoices.exe (PID: 7036 cmdline: 'C:\Users\user\Desktop\QuotationInvoices.exe' MD5: 9C51E2991C6C9708D783AAB030DCC0DA)
  - QuotationInvoices.exe (PID: 7072 cmdline: 'C:\Users\user\Desktop\QuotationInvoices.exe' MD5: 9C51E2991C6C9708D783AAB030DCC0DA)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "greatglass.servebeer.com:1961:0",
  "Assigned name": "RemoteHost",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "Remcos-I9UILL",
  "Keylog flag": "1",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "wikipedia;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "0",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000001.663167910.000000000400000.00000040.00020000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000001.00000001.663167910.000000000400000.00000040.00020000.sdmp	REMCOS_RAT_variants	unknown	unknown	• 0x5f6cc:$str_a1: C:\Windows\System32\cmd.exe • 0x5f648:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5f648:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5ec68:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x5f2c0:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x5e800:$str_b2: Executing file: • 0x5f810:$str_b3: GetDirectListeningPort • 0x5f080:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x5f40c:$str_b5: licence_code.txt • 0x5f2a8:$str_b7: \update.vbs • 0x5e870:$str_b9: Downloaded file: • 0x5e83c:$str_b10: Downloading file: • 0x5e824:$str_b12: Failed to upload file: • 0x5f7d8:$str_b13: StartForward • 0x5f7f8:$str_b14: StopForward • 0x5f250:$str_b15: fso.DeleteFile " • 0x5f1e4:$str_b16: On Error Resume Next • 0x5f280:$str_b17: fso.DeleteFolder " • 0x5e814:$str_b18: Uploaded file: • 0x5e8b0:$str_b19: Unable to delete: • 0x5f218:$str_b20: while fso.FileExists("
00000000.00000002.667197281.0000000002A70000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.667197281.0000000002A70000.00000004.00000001.sdmp	REMCOS_RAT_variants	unknown	unknown	• 0x5e8cc:$str_a1: C:\Windows\System32\cmd.exe • 0x5e848:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5e848:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5de68:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x5e4c0:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x5da00:$str_b2: Executing file: • 0x5ea10:$str_b3: GetDirectListeningPort • 0x5e280:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x5e60c:$str_b5: licence_code.txt • 0x5e4a8:$str_b7: \update.vbs • 0x5da70:$str_b9: Downloaded file: • 0x5da3c:$str_b10: Downloading file: • 0x5da24:$str_b12: Failed to upload file: • 0x5e9d8:$str_b13: StartForward • 0x5e9f8:$str_b14: StopForward • 0x5e450:$str_b15: fso.DeleteFile " • 0x5e3e4:$str_b16: On Error Resume Next • 0x5e480:$str_b17: fso.DeleteFolder " • 0x5da14:$str_b18: Uploaded file: • 0x5dab0:$str_b19: Unable to delete: • 0x5e418:$str_b20: while fso.FileExists("
00000001.00000002.919352966.0000000000487000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.QuotationInvoices.exe.400000.0.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
1.2.QuotationInvoices.exe.400000.0.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x5e8cc:$str_a1: C:\Windows\System32\cmd.exe • 0x5e848:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5e848:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5de68:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x5e4c0:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x5da00:$str_b2: Executing file: • 0x5ea10:$str_b3: GetDirectListeningPort • 0x5e280:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x5e60c:$str_b5: licence_code.txt • 0x5e4a8:$str_b7: \update.vbs • 0x5da70:$str_b9: Downloaded file: • 0x5da3c:$str_b10: Downloading file: • 0x5da24:$str_b12: Failed to upload file: • 0x5e9d8:$str_b13: StartForward • 0x5e9f8:$str_b14: StopForward • 0x5e450:$str_b15: fso.DeleteFile " • 0x5e3e4:$str_b16: On Error Resume Next • 0x5e480:$str_b17: fso.DeleteFolder " • 0x5da14:$str_b18: Uploaded file: • 0x5dab0:$str_b19: Unable to delete: • 0x5e418:$str_b20: while fso.FileExists("
1.1.QuotationInvoices.exe.400000.0.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

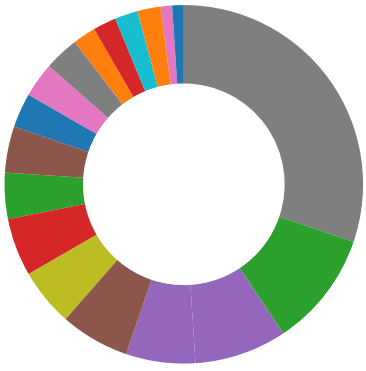
Source	Rule	Description	Author	Strings
1.1.QuotationInvoices.exe.400000.0.raw.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x5f6cc:$str_a1: C:\Windows\System32\cmd.exe • 0x5f648:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5f648:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5ec68:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x5f2c0:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x5e800:$str_b2: Executing file: • 0x5f810:$str_b3: GetDirectListeningPort • 0x5f080:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x5f40c:$str_b5: licence_code.txt • 0x5f2a8:$str_b7: \update.vbs • 0x5e870:$str_b9: Downloaded file: • 0x5e83c:$str_b10: Downloading file: • 0x5e824:$str_b12: Failed to upload file: • 0x5f7d8:$str_b13: StartForward • 0x5f7f8:$str_b14: StopForward • 0x5f250:$str_b15: fso.DeleteFile " • 0x5f1e4:$str_b16: On Error Resume Next • 0x5f280:$str_b17: fso.DeleteFolder " • 0x5e814:$str_b18: Uploaded file: • 0x5e8b0:$str_b19: Unable to delete: • 0x5f218:$str_b20: while fso.FileExists("
1.2.QuotationInvoices.exe.400000.0.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: Remcos

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Remcos RAT

Machine Learning detection for sample

Compliance:

- Detected unpacking (overwrites its own PE header)
- Uses 32bit PE files
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Networking:

- C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Contains functionality to capture and log keystrokes

E-Banking Fraud:

- Yara detected Remcos RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

- Delayed program exit found

HIPS / PFW / Operating System Protection Evasion:

- Contains functionality to inject code into remote processes
- Maps a DLL or memory area into another process

Stealing of Sensitive Information:

- Yara detected Remcos RAT
- Contains functionality to steal Chrome passwords or cookies
- Contains functionality to steal Firefox passwords or cookies

