ID: 412749
Sample Name: Purchase Order_12052021.exe
Cookbook: default.jbs
Time: 22:37:18
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

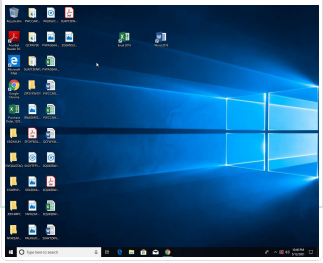
Analysis Report Purchase Order_12052021.exe

Overview

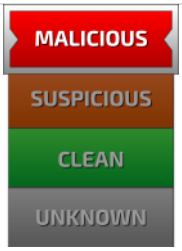
General Information

Sample Name:	Purchase Order_12052021.exe
Analysis ID:	412749
MD5:	b7394ccc239f48e..
SHA1:	020ae73c138a97..
SHA256:	41b785e6bf87195.
Tags:	exe Matiex
Infos:	

Most interesting Screenshot:



Detection



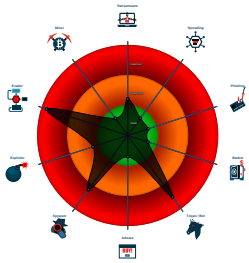
AgentTesla Matiex

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

Signatures

- Detected unpacking (changes PE se…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Yara detected Matiex Keylogger
- Contains functionality to check if a d…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- May check the online IP address of …
- PE file has nameless sections
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- Purchase Order_12052021.exe (PID: 3560 cmdline: 'C:\Users\user\Desktop\Purchase Order_12052021.exe' MD5: B7394CCC239F48EB4A041F1C0FB92D92)
  - Purchase Order_12052021.exe (PID: 404 cmdline: C:\Users\user\Desktop\Purchase Order_12052021.exe MD5: B7394CCC239F48EB4A041F1C0FB92D92)
  - Purchase Order_12052021.exe (PID: 2792 cmdline: C:\Users\user\Desktop\Purchase Order_12052021.exe MD5: B7394CCC239F48EB4A041F1C0FB92D92)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.219914273.000000000286 4000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.470992091.0000000002DC 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000003.00000002.467511051.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
00000003.00000002.467511051.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_BedsObfuscat or	Yara detected Beds Obfuscator	Joe Security	
00000003.00000002.467511051.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Click to see the 9 entries

Unpacked PEs

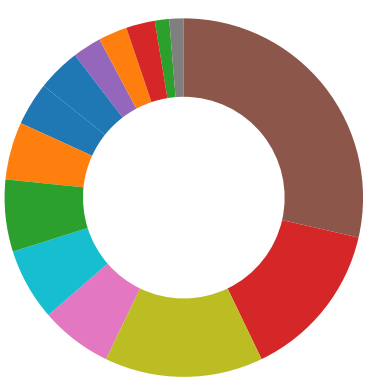
Source	Rule	Description	Author	Strings
0.2.Purchase Order_12052021.exe.3b46210.3.unpack	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	

Source	Rule	Description	Author	Strings
0.2.Purchase Order_12052021.exe.3b46210.3.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.Purchase Order_12052021.exe.3b46210.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.2.Purchase Order_12052021.exe.4224d4.1.raw.unpack	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
3.2.Purchase Order_12052021.exe.4224d4.1.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 9 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

May check the online IP address of the machine

System Summary:

Initial sample is a PE file and has a suspicious name

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Yara detected Beds Obfuscator

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Yara detected Beds Obfuscator

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected Matiex Keylogger

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

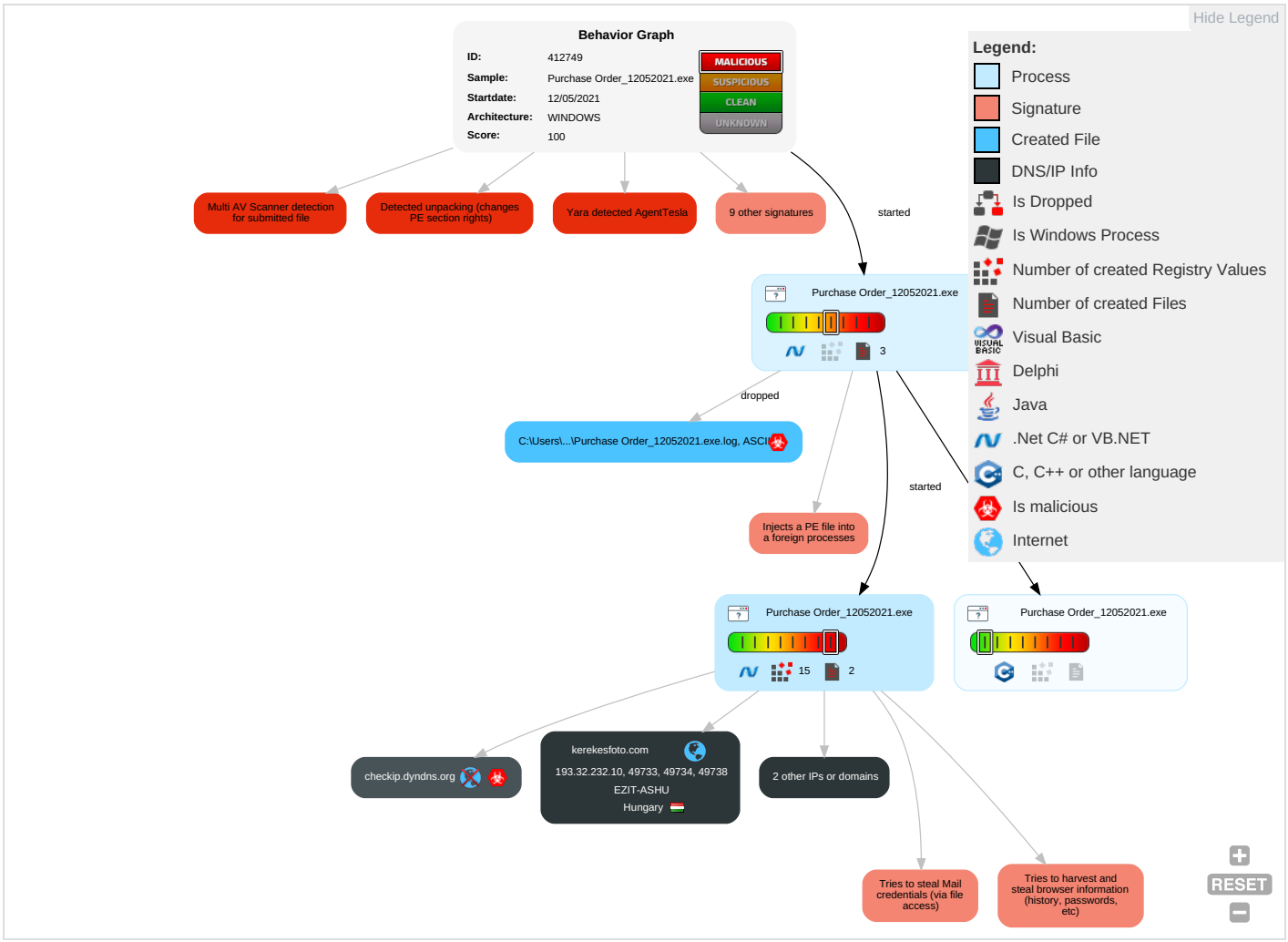
Yara detected AgentTesla

Yara detected Matiex Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 2 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eave Inse Netv Com
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Expl Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4 1	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Ingress Tool Transfer 1	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 1	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Remote System Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Application Layer Protocol 2 3	Man Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 3	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 2 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce

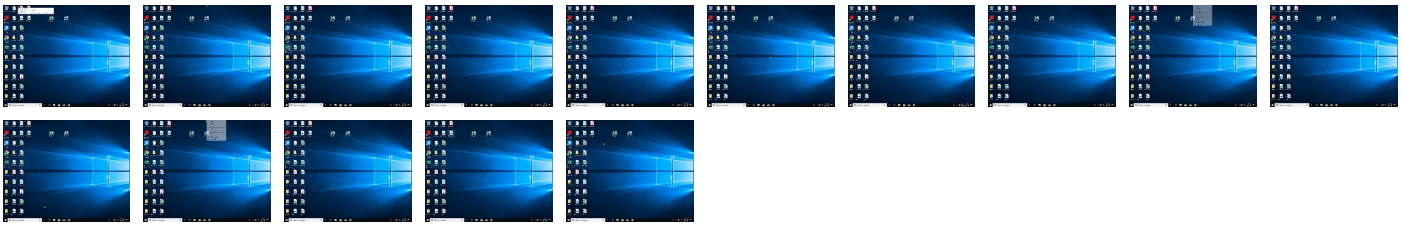
Behavior Graph



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
Purchase Order_12052021.exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
Purchase Order_12052021.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Purchase Order_12052021.exe.3b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.Purchase Order_12052021.exe.400000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File