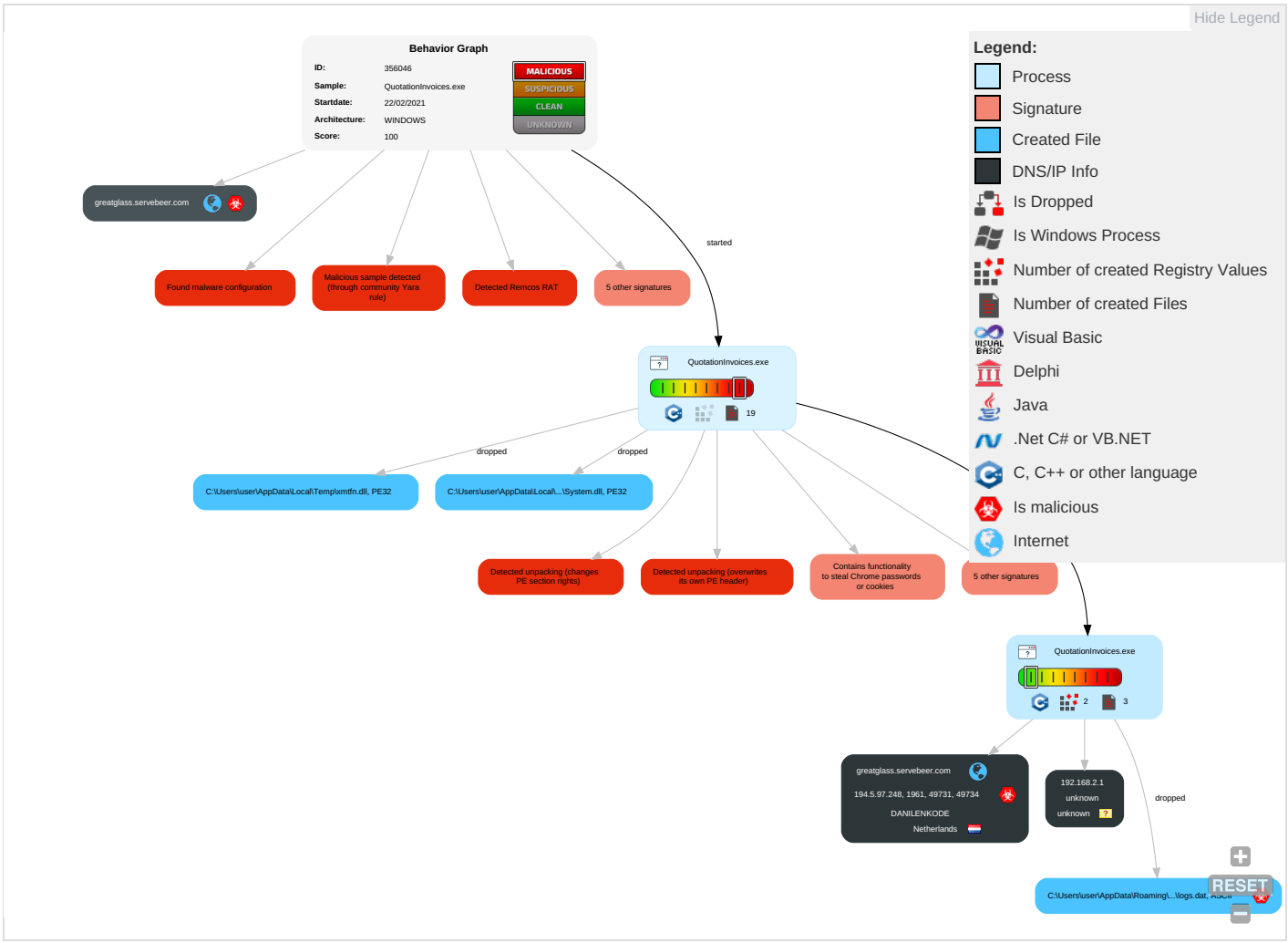
Remote Access Functionality:

- Detected Remcos RAT
- Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Command and Scripting Interpreter 1 2	Windows Service 1	Access Token Manipulation 1	Obfuscated Files or Information 3	Input Capture 1 1 1	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth
Domain Accounts	Service Execution 2	Logon Script (Windows)	Windows Service 1	Software Packing 2 1	Credentials In Files 2	System Service Discovery 1	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 2 2 2	Masquerading 1	NTDS	File and Directory Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2	LSA Secrets	System Information Discovery 3 4	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Security Software Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2 2 2	DCSync	Virtualization/Sandbox Evasion 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

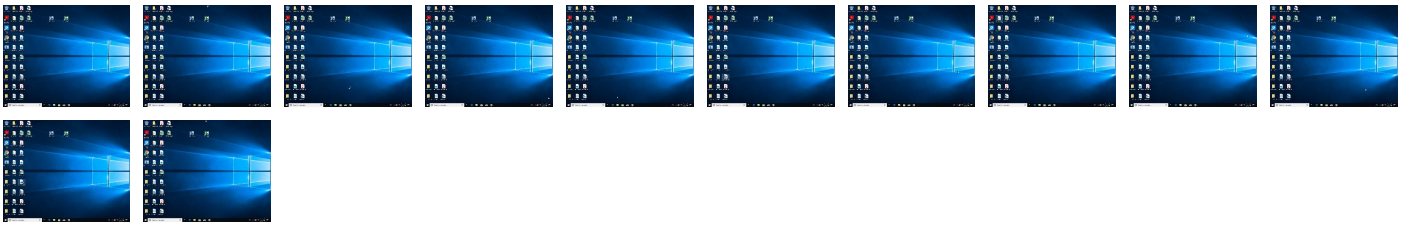
Behavior Graph



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
QuotationInvoices.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsc875C.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsc875C.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsc875C.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.QuotationInvoices.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.0.QuotationInvoices.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.QuotationInvoices.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

Source	Detection	Scanner	Label	Link
greatglass.servebeer.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
greatglass.servebeer.com	5%	Virustotal		Browse
greatglass.servebeer.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
greatglass.servebeer.com	194.5.97.248	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
greatglass.servebeer.com	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	QuotationInvoices.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	QuotationInvoices.exe	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.248	unknown	Netherlands		208476	DANILENKODE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356046
Start date:	22.02.2021
Start time:	13:56:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QuotationInvoices.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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@3/5@53/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16% (good quality ratio 15.4%) • Quality average: 83.5% • Quality standard deviation: 24.9%
HCA Information:	• Successful, ratio: 72% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.193.48, 51.104.144.132, 204.79.197.200, 13.107.21.200, 168.61.161.212, 23.211.6.115, 8.248.137.254, 8.248.135.254, 8.248.117.254, 8.248.115.254, 8.253.204.249, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:57:43	API Interceptor	1041x Sleep call for process: QuotationInvoices.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.248	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	
	QuotationCVXpo00029392.exe	Get hash	malicious	Browse	
	51MRQ TECH DATA -RFQ - SPECIFICATIONS -CHECK LIST.exe	Get hash	malicious	Browse	
	42MRQ TECH DATA -RFQ - SPECIFICATIONS -CHECK LIST.exe	Get hash	malicious	Browse	
	41BURULLUS - EPC WORKS FOR ROSETTA SHARING FACILITIES - PROJECT.exe	Get hash	malicious	Browse	
	45MRQ TECH DATA -RFQ - SPECIFICATIONS -CHECK LIST.exe	Get hash	malicious	Browse	
	44BURULLUS - EPC WORKS FOR ROSETTA SHARING FACILITIES - PROJECT.exe	Get hash	malicious	Browse	
	14MRQ TECH DATA -RFQ - SPECIFICATIONS -CHECK LIST.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	13BURULLUS - EPC WORKS FOR ROSETTA SHARING FACILITIES - PROJECT.exe	Get hash	malicious	Browse	
	33BURULLUS - EPC WORKS FOR ROSETTA SHARING FACILITIES - PROJECT.exe	Get hash	malicious	Browse	
	8MRQ TECH DATA -RFQ - SPECIFICATIONS -CHECK LIST.exe	Get hash	malicious	Browse	
	7BURULLUS - EPC WORKS FOR ROSETTA SHARING FACILITIES - PROJECT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
greatglass.servebeer.com	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• 194.5.97.248
	QuotationCVXpo00029392.exe	Get hash	malicious	Browse	• 194.5.97.248

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	PAYMENT_.EXE	Get hash	malicious	Browse	• 194.5.98.211
	payment.exe	Get hash	malicious	Browse	• 194.5.98.66
	RFQ_1101983736366355 1101938377388.exe	Get hash	malicious	Browse	• 194.5.98.21
	Slip copy .xls.exe	Get hash	malicious	Browse	• 194.5.97.116
	Scan0059.pdf.exe	Get hash	malicious	Browse	• 194.5.97.34
	DHL AWB # 6008824216.png.exe	Get hash	malicious	Browse	• 194.5.97.48
	Scan0019.exe	Get hash	malicious	Browse	• 194.5.97.34
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• 194.5.97.248
	Invoice467972.jar	Get hash	malicious	Browse	• 194.5.97.18
	Invoice467972.jar	Get hash	malicious	Browse	• 194.5.97.18
	Hk6Im7DPON.exe	Get hash	malicious	Browse	• 194.5.98.107
	Zfpmspqv.exe	Get hash	malicious	Browse	• 194.5.97.21
	Notification of payment.exe	Get hash	malicious	Browse	• 194.5.97.92
	Zv3r4M6NeJOSoDQ.exe	Get hash	malicious	Browse	• 194.5.98.26
	MT0128.jar	Get hash	malicious	Browse	• 194.5.97.18
	MT0128.jar	Get hash	malicious	Browse	• 194.5.97.18
	Orden.exe	Get hash	malicious	Browse	• 194.5.97.8
	DHL_6368638172 receipt document,pdf.exe	Get hash	malicious	Browse	• 194.5.97.21
	tax-irs.exe	Get hash	malicious	Browse	• 194.5.97.232
	a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe	Get hash	malicious	Browse	• 194.5.97.207

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsc875C.tmp\System.dll	PO.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.TrojanSpy.MSIL.Agent.22886.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.FileRepMalware.24882.exe	Get hash	malicious	Browse	
	PDF_doc.exe	Get hash	malicious	Browse	
	09000000000000.jar	Get hash	malicious	Browse	
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	
	notice of arrivalpdf.exe	Get hash	malicious	Browse	
	R5BNZ68i0f.exe	Get hash	malicious	Browse	
	payment.exe	Get hash	malicious	Browse	
	notice of arrival.xlsx	Get hash	malicious	Browse	
	Invoice Overdue.exe	Get hash	malicious	Browse	
	Invoice Overdue.exe	Get hash	malicious	Browse	
	CHEQUE COPY RECEIPT.exe	Get hash	malicious	Browse	
	Remittance copy.xlsx	Get hash	malicious	Browse	
	CI + PL.xlsx	Get hash	malicious	Browse	
	RFQ_Enquiry_0002379_.xlsx	Get hash	malicious	Browse	
	QUOTATION.exe	Get hash	malicious	Browse	
	AgroAG008021921doc_pdf.exe	Get hash	malicious	Browse	
	CHEQUE COPY.exe	Get hash	malicious	Browse	
	Bank Details.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsc875C.tmp\System.dll	
Process:	C:\Users\user\Desktop\QuotationInvoices.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: PO.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.TrojanSpy.MSIL.Agent.22886.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.FileRepMalware.24882.exe, Detection: malicious, Browse • Filename: PDF_doc.exe, Detection: malicious, Browse • Filename: 09000000000000.jar, Detection: malicious, Browse • Filename: quotation10204168.dox.xlsx, Detection: malicious, Browse • Filename: notice of arrivalpdf.exe, Detection: malicious, Browse • Filename: R5BNZ68i0f.exe, Detection: malicious, Browse • Filename: payment.exe, Detection: malicious, Browse • Filename: notice of arrival.xlsx, Detection: malicious, Browse • Filename: Invoice Overdue.exe, Detection: malicious, Browse • Filename: Invoice Overdue.exe, Detection: malicious, Browse • Filename: CHEQUE COPY RECEIPT.exe, Detection: malicious, Browse • Filename: Remittance copy.xlsx, Detection: malicious, Browse • Filename: CI + PL.xlsx, Detection: malicious, Browse • Filename: RFQ_Enquiry_0002379_.xlsx, Detection: malicious, Browse • Filename: QUOTATION.exe, Detection: malicious, Browse • Filename: AgroAG008021921doc_pdf.exe, Detection: malicious, Browse • Filename: CHEQUE COPY.exe, Detection: malicious, Browse • Filename: Bank Details.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsh872C.tmp	
Process:	C:\Users\user\Desktop\QuotationInvoices.exe
File Type:	data
Category:	dropped
Size (bytes):	504230
Entropy (8bit):	7.974803391738096
Encrypted:	false
SSDEEP:	6144:laXlqi0/y4lwKzPHdRAFexzsJ/PvzFjBTkBVg90SS6+qLHmFAgOSqxn+8fp2zwIL:yWySRbHdRAF8zQNVk80QSF3qVLUMXO
MD5:	1A5019ACCB8B2C592D98DDCA4D53EA6E
SHA1:	64EB9F091F2A25E64FE5DC52F614499BBBA755AA
SHA-256:	C4F464C4A1CEFF309A6388157AB9FBF26A795C6F5E770D4929892C1A92FFB68E
SHA-512:	9A8EDE65C20C9B24ECC3F72FFB4AB1003A7514596175A067BC006D0BF9BB66BBEAF02EFD82ADA1C1C460F114561972F8F98A94738E84B9FA5E82A0A564A9C0E
Malicious:	false
Reputation:	low
Preview:	.....,.....$..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\okqry.a	
Process:	C:\Users\user\Desktop\QuotationInvoices.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\okqry.a	
Category:	dropped
Size (bytes):	465408
Entropy (8bit):	**7.999601945479521**
Encrypted:	**true**
SSDEEP:	6144:Q/y4lwKzPHdRAFexzsJ/PvzFjBTkBVg90SS6+qLHmFAgOSqxn+8fp2zwI2P8LQ5:cySRbHdRAF8zQNVk80QSF3qVLUMX/
MD5:	96876AE06A1E7B087CA4B25713691E25
SHA1:	EB0C572D4DBD1303BCC20D5E13CA1B5DA6851980
SHA-256:	5144E9DBA5EE3C3CB46706B8095D6EAA2C1AA0D48B4016ECB03CABB844D8EA36
SHA-512:	B6F409C132903A752BC10FE083FF5D53366FC22C81DBAF1D7C737DD2F03D1E1A24F8DCA380BFD784232F79EDAB40E803E0AAB6386C4F4DF291E9AE4CC6793FC9
Malicious:	false
Reputation:	low
Preview:	..I..[..k.m..F....jq..#.f.....0.....U6./h.NL...!.....f.n.+.`~..Y.;f.U.{..p,..g...U..C...V...$..F.*d.....Z...'....=.:T.M...!..W..]. ..C.lt..#.s...X.....k"<.k.)a*.....H..O..F..:.nx..r...D.u"..c...o..g.. ..T...d.W...J..im.....@W<v...15....JH.....w.....7jYJ.X..>..]}...5...Z.k..6.9<..OZ.|.....=...T.}.....y...5...L.?...*.R..S=..\....Z..>..E.....a..Fp.....7..Lu.wW.$.>....~.)..S.np.:. .S....?.F...-.....v{.k(iB.c. ...LYKE..-.....s.pq..~{....g.....@.N@.<.....N...$/7)v..n.Q..'..F.h.d\|.El...Hy..G...yu.z..... :e..m.2.?.....P.z h.j=. h...s..{...h.W.._).FT.w..-4Z{]Z...D.ZT .F..^w7..5b.6\...dC2'..1....c.R~<rL.U7..R~.h.....5.....4.....\.../p...<#.O...3..W..n.".e..7V.y.....K..\7AD`....lhZ"~6...B2.....B.....p...7.0...F.J.:..?.j...c.u.B.F:Ka.n.y.].`.s,.... ...G\:q.d.1.p..\.....B.e...\|.$d.....a$_b.T....X)..D.zxp.Q7.3..T.U.U5$.Y..8a2...8..k.....(2q2l.4.....G7[f....J.e..$...-z?.*.G..G/..(H.Wb.....tX}O.W.