Domains

Source	Detection	Scanner	Label	Link
kerekesfoto.com	5%	Virustotal		Browse
freegeoip.app	1%	Virustotal		Browse
checkip.dyndns.com	0%	Virustotal		Browse
checkip.dyndns.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://www.digicert.coef	0%	Avira URL Cloud	safe	
http://https://www.geodatatool.com/en/?ip=3D84.17.52.78=0D=0A=0D=0ADat=	0%	Avira URL Cloud	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://servermanager.miixit.org/index_ru.htmlc	0%	Avira URL Cloud	safe	
http://https://www.geodatatool.com/en/?ip=	0%	URL Reputation	safe	
http://https://www.geodatatool.com/en/?ip=	0%	URL Reputation	safe	
http://https://www.geodatatool.com/en/?ip=	0%	URL Reputation	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://kerekesfoto.com	0%	Avira URL Cloud	safe	
http://https://www.digicert.	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.html	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	0%	URL Reputation	safe	
http://checkip.dyndns.org/HB	0%	Avira URL Cloud	safe	
http://https://www.geodatatool.com/en/?ip=84.17.52.78	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/report/reporter_index.php?name=	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/1	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/downloads/	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/hits/hit_index.php?k=	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/84.17.52.78	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.78	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.78	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kerekesfoto.com	193.32.232.10	true	false	• 5%, Virustotal, Browse	unknown
freegeoip.app	104.21.19.200	true	false	• 1%, Virustotal, Browse	unknown
checkip.dyndns.com	216.146.43.71	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	false	• Avira URL Cloud: safe	unknown