C:\Users\user\AppData\Local\Temp\xmtfn.dll	
Process:	C:\Users\user\Desktop\QuotationInvoices.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23552
Entropy (8bit):	7.589805073051753
Encrypted:	false
SSDEEP:	384:qlpTPQpU2T5eiynNSnAouNfxkSa598ZHWZoujzWxy9sp/x:6hPv29XiSnApNftS9aWZoujzWxX/x
MD5:	7B57E6D08CC3767914CA51A604BC6D13
SHA1:	AFE12DBF77D6FBCF8960D5761699D821AFCCB2B2
SHA-256:	29E898A600F9A16D828D3557093919813967351 39E3A8FDB6ADDA75F0AFC670B
SHA-512:	106CEEE1485DE5ABC7E977BE4CB17E388D1ECB54FCCD1B3ADD75AFC2A5625A81416998E8E9822DF8485CA8265FDA804826D308C2CF27DE2667EA80A359D82C0
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.J.e.J.e.J.e.JI..J.e.J..{J.e.J...J.e.J..\|J.e.J..yJ.e.JRich.e.J .....PE..L....3`.....!.....T..... .....$..I.... .....tex t...F..... ..`.rdata..... .....@..@.data....J...0...L.....@....rsrc.....Z.....@..@.....

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Users\user\Desktop\QuotationInvoices.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.716474907822009
Encrypted:	false
SSDEEP:	3:ttUHrCqDDIrA4RXMRPHv31aeo:tmcXqdHv3IP
MD5:	BD035BD4CCB00A887A17BA7CDE17D115
SHA1:	FCD6C75314E60CC8B7329184C4E866C783D66664
SHA-256:	9AFCF5D6F8CF2857C5DCD6C3B7C991F1BF3E41FFEFDA08F1DFC6E4BD75CD34E7
SHA-512:	22F353D48726C12134A9D1911FE299DB6D852D7D13110AA62AB5849B82386D058E452250D99849F3B93CADFEEBB9F04F41B611A5FCD67E643E13F0E81E49F924
Malicious:	**true**
Reputation:	low
Preview:	..[2021/02/22 13:57:43 Offline Keylogger Started]....[Program Manager]..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.974691206115224

General

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:	QuotationInvoices.exe
File size:	528567
MD5:	9c51e2991c6c9708d783aab030dcc0da
SHA1:	64accc9e3f84e7365d8236c580b9644427e3f9e3
SHA256:	572a6a6fa5277c2b4cc040710694d33b2def62ab74e2801893d33e92e7b105af
SHA512:	c8725d2abba8f2ae1c483d948f2909ff73736e4efa415d6a26f91cf2226431720b13f15868b4177d8b581287a1d41c4c051913a0faf8f95f599f14b5133ab5b0
SSDEEP:	12288:Nro6kYoqOR5HdRAFmzKNVky0QynxqHLUmb8uAT:NrEYyBRAFm2/ky0RxqHLLAT
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L..._.$_.....f...x.....4.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403486
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D75F [Sat Aug 1 02:45:51 2020 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:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h

Instruction
mov dword ptr [0042F44Ch], eax
je 00007FE020EC52D3h
push ebx
call 00007FE020EC844Eh
cmp eax, ebx
je 00007FE020EC52C9h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007FE020EC83CAh
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FE020EC52ADh
push 0000000Bh
call 00007FE020EC8422h
push 00000009h
call 00007FE020EC841Bh
push 00000007h
mov dword ptr [0042F444h], eax
call 00007FE020EC840Fh
cmp eax, ebx
je 00007FE020EC52D1h
push 0000001Eh
call eax
test eax, eax
je 00007FE020EC52C9h
or byte ptr [0042F44Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F518h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429878h
call dword ptr [0040816Ch]
push 0040A1ECh

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x9c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x65ad	0x6600	False	0.675628063725	data	6.48593060343	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4634765625	data	5.26110074066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25558	0x600	False	0.470052083333	data	4.21916068772	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x9c0	0xa00	False	0.466015625	data	4.37730261639	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x38148	0x100	data	English	United States
RT_DIALOG	0x38248	0x11c	data	English	United States
RT_DIALOG	0x38364	0x60	data	English	United States
RT_VERSION	0x383c4	0x2bc	data	English	United States
RT_MANIFEST	0x38680	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Version Infos

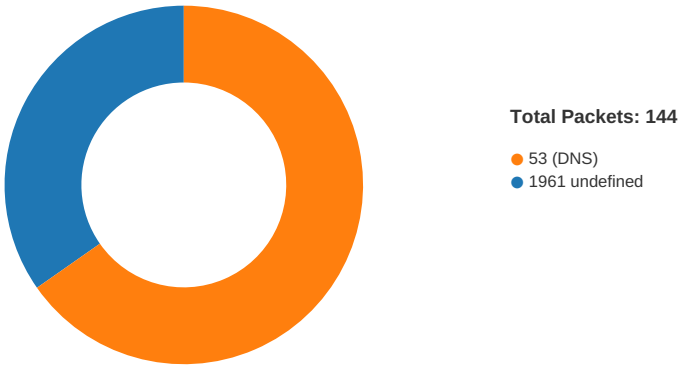
Description	Data
LegalCopyright	Copyright fire escape
FileVersion	95.84.67.13
CompanyName	Angas Proper Group 2 Cluster
LegalTrademarks	American dollar
Comments	Benin
ProductName	arability
FileDescription	Indonesian Sign Language
Translation	0x0409 0x04e4