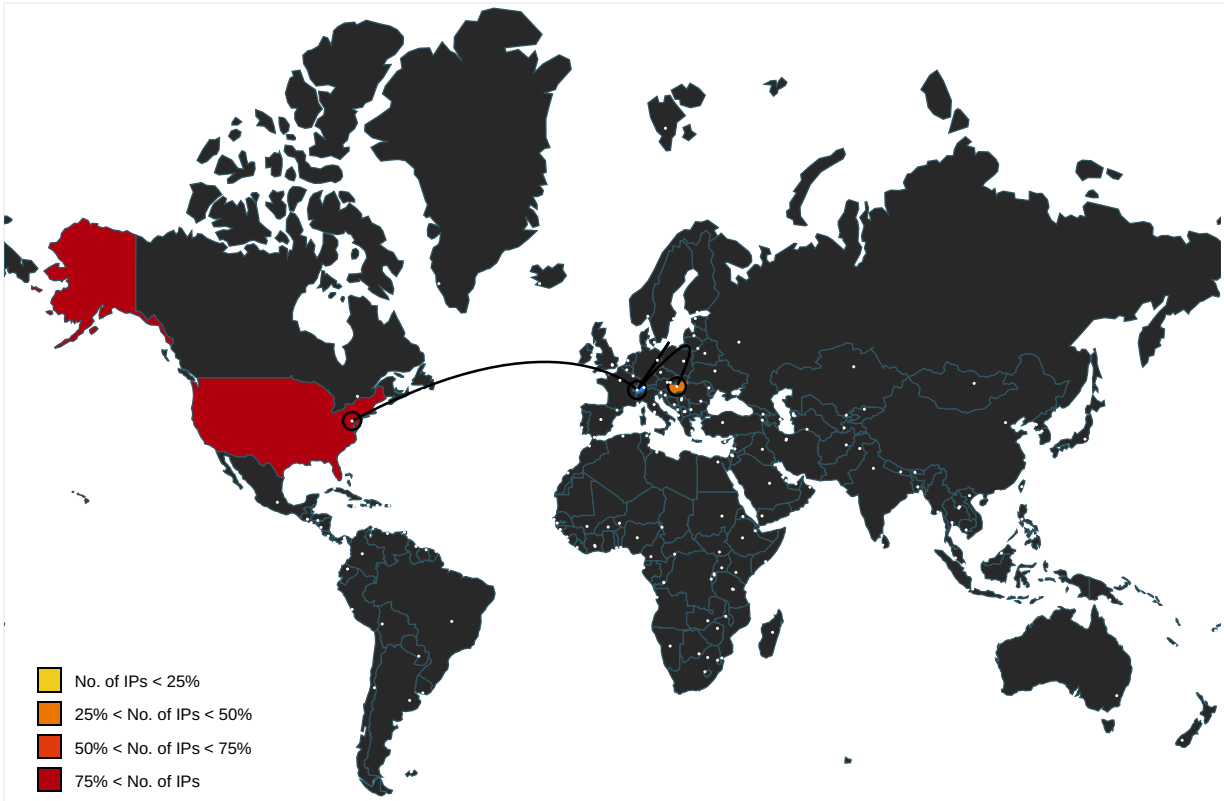
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://freegeoip.app/xml/	Purchase Order_12052021.exe, 00000003.00000002.471029009.0000002DF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.digicert.coef	Purchase Order_12052021.exe, 00000003.00000002.475714622.0000006840000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.geodatatool.com/en/?ip=3D84.17.52.78=0D=0A=0D=0ADat=	Purchase Order_12052021.exe, 00000003.00000002.473656695.0000003132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app	Purchase Order_12052021.exe, 00000003.00000002.471029009.0000002DF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servermanager.miixit.org/index_ru.htmlc	Purchase Order_12052021.exe, 00000000.00000003.213058949.0000003115000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.geodatatool.com/en/?ip=	Purchase Order_12052021.exe, 00000003.00000002.471083879.0000002E20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org	Purchase Order_12052021.exe, 00000003.00000002.470992091.0000002DC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kerekesfoto.com	Purchase Order_12052021.exe, 00000003.00000002.471885488.0000002F03000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Purchase Order_12052021.exe, 00000000.00000002.219914273.0000002864000.00000004.00000001.sdmp	false		high
http://https://www.digicert.	Purchase Order_12052021.exe, 00000003.00000002.475714622.0000006840000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC	Purchase Order_12052021.exe, 00000000.00000003.213058949.0000003115000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/index_ru.html	Purchase Order_12052021.exe, 00000000.00000003.213058949.0000003115000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	Purchase Order_12052021.exe, 00000003.00000002.470992091.0000002DC1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org/HB	Purchase Order_12052021.exe, 00000003.00000002.470992091.0000002DC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.geodatatool.com/en/?ip=84.17.52.78	Purchase Order_12052021.exe, 00000003.00000002.471482796.0000002E9E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/report/reporter_index.php?name=	Purchase Order_12052021.exe, 00000000.00000003.213058949.0000003115000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot/sendMessage?chat_id=&text=Createutf-8Win32_ComputerSystemModelManufactu	Purchase Order_12052021.exe, 00000003.00000002.470992091.0000002DC1000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/1	Purchase Order_12052021.exe, 00000000.00000003.213058949.0000003115000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Purchase Order_12052021.exe, 00000000.00000002.219818488.0000002811000.00000004.00000001.sdmp, Purchase Order_12052021.exe, 00000003.00000002.470992091.0000002DC1000.00000004.00000001.sdmp	false		high
http://https://i.imgur.com/GJD7Q5y.png195.239.51.11795.26.248.2989.208.29.13389.187.165.4792.118.13.1895.26	Purchase Order_12052021.exe, 00000003.00000002.470992091.0000002DC1000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC5servermana	Purchase Order_12052021.exe, 00000000.00000003.213058949.0000003115000.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/downloads/	Purchase Order_12052021.exe, 00000000.00000003.213058949.0000003115000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=	Purchase Order_12052021.exe, 00000000.00000003.213058949.0000003115000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app/xml/84.17.52.78	Purchase Order_12052021.exe, 00000003.00000002.471029009.0000002DF4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.19.200	freegeoip.app	United States		13335	CLOUDFLARENETUS	false
216.146.43.71	checkip.dyndns.com	United States		33517	DYNDNSUS	false
193.32.232.10	kerekesfoto.com	Hungary		62292	EZIT-ASHU	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412749
Start date:	12.05.2021
Start time:	22:37:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 25s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	Purchase Order_12052021.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:	26
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@5/1@36/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 1%) • Quality average: 44.1% • Quality standard deviation: 34.3%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 40.88.32.150, 104.42.151.234, 20.50.102.62, 23.57.80.111, 92.122.213.247, 92.122.213.194, 205.185.216.42, 205.185.216.10, 20.54.26.129, 20.49.157.6, 20.82.209.183 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, iris-de-ppe-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:38:10	API Interceptor	889x Sleep call for process: Purchase Order_12052021.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.19.200	Statement of Account April-2021.exe	Get hash	malicious	Browse	
	d0875029_by_Libranalysis.exe	Get hash	malicious	Browse	
	SNAOUOKKOI.exe	Get hash	malicious	Browse	
	ve #U00e7eki listesi ektedir Proforma.exe	Get hash	malicious	Browse	
	Due Invoices.exe	Get hash	malicious	Browse	
	Order-PO102.exe	Get hash	malicious	Browse	
	IMG_0125_30_227_06.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.36873970.29336.exe	Get hash	malicious	Browse	
	q3qhElKDnGNNjTi.exe	Get hash	malicious	Browse	
	ORDEN SURA OC CVE6535 _TVOP-MIO.exe	Get hash	malicious	Browse	
	f2b03f7e_by_Libranalysis.exe	Get hash	malicious	Browse	
	be8928c5_by_Libranalysis.exe	Get hash	malicious	Browse	
	PURCHASE_ORDER_0098_PDF.exe	Get hash	malicious	Browse	
	TWI-SHA 202102.exe	Get hash	malicious	Browse	
	Reconfirm invoice.exe	Get hash	malicious	Browse	
	INQUIRY.exe	Get hash	malicious	Browse	
	0908000000.exe	Get hash	malicious	Browse	
	Nuovo ordine _WJO-001, pdf.exe	Get hash	malicious	Browse	
	Tender Overview 10052021.doc	Get hash	malicious	Browse	
	59932e6d_by_Libranalysis.exe	Get hash	malicious	Browse	
216.146.43.71	Invoice...exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Statement of Account April-2021.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	eb57884e_by_Libranalysis.xlsx	Get hash	malicious	Browse	• checkip.dyndns.org/
	79cc8c05_by_Libranalysis.xlsx	Get hash	malicious	Browse	• checkip.dyndns.org/
	Tender Overview 10052021.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	SOA.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	QUOTATION.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	INQUIRY.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Payment_Advice.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SOA..exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	file.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Pre Shipment Doc..exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Purchase Order 883.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	39305.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PI.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Proforma adjunta N#U00ba 42037,pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	swift copy.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	DHL 4677348255142.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QEpa8OLm9Z.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	c7b8f5dc_by_Libranalysis.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
checkip.dyndns.com	Invoice...exe	Get hash	malicious	Browse	• 216.146.43.71
	Statement of Account April-2021.exe	Get hash	malicious	Browse	• 216.146.43.71
	FACTURA COMERCIAL_____ _____PDF__.exe	Get hash	malicious	Browse	• 162.88.193.70
	Technical data sheet.exe	Get hash	malicious	Browse	• 131.186.161.70
	d0875029_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.88.193.70
	SNAOUOKKOI.exe	Get hash	malicious	Browse	• 216.146.43.70
	ve #U00e7eki listesi ektedir Proforma.exe	Get hash	malicious	Browse	• 162.88.193.70
	Purchase Order 12052021.exe	Get hash	malicious	Browse	• 131.186.161.70
	Purchase Order 11052021.exe	Get hash	malicious	Browse	• 131.186.161.70
	Quotation_05082021 pdf.exe	Get hash	malicious	Browse	• 131.186.161.70
	Due Invoices.exe	Get hash	malicious	Browse	• 131.186.113.70
	Order-PO102.exe	Get hash	malicious	Browse	• 162.88.193.70
	IMG_0125_30_227_06.exe	Get hash	malicious	Browse	• 131.186.113.70
	SOA,.exe	Get hash	malicious	Browse	• 216.146.43.70
	vy38Kw9qRh.exe	Get hash	malicious	Browse	• 162.88.193.70
	SecuriteInfo.com.Trojan.GenericKD.36873970.29336.exe	Get hash	malicious	Browse	• 131.186.161.70
	q3qhElKDnGNNjTi.exe	Get hash	malicious	Browse	• 131.186.113.70
	purchase order..exe	Get hash	malicious	Browse	• 216.146.43.70
	ORDEN SURA OC CVE6535 _TVOP-MIO.exe	Get hash	malicious	Browse	• 131.186.113.70
	Quotation 68094.exe	Get hash	malicious	Browse	• 131.186.113.70
freegeoip.app	Invoice...exe	Get hash	malicious	Browse	• 172.67.188.154
	Statement of Account April-2021.exe	Get hash	malicious	Browse	• 104.21.19.200
	FACTURA COMERCIAL_____ _____PDF__.exe	Get hash	malicious	Browse	• 172.67.188.154
	Technical data sheet.exe	Get hash	malicious	Browse	• 172.67.188.154
	d0875029_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.19.200
	SNAOUOKKOI.exe	Get hash	malicious	Browse	• 104.21.19.200
	ve #U00e7eki listesi ektedir Proforma.exe	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order 12052021.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order 11052021.exe	Get hash	malicious	Browse	• 172.67.188.154
	Due Invoices.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order-PO102.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_0125_30_227_06.exe	Get hash	malicious	Browse	• 104.21.19.200
	SOA,.exe	Get hash	malicious	Browse	• 172.67.188.154
	vy38Kw9qRh.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Trojan.GenericKD.36873970.29336.exe	Get hash	malicious	Browse	• 104.21.19.200
	q3qhElKDnGNNjTi.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order..exe	Get hash	malicious	Browse	• 172.67.188.154
	ORDEN SURA OC CVE6535 _TVOP-MIO.exe	Get hash	malicious	Browse	• 104.21.19.200
	Quotation 68094.exe	Get hash	malicious	Browse	• 172.67.188.154
	DOCUMENTS AND CERTIFICATIONS.exe	Get hash	malicious	Browse	• 172.67.188.154
kerekesfoto.com	Purchase Order 12052021.exe	Get hash	malicious	Browse	• 193.32.232.10
	Purchase Order 11052021.exe	Get hash	malicious	Browse	• 193.32.232.10
	DHL Delivery Document.exe	Get hash	malicious	Browse	• 193.32.232.10
	DHL Delivery Documents.exe	Get hash	malicious	Browse	• 193.32.232.10
	Shipping Documents.exe	Get hash	malicious	Browse	• 193.32.232.10
	Shipping Documents.exe	Get hash	malicious	Browse	• 193.32.232.10
	Overdue Payment_USD.106,375.exe	Get hash	malicious	Browse	• 193.32.232.10
	Shipment Documents.exe	Get hash	malicious	Browse	• 193.32.232.10
	Proforma Invoice No.42037 USD.78116.exe	Get hash	malicious	Browse	• 193.32.232.10
	Proforma Invoice No.42037 For USD.78116.exe	Get hash	malicious	Browse	• 193.32.232.10
	Proforma Invoice No.42037.exe	Get hash	malicious	Browse	• 193.32.232.10
	Proforma Invoice No.42037.exe	Get hash	malicious	Browse	• 193.32.232.10
	Payment Copy For Confirmation_img.exe	Get hash	malicious	Browse	• 193.32.232.10
	RFQ-22100021664,pdf.exe	Get hash	malicious	Browse	• 193.32.232.10
	Overdue_Invoice 26022021.exe	Get hash	malicious	Browse	• 193.32.232.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Overdue_Invoice 25022021.exe	Get hash	malicious	Browse	• 193.32.232.10
	RFQ-22100026655Q.pdf.exe	Get hash	malicious	Browse	• 193.32.232.10
	FORM-B Airwaybill 1738623041.exe	Get hash	malicious	Browse	• 193.32.232.10
	INQUIRY-2212020.jpg.exe	Get hash	malicious	Browse	• 193.32.232.10
	bee0053.exe	Get hash	malicious	Browse	• 193.32.232.10

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DYNDNSUS	Invoice...exe	Get hash	malicious	Browse	• 216.146.43.71
	Statement of Account April-2021.exe	Get hash	malicious	Browse	• 216.146.43.71
	FACTURA COMERCIAL_____ _____PDF__.exe	Get hash	malicious	Browse	• 162.88.193.70
	Technical data sheet.exe	Get hash	malicious	Browse	• 131.186.161.70
	d0875029_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.88.193.70
	SNAOUOKKOI.exe	Get hash	malicious	Browse	• 216.146.43.70
	ve #U00e7eki listesi ektedir Proforma.exe	Get hash	malicious	Browse	• 162.88.193.70
	Purchase Order 12052021.exe	Get hash	malicious	Browse	• 131.186.161.70
	Purchase Order 11052021.exe	Get hash	malicious	Browse	• 131.186.161.70
	Quotation_05082021 pdf.exe	Get hash	malicious	Browse	• 131.186.161.70
	Due Invoices.exe	Get hash	malicious	Browse	• 131.186.113.70
	Order-PO102.exe	Get hash	malicious	Browse	• 162.88.193.70
	IMG_0125_30_227_06.exe	Get hash	malicious	Browse	• 131.186.113.70
	SOA,.exe	Get hash	malicious	Browse	• 216.146.43.70
	vy38Kw9qRh.exe	Get hash	malicious	Browse	• 162.88.193.70
	SecuriteInfo.com.Trojan.GenericKD.36873970.29336.exe	Get hash	malicious	Browse	• 131.186.161.70
	q3qhElKDnGNNjTi.exe	Get hash	malicious	Browse	• 131.186.113.70
	purchase order..exe	Get hash	malicious	Browse	• 216.146.43.70
	ORDEN SURA OC CVE6535 _TVOP-MIO.exe	Get hash	malicious	Browse	• 131.186.113.70
	Quotation 68094.exe	Get hash	malicious	Browse	• 131.186.113.70
CLOUDFLARENETUS	5781525.html	Get hash	malicious	Browse	• 172.67.150.89
	50eba5e3_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.20.184.68
	6f61bc36_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.20.185.68
	50eba5e3_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.20.184.68
	5781525.html	Get hash	malicious	Browse	• 172.67.150.89
	6f61bc36_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.20.184.68
	7e718f4b_by_Libranalysis.exe	Get hash	malicious	Browse	• 172.67.145.48
	1ChCpaSGY7.dll	Get hash	malicious	Browse	• 104.20.184.68
	1cec9342_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	M7LEWK86J8.exe	Get hash	malicious	Browse	• 104.21.13.168
	Product specification.xlsx	Get hash	malicious	Browse	• 172.67.171.184
	595e3339_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.67.156.7
	7+ Taskbar Tweaker.exe	Get hash	malicious	Browse	• 172.67.151.27
	7+ Taskbar Tweaker.exe	Get hash	malicious	Browse	• 104.21.0.149
	GmCEpa2M7R.dll	Get hash	malicious	Browse	• 104.20.185.68
	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	7bYDInO.rtf	Get hash	malicious	Browse	• 104.16.18.94
	Invoice...exe	Get hash	malicious	Browse	• 172.67.188.154
	Tek_multiloader_5.exe	Get hash	malicious	Browse	• 162.159.133.233
	PO 367628usa.exe	Get hash	malicious	Browse	• 66.235.200.147
EZIT-ASHU	Purchase Order 12052021.exe	Get hash	malicious	Browse	• 193.32.232.10
	Purchase Order 11052021.exe	Get hash	malicious	Browse	• 193.32.232.10
	DHL Delivery Document.exe	Get hash	malicious	Browse	• 193.32.232.10
	DHL Delivery Documents.exe	Get hash	malicious	Browse	• 193.32.232.10
	Shipping Documents.exe	Get hash	malicious	Browse	• 193.32.232.10
	Shipping Documents.exe	Get hash	malicious	Browse	• 193.32.232.10
	Overdue Payment_USD.106,375.exe	Get hash	malicious	Browse	• 193.32.232.10
	Shipment Documents.exe	Get hash	malicious	Browse	• 193.32.232.10
	Proforma Invoice No.42037 USD.78116.exe	Get hash	malicious	Browse	• 193.32.232.10
	Proforma Invoice No.42037 For USD.78116.exe	Get hash	malicious	Browse	• 193.32.232.10
	Proforma Invoice No.42037.exe	Get hash	malicious	Browse	• 193.32.232.10
	Proforma Invoice No.42037.exe	Get hash	malicious	Browse	• 193.32.232.10
	Payment Copy For Confirmation_img.exe	Get hash	malicious	Browse	• 193.32.232.10
	RFQ-22100021664,pdf.exe	Get hash	malicious	Browse	• 193.32.232.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Overdue_Invoice 25022021.exe	Get hash	malicious	Browse	• 193.32.232.10
	RFQ-22100026655Q.pdf.exe	Get hash	malicious	Browse	• 193.32.232.10
	FORM-B Airwaybill 1738623041.exe	Get hash	malicious	Browse	• 193.32.232.10
	INQUIRY-2212020.jpg.exe	Get hash	malicious	Browse	• 193.32.232.10
	bee0053.exe	Get hash	malicious	Browse	• 193.32.232.10
	New Bank Details..doc	Get hash	malicious	Browse	• 213.181.192.180

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Invoice...exe	Get hash	malicious	Browse	• 104.21.19.200
	Statement of Account April-2021.exe	Get hash	malicious	Browse	• 104.21.19.200
	2070121SN-WS for Woosim i250MSR.pif.exe	Get hash	malicious	Browse	• 104.21.19.200
	FACTURA COMERCIAL_____ _____PDF__.exe	Get hash	malicious	Browse	• 104.21.19.200
	Quotation.exe	Get hash	malicious	Browse	• 104.21.19.200
	Technical data sheet.exe	Get hash	malicious	Browse	• 104.21.19.200
	d0875029_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.19.200
	Account Ledger for 2020-APRIL 2021.exe	Get hash	malicious	Browse	• 104.21.19.200
	New purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	PO202104-543_ Inox Doan - Trading Co., Ltd,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	POI9090009.exe	Get hash	malicious	Browse	• 104.21.19.200
	SNAOUOKKOI.exe	Get hash	malicious	Browse	• 104.21.19.200
	ve #U00e7eki listesi ektedir Proforma.exe	Get hash	malicious	Browse	• 104.21.19.200
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order 12052021.exe	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order 11052021.exe	Get hash	malicious	Browse	• 104.21.19.200
	1578D1E95037312FDBB8E0F46F086316E68BAD3B9C8CD.exe	Get hash	malicious	Browse	• 104.21.19.200
	Due Invoices.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order-PO102.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_0125_30_227_06.exe	Get hash	malicious	Browse	• 104.21.19.200

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order_12052021.exe.log

Process:	C:\Users\user\Desktop\Purchase Order_12052021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHR
MD5:	8198C64CE0786EABD4C792E7E6FC30E5
SHA1:	71E1676126F4616B18C751A0A775B2D64944A15A
SHA-256:	C58018934011086A883D1D56B21F6C1916B1CD83206ADD1865C9BDD29DADCBC4
SHA-512:	EE293C0F88A12AB10041F66DDFAE89BC11AB3B3AAD8604F1A418ABE43DF0980245C3B7F8FEB709AEE8E9474841A280E073EC063045EA39948E853AA6B4EC0FB0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.706444670572532
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Purchase Order_12052021.exe
File size:	1000448
MD5:	b7394ccc239f48eb4a041f1c0fb92d92
SHA1:	020ae73c138a97eb413e2289822e8bacb7e15515
SHA256:	41b785e6bf871959db57c7f41ca190343a4e0fb48c0f945f776dda09c93bd8c2
SHA512:	5a6308403d41166bad0359706190d91f8b9c7a5eed7cb4a610b70767a56ec0615dd63d5f670130fd8f40a0f9047fc1a75decd3a7601f44eb88138d13f6b59403
SSDEEP:	24576:gxL+fNW9+EZ1uX+97dmn28Zv/alw+418coUy:7W9Ndmn3Zv/D3V
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....~..... ....@.. .....@.....