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 13:57:43.352075100 CET	49731	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:43.401926994 CET	1961	49731	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:44.073777914 CET	49731	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:44.123581886 CET	1961	49731	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:44.683206081 CET	49731	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:44.733222008 CET	1961	49731	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:45.844968081 CET	49734	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:45.895118952 CET	1961	49734	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:46.574366093 CET	49734	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:46.624531984 CET	1961	49734	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:47.183406115 CET	49734	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:47.236166000 CET	1961	49734	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:48.359405041 CET	49737	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:48.409497976 CET	1961	49737	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:49.074224949 CET	49737	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:49.124393940 CET	1961	49737	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:49.636784077 CET	49737	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:49.688222885 CET	1961	49737	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:50.799252033 CET	49740	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:50.849482059 CET	1961	49740	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:51.355676889 CET	49740	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:51.406126022 CET	1961	49740	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:51.918296099 CET	49740	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:51.968597889 CET	1961	49740	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:53.068404913 CET	49742	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:53.120964050 CET	1961	49742	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:53.621481895 CET	49742	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:53.671588898 CET	1961	49742	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:54.183969975 CET	49742	1961	192.168.2.4	194.5.97.248

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 13:57:54.234508038 CET	1961	49742	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:55.346158981 CET	49745	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:55.398158073 CET	1961	49745	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:55.902920961 CET	49745	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:55.953052998 CET	1961	49745	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:56.465475082 CET	49745	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:56.515491009 CET	1961	49745	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:57.913294077 CET	49746	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:57.963583946 CET	1961	49746	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:58.465712070 CET	49746	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:58.515902996 CET	1961	49746	194.5.97.248	192.168.2.4
Feb 22, 2021 13:57:59.028270006 CET	49746	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:57:59.078471899 CET	1961	49746	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:00.185934067 CET	49747	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:00.235944986 CET	1961	49747	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:00.747117996 CET	49747	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:00.797133923 CET	1961	49747	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:01.309602976 CET	49747	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:01.359744072 CET	1961	49747	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:02.470401049 CET	49748	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:02.520298958 CET	1961	49748	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:03.028613091 CET	49748	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:03.080817938 CET	1961	49748	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:03.591046095 CET	49748	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:03.642575979 CET	1961	49748	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:04.743042946 CET	49749	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:04.795856953 CET	1961	49749	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:05.309971094 CET	49749	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:05.360222101 CET	1961	49749	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:05.872490883 CET	49749	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:05.922924995 CET	1961	49749	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:07.025953054 CET	49752	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:07.076220036 CET	1961	49752	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:07.591339111 CET	49752	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:07.643918037 CET	1961	49752	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:08.153973103 CET	49752	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:08.204159975 CET	1961	49752	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:09.296627045 CET	49753	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:09.346679926 CET	1961	49753	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:09.857320070 CET	49753	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:09.909199953 CET	1961	49753	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:10.419747114 CET	49753	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:10.469902992 CET	1961	49753	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:11.568994999 CET	49754	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:11.620316982 CET	1961	49754	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:12.123130083 CET	49754	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:12.173362970 CET	1961	49754	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:12.685606003 CET	49754	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:12.735862970 CET	1961	49754	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:14.202236891 CET	49755	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:14.254498005 CET	1961	49755	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:14.779519081 CET	49755	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:14.830630064 CET	1961	49755	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:15.342042923 CET	49755	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:15.394045115 CET	1961	49755	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:16.731570005 CET	49756	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:16.784250975 CET	1961	49756	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:17.373569965 CET	49756	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:17.423772097 CET	1961	49756	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:18.061012030 CET	49756	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:18.111196041 CET	1961	49756	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:19.202740908 CET	49757	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:19.254518032 CET	1961	49757	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:19.764285088 CET	49757	1961	192.168.2.4	194.5.97.248