File Icon

Icon Hash:	90828c8c8c8a9010

Static PE Info

General

Entrypoint:	0x4fa00a
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609B8AFC [Wed May 12 07:59:56 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [004FA000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc08dc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xcc000	0x2ab28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf8000	0xc	.reloc
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	0xfa000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0xc0000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
NLNe	0x2000	0xbcfe8	0xbd000	False	1.00031777034	data	7.99974141279	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0xc0000	0xbe88	0xc000	False	0.443725585938	data	5.99098442222	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xcc000	0x2ab28	0x2ac00	False	0.141778600146	data	4.57824829919	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf8000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0xfa000	0x10	0x200	False	0.044921875	dBase III DBT, version number 0, next free block index 788752	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xcc2e0	0x2270	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xce550	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xded78	0x94a8	data		
RT_ICON	0xe8220	0x5488	data		
RT_ICON	0xed6a8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967055		
RT_ICON	0xf18d0	0x25a8	data		
RT_ICON	0xf3e78	0x10a8	data		
RT_ICON	0xf4f20	0x988	data		
RT_ICON	0xf58a8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xf5d10	0x84	data		
RT_GROUP_ICON	0xf5d94	0x14	data		
RT_VERSION	0xf5da8	0x314	data		
RT_MANIFEST	0xf60bc	0xa65	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	36.27.47.25
InternalName	ContextAttribute.exe
FileVersion	82.99.17.85
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	82.99.17.85
FileDescription	
OriginalFilename	ContextAttribute.exe

Network Behavior

Network Port Distribution

Total Packets: 115

- 53 (DNS)
- 587 undefined
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:38:16.958307981 CEST	49726	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:17.018596888 CEST	80	49726	216.146.43.71	192.168.2.3
May 12, 2021 22:38:17.019165993 CEST	49726	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:17.019448996 CEST	49726	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:17.079544067 CEST	80	49726	216.146.43.71	192.168.2.3
May 12, 2021 22:38:17.079794884 CEST	80	49726	216.146.43.71	192.168.2.3
May 12, 2021 22:38:17.079826117 CEST	80	49726	216.146.43.71	192.168.2.3
May 12, 2021 22:38:17.080029964 CEST	49726	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:17.080986977 CEST	49726	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:17.141161919 CEST	80	49726	216.146.43.71	192.168.2.3
May 12, 2021 22:38:17.395709991 CEST	49727	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:17.456341982 CEST	80	49727	216.146.43.71	192.168.2.3
May 12, 2021 22:38:17.456507921 CEST	49727	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:17.457448006 CEST	49727	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:17.517885923 CEST	80	49727	216.146.43.71	192.168.2.3
May 12, 2021 22:38:17.517930984 CEST	80	49727	216.146.43.71	192.168.2.3
May 12, 2021 22:38:17.517957926 CEST	80	49727	216.146.43.71	192.168.2.3
May 12, 2021 22:38:17.518040895 CEST	49727	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:17.519391060 CEST	49727	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:17.580168962 CEST	80	49727	216.146.43.71	192.168.2.3
May 12, 2021 22:38:20.387667894 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:20.430658102 CEST	443	49729	104.21.19.200	192.168.2.3
May 12, 2021 22:38:20.432112932 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:20.468041897 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:20.509073019 CEST	443	49729	104.21.19.200	192.168.2.3
May 12, 2021 22:38:20.511553049 CEST	443	49729	104.21.19.200	192.168.2.3
May 12, 2021 22:38:20.511599064 CEST	443	49729	104.21.19.200	192.168.2.3
May 12, 2021 22:38:20.511950016 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:20.519567966 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:20.560606956 CEST	443	49729	104.21.19.200	192.168.2.3
May 12, 2021 22:38:20.560806990 CEST	443	49729	104.21.19.200	192.168.2.3
May 12, 2021 22:38:20.611787081 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:20.830530882 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:20.873151064 CEST	443	49729	104.21.19.200	192.168.2.3
May 12, 2021 22:38:20.887747049 CEST	443	49729	104.21.19.200	192.168.2.3
May 12, 2021 22:38:20.939893007 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:21.739523888 CEST	49730	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:21.800215006 CEST	80	49730	216.146.43.71	192.168.2.3
May 12, 2021 22:38:21.800298929 CEST	49730	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:21.800576925 CEST	49730	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:21.869107962 CEST	80	49730	216.146.43.71	192.168.2.3
May 12, 2021 22:38:21.869155884 CEST	80	49730	216.146.43.71	192.168.2.3
May 12, 2021 22:38:21.869188070 CEST	80	49730	216.146.43.71	192.168.2.3
May 12, 2021 22:38:21.869293928 CEST	49730	80	192.168.2.3	216.146.43.71

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:38:21.869544029 CEST	49730	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:21.870023012 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:21.929929018 CEST	80	49730	216.146.43.71	192.168.2.3
May 12, 2021 22:38:21.939834118 CEST	443	49729	104.21.19.200	192.168.2.3
May 12, 2021 22:38:21.987425089 CEST	49731	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:22.048624992 CEST	80	49731	216.146.43.71	192.168.2.3
May 12, 2021 22:38:22.048805952 CEST	49731	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:22.049122095 CEST	49731	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:22.096214056 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:22.109622002 CEST	80	49731	216.146.43.71	192.168.2.3
May 12, 2021 22:38:22.109713078 CEST	80	49731	216.146.43.71	192.168.2.3
May 12, 2021 22:38:22.109755993 CEST	80	49731	216.146.43.71	192.168.2.3
May 12, 2021 22:38:22.109821081 CEST	49731	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:22.110146999 CEST	49731	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:22.110704899 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:22.170557976 CEST	80	49731	216.146.43.71	192.168.2.3
May 12, 2021 22:38:22.170661926 CEST	443	49729	104.21.19.200	192.168.2.3
May 12, 2021 22:38:22.226885080 CEST	49732	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:22.287388086 CEST	80	49732	216.146.43.71	192.168.2.3
May 12, 2021 22:38:22.287503004 CEST	49732	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:22.287869930 CEST	49732	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:22.348252058 CEST	80	49732	216.146.43.71	192.168.2.3
May 12, 2021 22:38:22.348305941 CEST	80	49732	216.146.43.71	192.168.2.3
May 12, 2021 22:38:22.348346949 CEST	80	49732	216.146.43.71	192.168.2.3
May 12, 2021 22:38:22.348437071 CEST	49732	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:22.348776102 CEST	49732	80	192.168.2.3	216.146.43.71
May 12, 2021 22:38:22.394833088 CEST	49729	443	192.168.2.3	104.21.19.200
May 12, 2021 22:38:22.408984900 CEST	80	49732	216.146.43.71	192.168.2.3
May 12, 2021 22:38:25.681958914 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:25.734335899 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:25.734426975 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:25.888634920 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:25.888964891 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:25.940056086 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:25.940434933 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:25.994430065 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:25.995282888 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:26.055994987 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:26.056063890 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:26.056093931 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:26.056401014 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:26.061367989 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:26.113342047 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:26.145499945 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:26.197482109 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:26.202594995 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:26.254532099 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:26.259999990 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:26.318891048 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:26.323026896 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:26.374403954 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:26.376019001 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:26.448369026 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:26.452624083 CEST	49733	587	192.168.2.3	193.32.232.10
May 12, 2021 22:38:26.504405022 CEST	587	49733	193.32.232.10	192.168.2.3
May 12, 2021 22:38:26.507388115 CEST	49733	587	192.168.2.3	193.32.232.10

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:37:58.213320971 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 22:37:58.273494959 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 22:37:58.413022041 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 22:37:58.471400976 CEST	53	64185	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:37:59.252942085 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 22:37:59.304204941 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 22:38:00.336466074 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:00.397910118 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 22:38:01.446651936 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:01.495640039 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 22:38:02.757764101 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:02.809500933 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 22:38:04.137573004 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:04.194076061 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 22:38:04.949498892 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:05.002468109 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 22:38:06.051246881 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:06.131366968 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 22:38:06.949109077 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:07.002259016 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 22:38:08.083487034 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:08.141014099 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 22:38:09.442200899 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:09.491264105 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 22:38:11.372591019 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:11.421771049 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 22:38:12.450375080 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:12.499358892 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 22:38:13.403558969 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:13.455456972 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 22:38:14.520730019 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:14.578058958 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 22:38:15.329224110 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:15.378103018 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 22:38:16.629599094 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:16.681246042 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 22:38:16.815216064 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:16.865921021 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 22:38:16.884315968 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:16.933489084 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 22:38:17.445800066 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:17.494831085 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 22:38:20.313523054 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:20.373222113 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 22:38:25.605627060 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:25.680619001 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 22:38:28.907752991 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:28.982994080 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 22:38:31.068948030 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:31.128180981 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 22:38:31.971414089 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:32.028805017 CEST	53	60633	8.8.8.8	192.168.2.3
May 12, 2021 22:38:35.166553020 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:35.224009037 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 22:38:35.247884035 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:35.324811935 CEST	53	63619	8.8.8.8	192.168.2.3
May 12, 2021 22:38:38.640727997 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:38.697876930 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 22:38:43.419976950 CEST	61946	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:43.477114916 CEST	53	61946	8.8.8.8	192.168.2.3
May 12, 2021 22:38:44.685746908 CEST	64910	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:44.749908924 CEST	53	64910	8.8.8.8	192.168.2.3
May 12, 2021 22:38:46.559391975 CEST	52123	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:46.621087074 CEST	53	52123	8.8.8.8	192.168.2.3
May 12, 2021 22:38:49.622297049 CEST	56130	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:49.679780006 CEST	53	56130	8.8.8.8	192.168.2.3
May 12, 2021 22:38:52.820677996 CEST	56338	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:52.870800972 CEST	53	56338	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:38:54.448149920 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:54.497184992 CEST	53	59420	8.8.8.8	192.168.2.3
May 12, 2021 22:38:55.897001028 CEST	58784	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:55.954440117 CEST	53	58784	8.8.8.8	192.168.2.3
May 12, 2021 22:38:59.266124964 CEST	63978	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:59.338529110 CEST	53	63978	8.8.8.8	192.168.2.3
May 12, 2021 22:38:59.398322105 CEST	62938	53	192.168.2.3	8.8.8.8
May 12, 2021 22:38:59.457496881 CEST	53	62938	8.8.8.8	192.168.2.3
May 12, 2021 22:39:02.457098007 CEST	55708	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:02.507409096 CEST	53	55708	8.8.8.8	192.168.2.3
May 12, 2021 22:39:05.432210922 CEST	56803	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:05.489253998 CEST	53	56803	8.8.8.8	192.168.2.3
May 12, 2021 22:39:06.898775101 CEST	57145	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:06.964095116 CEST	53	57145	8.8.8.8	192.168.2.3
May 12, 2021 22:39:08.430386066 CEST	55359	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:08.488847017 CEST	53	55359	8.8.8.8	192.168.2.3
May 12, 2021 22:39:10.884529114 CEST	58306	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:10.946517944 CEST	53	58306	8.8.8.8	192.168.2.3
May 12, 2021 22:39:11.530456066 CEST	64124	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:11.588121891 CEST	53	64124	8.8.8.8	192.168.2.3
May 12, 2021 22:39:14.703941107 CEST	49361	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:14.762492895 CEST	53	49361	8.8.8.8	192.168.2.3
May 12, 2021 22:39:17.914963007 CEST	63150	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:17.974919081 CEST	53	63150	8.8.8.8	192.168.2.3
May 12, 2021 22:39:21.034949064 CEST	53279	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:21.083796024 CEST	53	53279	8.8.8.8	192.168.2.3
May 12, 2021 22:39:24.059741020 CEST	56881	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:24.112306118 CEST	53	56881	8.8.8.8	192.168.2.3
May 12, 2021 22:39:27.093197107 CEST	53642	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:27.169698954 CEST	53	53642	8.8.8.8	192.168.2.3
May 12, 2021 22:39:30.150273085 CEST	55667	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:30.199141979 CEST	53	55667	8.8.8.8	192.168.2.3
May 12, 2021 22:39:33.218732119 CEST	54833	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:33.278842926 CEST	53	54833	8.8.8.8	192.168.2.3
May 12, 2021 22:39:36.183789968 CEST	62476	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:36.244046926 CEST	53	62476	8.8.8.8	192.168.2.3
May 12, 2021 22:39:39.161453009 CEST	49705	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:39.218348026 CEST	53	49705	8.8.8.8	192.168.2.3
May 12, 2021 22:39:41.990964890 CEST	61477	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:42.058876038 CEST	53	61477	8.8.8.8	192.168.2.3
May 12, 2021 22:39:42.126431942 CEST	61633	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:42.174977064 CEST	53	61633	8.8.8.8	192.168.2.3
May 12, 2021 22:39:43.538593054 CEST	55949	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:43.597984076 CEST	53	55949	8.8.8.8	192.168.2.3
May 12, 2021 22:39:45.227268934 CEST	57601	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:45.284483910 CEST	53	57601	8.8.8.8	192.168.2.3
May 12, 2021 22:39:49.036335945 CEST	49342	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:49.087858915 CEST	53	49342	8.8.8.8	192.168.2.3
May 12, 2021 22:39:52.017132998 CEST	56253	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:52.066236019 CEST	53	56253	8.8.8.8	192.168.2.3
May 12, 2021 22:39:55.092850924 CEST	49667	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:55.141856909 CEST	53	49667	8.8.8.8	192.168.2.3
May 12, 2021 22:39:58.089673042 CEST	55439	53	192.168.2.3	8.8.8.8
May 12, 2021 22:39:58.138381958 CEST	53	55439	8.8.8.8	192.168.2.3
May 12, 2021 22:40:01.081578016 CEST	57069	53	192.168.2.3	8.8.8.8
May 12, 2021 22:40:01.130450010 CEST	53	57069	8.8.8.8	192.168.2.3
May 12, 2021 22:40:04.389478922 CEST	57659	53	192.168.2.3	8.8.8.8
May 12, 2021 22:40:04.446754932 CEST	53	57659	8.8.8.8	192.168.2.3
May 12, 2021 22:40:07.376486063 CEST	54717	53	192.168.2.3	8.8.8.8
May 12, 2021 22:40:07.433969975 CEST	53	54717	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 22:38:16.815216064 CEST	192.168.2.3	8.8.8.8	0x5d66	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
May 12, 2021 22:38:16.884315968 CEST	192.168.2.3	8.8.8.8	0x1a54	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
May 12, 2021 22:38:20.313523054 CEST	192.168.2.3	8.8.8.8	0x826c	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)
May 12, 2021 22:38:25.605627060 CEST	192.168.2.3	8.8.8.8	0xbc4f	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:38:28.907752991 CEST	192.168.2.3	8.8.8.8	0x121a	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:38:31.971414089 CEST	192.168.2.3	8.8.8.8	0x6249	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:38:35.166553020 CEST	192.168.2.3	8.8.8.8	0xf492	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:38:38.640727997 CEST	192.168.2.3	8.8.8.8	0xbcbb	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:38:43.419976950 CEST	192.168.2.3	8.8.8.8	0xc95c	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:38:46.559391975 CEST	192.168.2.3	8.8.8.8	0xf58d	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:38:49.622297049 CEST	192.168.2.3	8.8.8.8	0x842a	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:38:52.820677996 CEST	192.168.2.3	8.8.8.8	0x9bb5	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:38:55.897001028 CEST	192.168.2.3	8.8.8.8	0x9437	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:38:59.398322105 CEST	192.168.2.3	8.8.8.8	0xdefd	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:02.457098007 CEST	192.168.2.3	8.8.8.8	0xfbde	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:05.432210922 CEST	192.168.2.3	8.8.8.8	0x9b57	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:08.430386066 CEST	192.168.2.3	8.8.8.8	0xdac0	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:11.530456066 CEST	192.168.2.3	8.8.8.8	0x3eed	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:14.703941107 CEST	192.168.2.3	8.8.8.8	0xb8e2	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:17.914963007 CEST	192.168.2.3	8.8.8.8	0x6f9	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:21.034949064 CEST	192.168.2.3	8.8.8.8	0xec0c	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:24.059741020 CEST	192.168.2.3	8.8.8.8	0xc16c	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:27.093197107 CEST	192.168.2.3	8.8.8.8	0xfb52	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:30.150273085 CEST	192.168.2.3	8.8.8.8	0x4c0d	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:33.218732119 CEST	192.168.2.3	8.8.8.8	0x5b88	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:36.183789968 CEST	192.168.2.3	8.8.8.8	0x1d14	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:39.161453009 CEST	192.168.2.3	8.8.8.8	0x1aa4	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:42.126431942 CEST	192.168.2.3	8.8.8.8	0xb033	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:45.227268934 CEST	192.168.2.3	8.8.8.8	0x941b	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:49.036335945 CEST	192.168.2.3	8.8.8.8	0x31d7	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:52.017132998 CEST	192.168.2.3	8.8.8.8	0x1f18	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:55.092850924 CEST	192.168.2.3	8.8.8.8	0xceb3	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:39:58.089673042 CEST	192.168.2.3	8.8.8.8	0x388c	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:40:01.081578016 CEST	192.168.2.3	8.8.8.8	0x6513	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:40:04.389478922 CEST	192.168.2.3	8.8.8.8	0xdd97	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:40:07.376486063 CEST	192.168.2.3	8.8.8.8	0x17b1	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 22:38:16.865921021 CEST	8.8.8.8	192.168.2.3	0x5d66	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 22:38:16.865921021 CEST	8.8.8.8	192.168.2.3	0x5d66	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
May 12, 2021 22:38:16.865921021 CEST	8.8.8.8	192.168.2.3	0x5d66	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
May 12, 2021 22:38:16.865921021 CEST	8.8.8.8	192.168.2.3	0x5d66	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
May 12, 2021 22:38:16.865921021 CEST	8.8.8.8	192.168.2.3	0x5d66	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
May 12, 2021 22:38:16.865921021 CEST	8.8.8.8	192.168.2.3	0x5d66	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
May 12, 2021 22:38:16.933489084 CEST	8.8.8.8	192.168.2.3	0x1a54	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 22:38:16.933489084 CEST	8.8.8.8	192.168.2.3	0x1a54	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
May 12, 2021 22:38:16.933489084 CEST	8.8.8.8	192.168.2.3	0x1a54	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
May 12, 2021 22:38:16.933489084 CEST	8.8.8.8	192.168.2.3	0x1a54	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
May 12, 2021 22:38:16.933489084 CEST	8.8.8.8	192.168.2.3	0x1a54	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
May 12, 2021 22:38:16.933489084 CEST	8.8.8.8	192.168.2.3	0x1a54	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
May 12, 2021 22:38:20.373222113 CEST	8.8.8.8	192.168.2.3	0x826c	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
May 12, 2021 22:38:20.373222113 CEST	8.8.8.8	192.168.2.3	0x826c	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
May 12, 2021 22:38:25.680619001 CEST	8.8.8.8	192.168.2.3	0xbc4f	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:38:28.982994080 CEST	8.8.8.8	192.168.2.3	0x121a	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:38:32.028805017 CEST	8.8.8.8	192.168.2.3	0x6249	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:38:35.224009037 CEST	8.8.8.8	192.168.2.3	0xf492	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:38:38.697876930 CEST	8.8.8.8	192.168.2.3	0xbcbb	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:38:43.477114916 CEST	8.8.8.8	192.168.2.3	0xc95c	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:38:46.621087074 CEST	8.8.8.8	192.168.2.3	0xf58d	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:38:49.679780006 CEST	8.8.8.8	192.168.2.3	0x842a	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:38:52.870800972 CEST	8.8.8.8	192.168.2.3	0x9bb5	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:38:55.954440117 CEST	8.8.8.8	192.168.2.3	0x9437	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:38:59.457496881 CEST	8.8.8.8	192.168.2.3	0xdefd	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:02.507409096 CEST	8.8.8.8	192.168.2.3	0xfbde	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 22:39:05.489253998 CEST	8.8.8.8	192.168.2.3	0x9b57	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:08.488847017 CEST	8.8.8.8	192.168.2.3	0xdac0	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:11.588121891 CEST	8.8.8.8	192.168.2.3	0x3eed	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:14.762492895 CEST	8.8.8.8	192.168.2.3	0xb8e2	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:17.974919081 CEST	8.8.8.8	192.168.2.3	0x6f9	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:21.083796024 CEST	8.8.8.8	192.168.2.3	0xec0c	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:24.112306118 CEST	8.8.8.8	192.168.2.3	0xc16c	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:27.169698954 CEST	8.8.8.8	192.168.2.3	0xfb52	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:30.199141979 CEST	8.8.8.8	192.168.2.3	0x4c0d	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:33.278842926 CEST	8.8.8.8	192.168.2.3	0x5b88	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:36.244046926 CEST	8.8.8.8	192.168.2.3	0x1d14	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:39.218348026 CEST	8.8.8.8	192.168.2.3	0x1aa4	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:42.174977064 CEST	8.8.8.8	192.168.2.3	0xb033	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:45.284483910 CEST	8.8.8.8	192.168.2.3	0x941b	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:49.087858915 CEST	8.8.8.8	192.168.2.3	0x31d7	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:52.066236019 CEST	8.8.8.8	192.168.2.3	0x1f18	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:55.141856909 CEST	8.8.8.8	192.168.2.3	0xceb3	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:39:58.138381958 CEST	8.8.8.8	192.168.2.3	0x388c	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:40:01.130450010 CEST	8.8.8.8	192.168.2.3	0x6513	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:40:04.446754932 CEST	8.8.8.8	192.168.2.3	0xdd97	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:40:07.433969975 CEST	8.8.8.8	192.168.2.3	0x17b1	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49726	216.146.43.71	80	C:\Users\user\Desktop\Purchase Order_12052021.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:38:17.019448996 CEST	1295	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
May 12, 2021 22:38:17.079794884 CEST	1298	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.78</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49727	216.146.43.71	80	C:\Users\user\Desktop\Purchase Order_12052021.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:38:17.457448006 CEST	1303	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
May 12, 2021 22:38:17.517930984 CEST	1304	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.78</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49730	216.146.43.71	80	C:\Users\user\Desktop\Purchase Order_12052021.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:38:21.800576925 CEST	1322	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
May 12, 2021 22:38:21.869155884 CEST	1323	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.78</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49731	216.146.43.71	80	C:\Users\user\Desktop\Purchase Order_12052021.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:38:22.049122095 CEST	1325	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
May 12, 2021 22:38:22.109713078 CEST	1325	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.78</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49732	216.146.43.71	80	C:\Users\user\Desktop\Purchase Order_12052021.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:38:22.287869930 CEST	1327	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
May 12, 2021 22:38:22.348305941 CEST	1328	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.78</body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 22:38:20.511599064 CEST	104.21.19.200	443	192.168.2.3	49729	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 10 02:00:00 CEST 2020	Tue Aug 10 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 22:38:25.888634920 CEST	587	49733	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:25 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:25.888964891 CEST	49733	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:25.940056086 CEST	587	49733	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:25.940434933 CEST	49733	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:25.994430065 CEST	587	49733	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:38:29.132107973 CEST	587	49734	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:29 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:29.132386923 CEST	49734	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:29.183377028 CEST	587	49734	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:29.183686018 CEST	49734	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:29.236675978 CEST	587	49734	193.32.232.10	192.168.2.3	220 TLS go ahead