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 13:58:19.814393997 CET	1961	49757	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:20.329847097 CET	49757	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:20.379925013 CET	1961	49757	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:21.470912933 CET	49758	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:21.524544954 CET	1961	49758	194.5.97.248	192.168.2.4
Feb 22, 2021 13:58:22.030051947 CET	49758	1961	192.168.2.4	194.5.97.248
Feb 22, 2021 13:58:22.080391884 CET	1961	49758	194.5.97.248	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 13:57:30.884157896 CET	65248	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:30.932887077 CET	53	65248	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:31.995923996 CET	53723	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:32.044653893 CET	53	53723	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:32.189984083 CET	64646	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:32.241077900 CET	53	64646	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:32.368320942 CET	65298	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:32.416887999 CET	53	65298	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:32.958420038 CET	59123	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:33.007092953 CET	53	59123	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:33.925764084 CET	54531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:33.977324009 CET	53	54531	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:34.594816923 CET	49714	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:34.653037071 CET	53	49714	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:35.155740023 CET	58028	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:35.207124949 CET	53	58028	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:36.390825987 CET	53097	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:36.448599100 CET	53	53097	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:37.644206047 CET	49257	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:37.694472075 CET	53	49257	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:38.995876074 CET	62389	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:39.047319889 CET	53	62389	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:40.487632036 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:40.536463976 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:41.704668045 CET	55854	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:41.756934881 CET	53	55854	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:43.046756029 CET	64549	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:43.100265026 CET	53	64549	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:43.281383991 CET	63153	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:43.340078115 CET	53	63153	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:44.232898951 CET	52991	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:44.281585932 CET	53	52991	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:45.437531948 CET	53700	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:45.490942001 CET	53	53700	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:45.782011986 CET	51726	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:45.843770027 CET	53	51726	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:46.696166992 CET	56794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:46.744786024 CET	53	56794	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:47.899638891 CET	56534	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:47.954885960 CET	53	56534	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:48.295202017 CET	56627	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:48.358426094 CET	53	56627	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:48.874819040 CET	56621	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:48.925355911 CET	53	56621	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:50.140919924 CET	63116	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:50.189668894 CET	53	63116	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:50.736525059 CET	64078	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:50.798317909 CET	53	64078	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:51.098829985 CET	64801	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:51.147923946 CET	53	64801	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:53.005208015 CET	61721	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:53.067468882 CET	53	61721	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:53.163702011 CET	51255	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 13:57:53.215184927 CET	53	51255	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:54.339315891 CET	61522	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:54.391067982 CET	53	61522	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:55.282325029 CET	52337	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:55.343982935 CET	53	52337	8.8.8.8	192.168.2.4
Feb 22, 2021 13:57:57.862533092 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:57:57.912153006 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:00.124687910 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:00.184590101 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:02.406542063 CET	49285	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:02.469014883 CET	53	49285	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:04.680299044 CET	50601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:04.741290092 CET	53	50601	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:06.359139919 CET	60875	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:06.407919884 CET	53	60875	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:06.964596033 CET	56448	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:07.023207903 CET	53	56448	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:09.238373041 CET	59172	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:09.295730114 CET	53	59172	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:11.507550955 CET	62420	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:11.565102100 CET	53	62420	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:14.141773939 CET	60579	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:14.198827982 CET	53	60579	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:16.668684959 CET	50183	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:16.730441093 CET	53	50183	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:19.152645111 CET	61531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:19.201297045 CET	53	61531	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:21.412386894 CET	49228	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:21.469583988 CET	53	49228	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:23.686291933 CET	59794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:23.743386030 CET	53	59794	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:25.964018106 CET	55916	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:26.021049976 CET	53	55916	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:26.651815891 CET	52752	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:26.705871105 CET	53	52752	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:26.998788118 CET	60542	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:27.074356079 CET	53	60542	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:28.138034105 CET	60689	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:28.246357918 CET	53	60689	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:28.293483019 CET	64206	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:28.345366955 CET	53	64206	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:28.834017992 CET	50904	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:28.893484116 CET	53	50904	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:29.362914085 CET	57525	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:29.420852900 CET	53	57525	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:30.026035070 CET	53814	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:30.029351950 CET	53418	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:30.101344109 CET	53	53418	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:30.105496883 CET	53	53814	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:30.669245958 CET	62833	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:30.729173899 CET	53	62833	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:30.732491970 CET	59260	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:30.781126022 CET	53	59260	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:31.304718971 CET	49944	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:31.385407925 CET	53	49944	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:32.175874949 CET	63300	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:32.235533953 CET	53	63300	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:33.089649916 CET	61449	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:33.137404919 CET	51275	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:33.146944046 CET	53	61449	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:33.194329977 CET	53	51275	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:33.689402103 CET	63492	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:33.752295971 CET	53	63492	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:35.352124929 CET	58945	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 13:58:35.408977985 CET	53	58945	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:37.617449045 CET	60779	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:37.674660921 CET	53	60779	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:39.893341064 CET	64014	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:39.944017887 CET	53	64014	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:42.163970947 CET	57091	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:42.197487116 CET	55904	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:42.212634087 CET	53	57091	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:42.246172905 CET	53	55904	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:42.406217098 CET	52109	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:42.466309071 CET	53	52109	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:44.456279039 CET	54450	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:44.507868052 CET	53	54450	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:45.970840931 CET	49374	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:46.030608892 CET	53	49374	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:46.754059076 CET	50436	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:46.812547922 CET	53	50436	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:49.044269085 CET	62605	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:49.105220079 CET	53	62605	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:51.340818882 CET	54256	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:51.406141996 CET	53	54256	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:53.647906065 CET	52189	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:53.708487034 CET	53	52189	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:55.943375111 CET	56131	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:56.003597975 CET	53	56131	8.8.8.8	192.168.2.4
Feb 22, 2021 13:58:58.224080086 CET	62992	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:58:58.276984930 CET	53	62992	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:00.499053955 CET	54432	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:00.550509930 CET	53	54432	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:02.975363016 CET	57227	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:03.037074089 CET	53	57227	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:05.908447981 CET	58383	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:05.966707945 CET	53	58383	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:08.214849949 CET	63136	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:08.274915934 CET	53	63136	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:10.491177082 CET	50911	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:10.552557945 CET	53	50911	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:12.773044109 CET	63409	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:12.830398083 CET	53	63409	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:15.077661991 CET	59185	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:15.137773037 CET	53	59185	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:17.362710953 CET	64236	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:17.419770002 CET	53	64236	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:19.654303074 CET	56157	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:19.711353064 CET	53	56157	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:20.151802063 CET	55601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:20.200400114 CET	53	55601	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:21.991266966 CET	52984	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:22.049139977 CET	53	52984	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:22.722409964 CET	51141	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:22.779922009 CET	53	51141	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:24.288728952 CET	53610	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:24.345722914 CET	53	53610	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:26.587452888 CET	61247	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:26.639040947 CET	53	61247	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:28.864841938 CET	65165	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:28.916455030 CET	53	65165	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:31.158606052 CET	52076	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:31.207633972 CET	53	52076	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:33.446224928 CET	54903	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:33.507658005 CET	53	54903	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:35.753556967 CET	55045	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:35.802786112 CET	53	55045	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:38.046181917 CET	54464	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 13:59:38.108414888 CET	53	54464	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:40.350781918 CET	50970	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:40.401925087 CET	53	50970	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:42.585230112 CET	55261	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:42.634088993 CET	53	55261	8.8.8.8	192.168.2.4
Feb 22, 2021 13:59:44.822701931 CET	59809	53	192.168.2.4	8.8.8.8
Feb 22, 2021 13:59:44.885376930 CET	53	59809	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 13:57:43.281383991 CET	192.168.2.4	8.8.8.8	0xde5a	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:45.782011986 CET	192.168.2.4	8.8.8.8	0x4f79	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:48.295202017 CET	192.168.2.4	8.8.8.8	0x76a7	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:50.736525059 CET	192.168.2.4	8.8.8.8	0x4057	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:53.005208015 CET	192.168.2.4	8.8.8.8	0xfcc3	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:55.282325029 CET	192.168.2.4	8.8.8.8	0x8df4	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:57.862533092 CET	192.168.2.4	8.8.8.8	0xfc4a	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:00.124687910 CET	192.168.2.4	8.8.8.8	0x18e3	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:02.406542063 CET	192.168.2.4	8.8.8.8	0x2294	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:04.680299044 CET	192.168.2.4	8.8.8.8	0x81e4	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:06.964596033 CET	192.168.2.4	8.8.8.8	0x4364	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:09.238373041 CET	192.168.2.4	8.8.8.8	0xcbb9	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:11.507550955 CET	192.168.2.4	8.8.8.8	0x3f87	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:14.141773939 CET	192.168.2.4	8.8.8.8	0x7c01	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:16.668684959 CET	192.168.2.4	8.8.8.8	0x4ec5	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:19.152645111 CET	192.168.2.4	8.8.8.8	0x4332	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:21.412386894 CET	192.168.2.4	8.8.8.8	0xf26c	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:23.686291933 CET	192.168.2.4	8.8.8.8	0xef30	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:25.964018106 CET	192.168.2.4	8.8.8.8	0xeef9	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:28.293483019 CET	192.168.2.4	8.8.8.8	0xa17b	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:30.732491970 CET	192.168.2.4	8.8.8.8	0xb344	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:33.089649916 CET	192.168.2.4	8.8.8.8	0x1aa5	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:35.352124929 CET	192.168.2.4	8.8.8.8	0x326b	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:37.617449045 CET	192.168.2.4	8.8.8.8	0xf5f2	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:39.893341064 CET	192.168.2.4	8.8.8.8	0x3eb2	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:42.163970947 CET	192.168.2.4	8.8.8.8	0x71df	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:44.456279039 CET	192.168.2.4	8.8.8.8	0xd87	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:46.754059076 CET	192.168.2.4	8.8.8.8	0xb6f8	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:49.044269085 CET	192.168.2.4	8.8.8.8	0xbe80	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:51.340818882 CET	192.168.2.4	8.8.8.8	0x7899	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:53.647906065 CET	192.168.2.4	8.8.8.8	0xf149	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 13:58:55.943375111 CET	192.168.2.4	8.8.8.8	0x2070	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:58.224080086 CET	192.168.2.4	8.8.8.8	0x43dc	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:00.499053955 CET	192.168.2.4	8.8.8.8	0x4f83	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:02.975363016 CET	192.168.2.4	8.8.8.8	0x27e1	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:05.908447981 CET	192.168.2.4	8.8.8.8	0x6128	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:08.214849949 CET	192.168.2.4	8.8.8.8	0x174f	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:10.491177082 CET	192.168.2.4	8.8.8.8	0x8d7	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:12.773044109 CET	192.168.2.4	8.8.8.8	0x3f68	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:15.077661991 CET	192.168.2.4	8.8.8.8	0xcfc	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:17.362710953 CET	192.168.2.4	8.8.8.8	0xd2d2	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:19.654303074 CET	192.168.2.4	8.8.8.8	0xf13f	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:21.991266966 CET	192.168.2.4	8.8.8.8	0x55fb	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:24.288728952 CET	192.168.2.4	8.8.8.8	0xa732	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:26.587452888 CET	192.168.2.4	8.8.8.8	0xb854	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:28.864841938 CET	192.168.2.4	8.8.8.8	0x698f	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:31.158606052 CET	192.168.2.4	8.8.8.8	0xe4e9	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:33.446224928 CET	192.168.2.4	8.8.8.8	0xc7e	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:35.753556967 CET	192.168.2.4	8.8.8.8	0x9f8f	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:38.046181917 CET	192.168.2.4	8.8.8.8	0x2a19	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:40.350781918 CET	192.168.2.4	8.8.8.8	0xc7dc	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:42.585230112 CET	192.168.2.4	8.8.8.8	0xcae	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:44.822701931 CET	192.168.2.4	8.8.8.8	0xbe0e	Standard query (0)	greatglass .servebeer.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 13:57:43.340078115 CET	8.8.8.8	192.168.2.4	0xde5a	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:45.843770027 CET	8.8.8.8	192.168.2.4	0x4f79	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:48.358426094 CET	8.8.8.8	192.168.2.4	0x76a7	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:50.798317909 CET	8.8.8.8	192.168.2.4	0x4057	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:53.067468882 CET	8.8.8.8	192.168.2.4	0xfcc3	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:55.343982935 CET	8.8.8.8	192.168.2.4	0x8df4	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:57:57.912153006 CET	8.8.8.8	192.168.2.4	0xfc4a	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:00.184590101 CET	8.8.8.8	192.168.2.4	0x18e3	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:02.469014883 CET	8.8.8.8	192.168.2.4	0x2294	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 13:58:04.741290092 CET	8.8.8.8	192.168.2.4	0x81e4	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:07.023207903 CET	8.8.8.8	192.168.2.4	0x4364	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:09.295730114 CET	8.8.8.8	192.168.2.4	0xcbb9	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:11.565102100 CET	8.8.8.8	192.168.2.4	0x3f87	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:14.198827982 CET	8.8.8.8	192.168.2.4	0x7c01	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:16.730441093 CET	8.8.8.8	192.168.2.4	0x4ec5	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:19.201297045 CET	8.8.8.8	192.168.2.4	0x4332	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:21.469583988 CET	8.8.8.8	192.168.2.4	0xf26c	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:23.743386030 CET	8.8.8.8	192.168.2.4	0xef30	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:26.021049976 CET	8.8.8.8	192.168.2.4	0xeef9	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:28.345366955 CET	8.8.8.8	192.168.2.4	0xa17b	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:30.781126022 CET	8.8.8.8	192.168.2.4	0xb344	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:33.146944046 CET	8.8.8.8	192.168.2.4	0x1aa5	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:35.408977985 CET	8.8.8.8	192.168.2.4	0x326b	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:37.674660921 CET	8.8.8.8	192.168.2.4	0xf5f2	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:39.944017887 CET	8.8.8.8	192.168.2.4	0x3eb2	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:42.212634087 CET	8.8.8.8	192.168.2.4	0x71df	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:44.507868052 CET	8.8.8.8	192.168.2.4	0xd87	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:46.812547922 CET	8.8.8.8	192.168.2.4	0xb6f8	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:49.105220079 CET	8.8.8.8	192.168.2.4	0xbe80	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:51.406141996 CET	8.8.8.8	192.168.2.4	0x7899	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:53.708487034 CET	8.8.8.8	192.168.2.4	0xf149	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:56.003597975 CET	8.8.8.8	192.168.2.4	0x2070	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:58:58.276984930 CET	8.8.8.8	192.168.2.4	0x43dc	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:00.550509930 CET	8.8.8.8	192.168.2.4	0x4f83	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:03.037074089 CET	8.8.8.8	192.168.2.4	0x27e1	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)

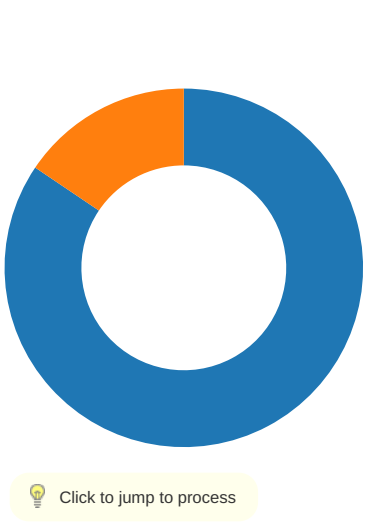
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 13:59:05.966707945 CET	8.8.8.8	192.168.2.4	0x6128	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:08.274915934 CET	8.8.8.8	192.168.2.4	0x174f	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:10.552557945 CET	8.8.8.8	192.168.2.4	0x8d7	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:12.830398083 CET	8.8.8.8	192.168.2.4	0x3f68	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:15.137773037 CET	8.8.8.8	192.168.2.4	0xcfc	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:17.419770002 CET	8.8.8.8	192.168.2.4	0xd2d2	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:19.711353064 CET	8.8.8.8	192.168.2.4	0xf13f	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:22.049139977 CET	8.8.8.8	192.168.2.4	0x55fb	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:24.345722914 CET	8.8.8.8	192.168.2.4	0xa732	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:26.639040947 CET	8.8.8.8	192.168.2.4	0xb854	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:28.916455030 CET	8.8.8.8	192.168.2.4	0x698f	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:31.207633972 CET	8.8.8.8	192.168.2.4	0xe4e9	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:33.507658005 CET	8.8.8.8	192.168.2.4	0xc7e	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:35.802786112 CET	8.8.8.8	192.168.2.4	0x9f8f	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:38.108414888 CET	8.8.8.8	192.168.2.4	0x2a19	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:40.401925087 CET	8.8.8.8	192.168.2.4	0xc7dc	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:42.634088993 CET	8.8.8.8	192.168.2.4	0xcae	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)
Feb 22, 2021 13:59:44.885376930 CET	8.8.8.8	192.168.2.4	0xbe0e	No error (0)	greatglass .servebeer.com		194.5.97.248	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

● QuotationInvoices.exe



System Behavior

Analysis Process: QuotationInvoices.exe PID: 7036 Parent PID: 5924

General

Start time:	13:57:38
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\QuotationInvoices.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QuotationInvoices.exe'
Imagebase:	0x400000
File size:	528567 bytes
MD5 hash:	9C51E2991C6C9708D783AAB030DCC0DA
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: 00000000.00000002.667197281.0000000002A70000.00000004.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000000.00000002.667197281.0000000002A70000.00000004.00000001.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsh872B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsh872C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\xmtfn.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\okqry.a	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\nsc875C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsc875C.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405883	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsc875C.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh872B.tmp	success or wait	1	4036FD	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsc875C.tmp	success or wait	1	405A44	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh872C.tmp	unknown	23449	96 0d 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 24 00 00 00 b4 09 00 00 00 00 00 d0 0c 00 00 01 00 00 00 96 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........,...................$.	success or wait	31	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\xmtfn.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 f1 04 db 19 b5 65 b5 4a b5 65 b5 4a b5 65 b5 4a b5 65 b4 4a 96 65 b5 4a 49 12 0c 4a ba 65 b5 4a 92 a3 7b 4a b4 65 b5 4a 92 a3 7f 4a b4 65 b5 4a 92 a3 7c 4a b4 65 b5 4a 92 a3 79 4a b4 65 b5 4a 52 69 63 68 b5 65 b5 4a 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 a7 8a 33 60 00 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0b 00 00 04 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00 10 00	MZ....................@..... ....!..L.!This program cannot be run in DOS mode.... $...........e.J.e.J.e.J.e.J.e .JI..J.e.J..{J.e.J...J.e.J..|J .e.J..yJ.e.JRich.e.J........PE ..L.....3`...........!........ .T............	success or wait	2	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\okqry.a	unknown	16384	e1 b2 13 49 c1 07 5b ea 04 6b bf 6d f5 80 46 8a f6 06 1c 6a 71 07 c2 be 23 a4 66 ab 08 e4 e3 83 85 13 de 03 a1 11 30 ac 86 b0 f9 cd 0e b8 55 36 ef b2 a2 2f 68 f1 b3 4e 4c bb c3 eb 21 cd c9 be e0 15 8c a0 87 d1 66 be 6e fe 2b c3 60 7e 87 f8 59 c9 3b 66 0e 55 cc 7b f5 93 70 2c da c2 67 9a 1a 9d 55 8c 0b 43 d4 96 0a 1b 56 04 99 ef 24 d9 1d 46 a0 2a 64 ae f2 8a 2e 19 c5 94 c6 5a 1a b2 ba 27 93 14 fe 99 3d be 3a 54 9e 4d ee c4 cf 21 a1 1e 57 9b 99 5d 03 20 a5 ce 43 b6 6c 74 fb dd bd 23 fa 73 b8 b9 8c 58 d6 ae a6 c8 f5 be 6b 22 3c e3 6b e6 b2 b2 29 61 2a 98 b5 13 ae b5 48 1a ec 4f d3 c1 46 b3 f1 3a e4 a7 6e 78 a5 b9 72 f1 ec 89 c3 44 b2 75 22 f4 9e 63 a6 b5 cf 6f ad c3 67 87 ed ca b6 c5 54 01 bc b2 64 bc 57 e1 f9 f7 4a e0 9d 69 6d ff a8 ad 03 e3 40 57 3c 76 86	...I..[..k.m..F....jq...#.f... ....0.......U6.../h..NL... !.........f.n.+.`~..Y.;f.U.{.. p,..g...U..C....V...$..F.*d... .....Z...'....=.:T.M...!..W..]. ..C.lt...#.s...X......k"<.k. ..)a*.....H..O..F..:..nx..r... .D.u"..c...o..g.....T...d.W... J..im.....@W<v.	success or wait	29	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\nsc875C.tmp\System.dll	unknown	11776	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 69 72 2a 92 2d 13 44 c1 2d 13 44 c1 2d 13 44 c1 ae 0f 4a c1 2a 13 44 c1 2d 13 45 c1 3e 13 44 c1 ee 1c 19 c1 2a 13 44 c1 79 30 74 c1 29 13 44 c1 4e 31 6e c1 2c 13 44 c1 d2 33 40 c1 2c 13 44 c1 52 69 63 68 2d 13 44 c1 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 a8 d5 24 5f 00 00 00 00 00 00 00 00 e0 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......ir*.-.D.-.D.- .D...J.*.D.- .E.>.D.....*.D.y0t.).D.N1n. ,.D..3@.,.D.Rich- .D.........PE ..L.....$_...........!..... .. ..!).....	success or wait	1	405EA7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\QuotationInvoices.exe	unknown	512	success or wait	72	405E78	ReadFile
C:\Users\user\Desktop\QuotationInvoices.exe	unknown	16384	success or wait	31	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsh872C.tmp	unknown	4	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsh872C.tmp	unknown	3478	success or wait	1	4032A5	ReadFile
C:\Users\user\AppData\Local\Temp\nsh872C.tmp	unknown	4	success or wait	3	405E78	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh872C.tmp	unknown	16384	success or wait	32	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\okqry.a	unknown	465408	success or wait	1	10006D0B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10003885	ReadFile

Analysis Process: QuotationInvoices.exe PID: 7072 Parent PID: 7036

General

Start time:	13:57:39
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\QuotationInvoices.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QuotationInvoices.exe'
Imagebase:	0x400000
File size:	528567 bytes
MD5 hash:	9C51E2991C6C9708D783AAB030DCC0DA
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: 00000001.00000001.663167910.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000001.00000001.663167910.0000000000400000.00000040.00020000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000001.00000002.919352966.0000000000487000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000001.00000002.919290826.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000001.00000002.919290826.0000000000400000.00000040.00000001.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4086A6	CreateDirectoryW
C:\Users\user\AppData\Roaming\remcos\logs.dat	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	41730B	CreateFileW
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4086A6	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\remcos\logs.dat	unknown	51	0d 0a 5b 32 30 32 31 2f 30 32 2f 32 32 20 31 33 3a 35 37 3a 34 33 20 4f 66 66 6c 69 6e 65 20 4b 65 79 6c 6f 67 67 65 72 20 53 74 61 72 74 65 64 5d 0d 0a	..[2021/02/22 13:57:43 Offline Keylogger Started]..	success or wait	2	417345	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Remcos-I9UILL\	success or wait	1	41037C	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Remcos-I9UILL	exepath	binary	76 01 C4 6A 97 F1 A5 84 1C B8 B9 62 BB 95 40 34 E5 94 6B 68 BE 72 67 C0 D6 F8 FE 3F 4E 58 E2 8F 2A 98 39 12 1E AE 29 64 56 8D 6D 6A B5 1B C7 C7 6A 45 3A 40 8D 18 C4 B1 A9 C8 F7 13 E9 56 3B 15 9E 3D 3A C8 41 6F 40 27 B7 B8 46 2D 4E 02 92 AC 36 67 AF E0 D9 8C 01 E1 C2 4C	success or wait	1	4103A4	RegSetValueExA
HKEY_CURRENT_USER\Software\Remcos-I9UILL	licence	unicode	9F6C3147F99BA77ACE86615FDD78B139	success or wait	1	4103A4	RegSetValueExA

Disassembly

Code Analysis