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 22:38:32.197485924 CEST	587	49738	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:32 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:32.197793961 CEST	49738	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:32.251027107 CEST	587	49738	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:32.251337051 CEST	49738	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:32.305463076 CEST	587	49738	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:38:35.409621954 CEST	587	49741	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:35 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:35.410235882 CEST	49741	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:35.461461067 CEST	587	49741	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:35.465526104 CEST	49741	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:35.519682884 CEST	587	49741	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:38:38.952658892 CEST	587	49743	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:38 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:39.633022070 CEST	49743	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:39.684560061 CEST	587	49743	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:39.695327044 CEST	49743	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:39.749614954 CEST	587	49743	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:38:43.651684999 CEST	587	49744	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:43 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:43.653548002 CEST	49744	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:43.704747915 CEST	587	49744	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:43.704968929 CEST	49744	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:43.758624077 CEST	587	49744	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:38:46.768477917 CEST	587	49746	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:46 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:46.768723965 CEST	49746	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:46.819967031 CEST	587	49746	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:46.820465088 CEST	49746	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:46.874376059 CEST	587	49746	193.32.232.10	192.168.2.3	220 TLS go ahead

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 22:38:49.828669071 CEST	587	49747	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:49 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:49.828953981 CEST	49747	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:49.880079985 CEST	587	49747	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:49.880336046 CEST	49747	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:49.934228897 CEST	587	49747	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:38:53.038117886 CEST	587	49748	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:53 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:53.038378000 CEST	49748	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:53.089189053 CEST	587	49748	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:53.089417934 CEST	49748	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:53.143671989 CEST	587	49748	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:38:56.103802919 CEST	587	49750	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:56 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:56.104031086 CEST	49750	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:56.154942989 CEST	587	49750	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:56.155219078 CEST	49750	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:56.207966089 CEST	587	49750	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:38:59.609776020 CEST	587	49752	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:38:59 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:38:59.610115051 CEST	49752	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:38:59.662581921 CEST	587	49752	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:38:59.662812948 CEST	49752	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:38:59.719470024 CEST	587	49752	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:02.657814980 CEST	587	49753	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:02 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:02.658160925 CEST	49753	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:02.710290909 CEST	587	49753	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:02.714019060 CEST	49753	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:02.766189098 CEST	587	49753	193.32.232.10	192.168.2.3	220 TLS go ahead

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 22:39:05.641846895 CEST	587	49754	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:05 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:05.642152071 CEST	49754	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:05.695974112 CEST	587	49754	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:05.696294069 CEST	49754	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:05.751768112 CEST	587	49754	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:08.637576103 CEST	587	49758	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:08 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:08.637857914 CEST	49758	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:08.689131021 CEST	587	49758	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:08.689454079 CEST	49758	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:08.742544889 CEST	587	49758	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:11.723929882 CEST	587	49764	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:11 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:11.724150896 CEST	49764	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:11.777328968 CEST	587	49764	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:11.777564049 CEST	49764	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:11.831804991 CEST	587	49764	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:14.937293053 CEST	587	49765	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:14 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:14.937505007 CEST	49765	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:14.989166975 CEST	587	49765	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:14.989521027 CEST	49765	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:15.043912888 CEST	587	49765	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:18.134459972 CEST	587	49766	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:18 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:18.134676933 CEST	49766	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:18.185771942 CEST	587	49766	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:18.186606884 CEST	49766	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:18.241451025 CEST	587	49766	193.32.232.10	192.168.2.3	220 TLS go ahead

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 22:39:21.235661030 CEST	587	49767	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:21 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:21.235918999 CEST	49767	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:21.286895037 CEST	587	49767	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:21.287137985 CEST	49767	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:21.342760086 CEST	587	49767	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:24.248783112 CEST	587	49768	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:24 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:24.249223948 CEST	49768	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:24.300992012 CEST	587	49768	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:24.301321030 CEST	49768	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:24.355427980 CEST	587	49768	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:27.319574118 CEST	587	49769	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:27 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:27.320009947 CEST	49769	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:27.371115923 CEST	587	49769	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:27.371406078 CEST	49769	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:27.424992085 CEST	587	49769	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:30.373985052 CEST	587	49770	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:30 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:30.374295950 CEST	49770	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:30.425327063 CEST	587	49770	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:30.425825119 CEST	49770	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:30.480844021 CEST	587	49770	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:33.429408073 CEST	587	49771	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:33 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:33.429811001 CEST	49771	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:33.480855942 CEST	587	49771	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:33.481534958 CEST	49771	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:33.535408974 CEST	587	49771	193.32.232.10	192.168.2.3	220 TLS go ahead

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 22:39:36.366501093 CEST	587	49772	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:36 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:36.367079973 CEST	49772	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:36.420277119 CEST	587	49772	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:36.420774937 CEST	49772	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:36.474345922 CEST	587	49772	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:39.355858088 CEST	587	49773	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:39 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:39.356250048 CEST	49773	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:39.407392979 CEST	587	49773	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:39.407771111 CEST	49773	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:39.460494041 CEST	587	49773	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:42.323086977 CEST	587	49775	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:42 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:42.323323011 CEST	49775	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:42.374231100 CEST	587	49775	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:42.374475002 CEST	49775	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:42.428234100 CEST	587	49775	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:45.408426046 CEST	587	49777	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:45 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:45.478759050 CEST	49777	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:45.529841900 CEST	587	49777	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:46.301451921 CEST	49777	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:46.354165077 CEST	587	49777	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:49.210824966 CEST	587	49778	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:49 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:49.211108923 CEST	49778	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:49.263716936 CEST	587	49778	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:49.263982058 CEST	49778	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:49.317442894 CEST	587	49778	193.32.232.10	192.168.2.3	220 TLS go ahead

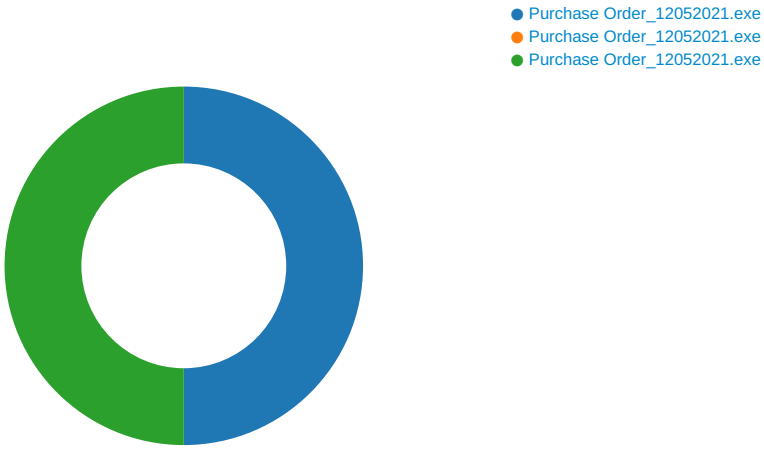
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 22:39:52.201212883 CEST	587	49779	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:52 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:52.201488018 CEST	49779	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:52.252479076 CEST	587	49779	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:52.252757072 CEST	49779	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:52.306229115 CEST	587	49779	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:55.288948059 CEST	587	49780	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:55 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:55.289232969 CEST	49780	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:55.340248108 CEST	587	49780	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:55.340534925 CEST	49780	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:55.393441916 CEST	587	49780	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:39:58.274290085 CEST	587	49781	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:39:58 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:39:58.274861097 CEST	49781	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:39:58.325934887 CEST	587	49781	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:39:58.326565027 CEST	49781	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:39:58.382201910 CEST	587	49781	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:40:01.266908884 CEST	587	49782	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:40:01 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:40:01.267385006 CEST	49782	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:40:01.318660975 CEST	587	49782	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:40:01.319211960 CEST	49782	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:40:01.373903990 CEST	587	49782	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:40:04.583982944 CEST	587	49783	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:40:04 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:40:04.584485054 CEST	49783	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:40:04.636044025 CEST	587	49783	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:40:04.636786938 CEST	49783	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:40:04.691268921 CEST	587	49783	193.32.232.10	192.168.2.3	220 TLS go ahead

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 22:40:07.555665970 CEST	587	49784	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:40:07 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:40:07.556175947 CEST	49784	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:40:07.607218981 CEST	587	49784	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:40:07.610018015 CEST	49784	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:40:07.664122105 CEST	587	49784	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:40:10.449016094 CEST	587	49785	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:40:10 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:40:10.449266911 CEST	49785	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:40:10.500260115 CEST	587	49785	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:40:10.500489950 CEST	49785	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:40:10.554462910 CEST	587	49785	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:40:13.378196001 CEST	587	49786	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:40:13 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:40:13.378406048 CEST	49786	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:40:13.429666996 CEST	587	49786	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:40:13.429955006 CEST	49786	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:40:13.483539104 CEST	587	49786	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:40:16.292247057 CEST	587	49787	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:40:16 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:40:16.292386055 CEST	49787	587	192.168.2.3	193.32.232.10	EHLO 114127
May 12, 2021 22:40:16.343879938 CEST	587	49787	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 114127 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 22:40:16.345164061 CEST	49787	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:40:16.399250031 CEST	587	49787	193.32.232.10	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Purchase Order_12052021.exe PID: 3560 Parent PID: 5640

General

Start time:	22:38:04
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Purchase Order_12052021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order_12052021.exe'
Imagebase:	0x3b0000
File size:	1000448 bytes
MD5 hash:	B7394CCC239F48EB4A041F1C0FB92D92
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.219914273.0000000002864000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000000.00000002.222285515.0000000003864000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.222285515.0000000003864000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.222285515.0000000003864000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E12CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E12CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order_12052021.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E43C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order_12052021.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"Microsoft.VisualBasic, Ver	success or wait	1	6E43C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E105705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E10CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile

Analysis Process: Purchase Order_12052021.exe PID: 404 Parent PID: 3560

General

Start time:	22:38:12
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Purchase Order_12052021.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Purchase Order_12052021.exe
Imagebase:	0x310000
File size:	1000448 bytes
MD5 hash:	B7394CCC239F48EB4A041F1C0FB92D92
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Purchase Order_12052021.exe PID: 2792 Parent PID: 3560

General

Start time:	22:38:13
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Purchase Order_12052021.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Order_12052021.exe
Imagebase:	0x960000
File size:	1000448 bytes
MD5 hash:	B7394CCC239F48EB4A041F1C0FB92D92
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.470992091.0000000002DC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000003.00000002.467511051.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000003.00000002.467511051.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.467511051.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E12CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E12CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	success or wait	1	6CF76A95	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	success or wait	1	6CF76A95	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	success or wait	1	6CF76A95	DeleteFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E105705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E10CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF71B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF71B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis