ID: 412757
Sample Name: e.exe
Cookbook: default.jbs
Time: 22:52:21
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report e.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Networking: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 11
Private 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASN 14
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 16
General 16
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 16
Data Directories 18
Sections 18

Resources 18
Imports 19
Version Infos 19
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 21
DNS Queries 23
DNS Answers 24
HTTP Request Dependency Graph 26
HTTP Packets 26
HTTPS Packets 27
SMTP Packets 28
Code Manipulations 36
Statistics 36
System Behavior 36
Analysis Process: e.exe PID: 6132 Parent PID: 5688 36
General 36
File Activities 36
File Created 36
File Deleted 36
File Read 37
Registry Activities 37
Disassembly 37
Code Analysis 37

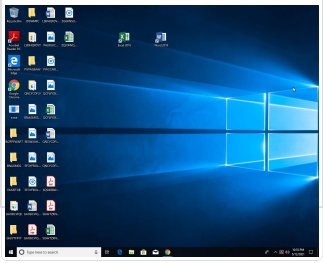
Analysis Report e.exe

Overview

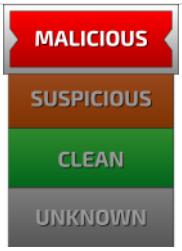
General Information

Sample Name:	e.exe
Analysis ID:	412757
MD5:	c69ddcf0dd4be5b..
SHA1:	4a1113c4889518..
SHA256:	31b5237e182f6a2.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



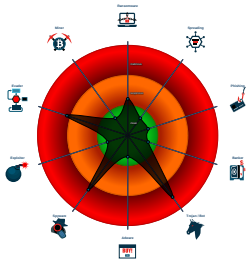
AgentTesla Matiex

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected Matiex Keylogger
- Machine Learning detection for samp…
- May check the online IP address of …
- Tries to harvest and steal browser in…
- Tries to steal Mail credentials (via fil…
- Yara detected Beds Obfuscator
- Antivirus or Machine Learning detec…
- Contains functionality to access load…
- Contains long sleeps (>= 3 min)

Classification



Startup

- **System is w10x64**
- e.exe (PID: 6132 cmdline: 'C:\Users\user\Desktop\e.exe' MD5: C69DDCF0DD4BE5B729D10475408A468C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
e.exe	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
e.exe	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
e.exe	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.461405433.000000000266 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000000.191074513.000000000030 2000.00000002.00020000.sdmp	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
00000000.00000000.191074513.000000000030 2000.00000002.00020000.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
00000000.00000000.191074513.000000000030 2000.00000002.00020000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.458925410.000000000030 2000.00000002.00020000.sdmp	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
Click to see the 5 entries				

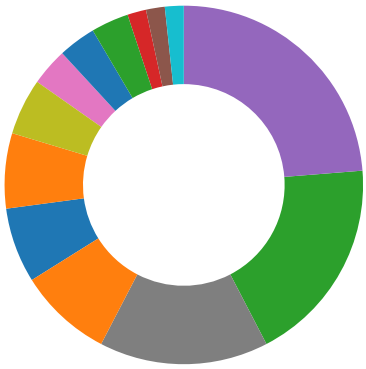
Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.e.exe.3224d4.1.raw.unpack	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
0.0.e.exe.3224d4.1.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.e.exe.3224d4.1.raw.unpack	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
0.2.e.exe.3224d4.1.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.0.e.exe.300000.0.unpack	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- 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

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

May check the online IP address of the machine

Data Obfuscation:

Yara detected Beds Obfuscator

Malware Analysis System Evasion:

Yara detected Beds Obfuscator

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:

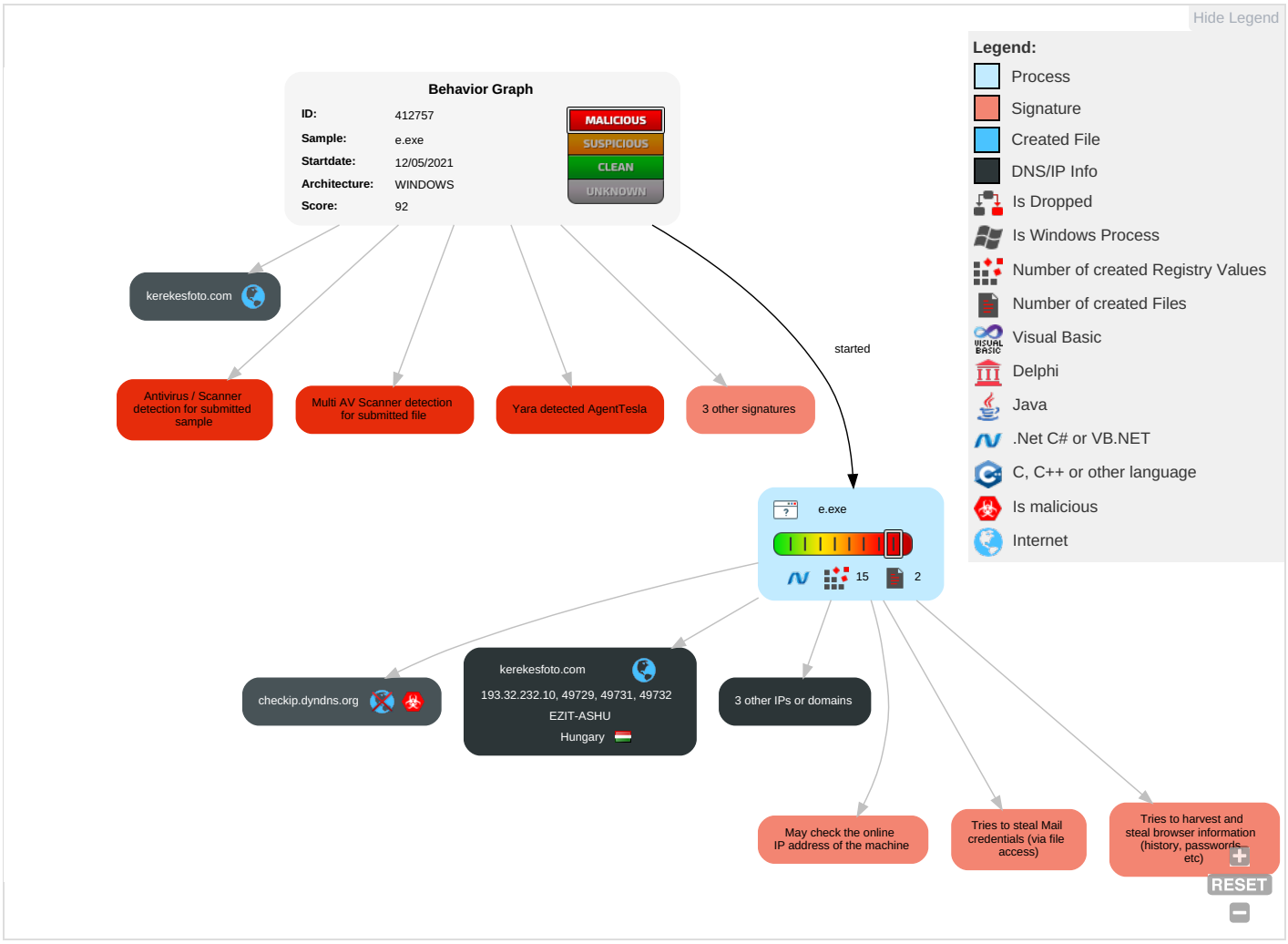
Yara detected AgentTesla

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	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1	Disable or Modify Tools 1	OS Credential Dumping 1	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdr Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Ingress Tool Transfer 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 3	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

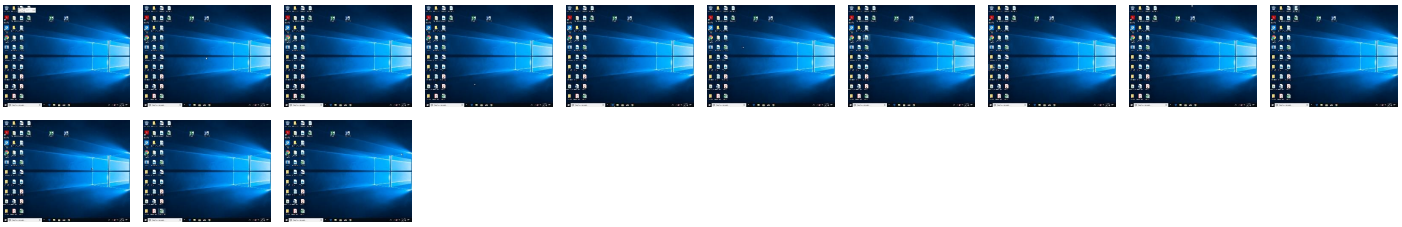
Behavior Graph



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
e.exe	60%	ReversingLabs	ByteCode-MSIL.Spyware.Matiex	
e.exe	100%	Avira	TR/Redcap.jajcu	
e.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.e.exe.300000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File
0.0.e.exe.300000.0.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

Source	Detection	Scanner	Label	Link
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://checkip.dyndns.org/	0%	Virustotal		Browse
http://checkip.dyndns.org/	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://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	0%	URL Reputation	safe	
http://https://www.geodatatool.com/en/?ip=3D84.17.52.78=0D=0A=0D=0ADat=	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/HB	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://https://freegeoip.app	0%	URL Reputation	safe	
http://https://www.geodatatool.com/en/?ip=84.17.52.78	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://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://wackip.dyndns.org/	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	172.67.188.154	true	false	• 1%, Virustotal, Browse	unknown
checkip.dyndns.com	162.88.193.70	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	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://freegeoip.app/xml/	e.exe, 00000000.00000002.46148 4579.0000000002694000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://freegeoip.app/xml/LoadTimeZoneCountryNameCountryCodehttps://www.geodatatool.com/en/?ip=/	e.exe, 00000000.00000002.46140 5433.0000000002661000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.geodatatool.com/en/?ip=3D84.17.52.78=0D=0A=0D=0ADat=	e.exe, 00000000.00000002.46439 0201.00000000029E9000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org/HB	e.exe, 00000000.00000002.46140 5433.0000000002661000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app	e.exe, 00000000.00000002.46148 4579.0000000002694000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.geodatatool.com/en/?ip=84.17.52.78	e.exe, 00000000.00000002.46325 7447.0000000002840000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot/sendMessage?chat_id=&text=Createutf-8Win32_ComputerSystemModelManufactu	e.exe, 00000000.00000002.46140 5433.0000000002661000.00000004 .00000001.sdmp	false		high
http://https://www.geodatatool.com/en/?ip=	e.exe, 00000000.00000002.46159 7614.00000000026C5000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org	e.exe, 00000000.00000002.46140 5433.0000000002661000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	e.exe, 00000000.00000002.46140 5433.0000000002661000.00000004 .00000001.sdmp	false		high
http://kerekesfoto.com	e.exe, 00000000.00000002.46325 7447.0000000002840000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i.imgur.com/GJD7Q5y.png195.239.51.11795.26.248.2989.208.29.13389.187.165.4792.118.13.1895.26	e.exe, 00000000.00000002.46140 5433.0000000002661000.00000004 .00000001.sdmp	false		high
http://https://wackip.dyndns.org/	e.exe, 00000000.00000003.21118 4805.000000005EC0000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app/xml/84.17.52.78	e.exe, 00000000.00000002.46148 4579.0000000002694000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412757
Start date:	12.05.2021
Start time:	22:52:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	e.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:	23
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:	mal92.troj.spyw.evad.winEXE@1/0@39/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 40.88.32.150, 168.61.161.212, 20.82.210.154, 23.57.80.111, 92.122.213.194, 92.122.213.247, 20.54.26.129, 2.20.143.16, 2.20.142.209, 20.82.209.183 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.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 • 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
22:53:11	API Interceptor	948x Sleep call for process: e.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.88.193.70	FACTURA COMERCIAL_____ _____PDF__.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	d0875029_by_Libranalysis.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	ve #U00e7eki listesi ektedir Proforma.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Order-PO102.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	vy38Kw9qRh.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	DOCUMENTS AND CERTIFICATIONS.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Octamod 2021 -#U2026P014 New Order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	f2b03f7e_by_Libranalysis.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	purchase order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER E3007921.EXE	Get hash	malicious	Browse	• checkip.dyndns.org/
	order 39305.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	XPBPS2DL.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	INQUIRY.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	0908000000.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Nuovo ordine _WJO-001, pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PDF.09336642.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Updated Order list -804333.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SecuriteInfo.com.Trojan.Win32.Save.a.32673.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Qoute.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	FPI_0485010214.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
172.67.188.154	3MndTUzGQn.exe	Get hash	malicious	Browse	• freegeoip.app/json

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
checkip.dyndns.com	Purchase Order_12052021.exe	Get hash	malicious	Browse	• 216.146.43.71
	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
kerekesfoto.com	Purchase Order_12052021.exe	Get hash	malicious	Browse	• 193.32.232.10
	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
	Overdue_Invoice 25022021.exe	Get hash	malicious	Browse	• 193.32.232.10
	RFQ-22100026655Q.pdf.exe	Get hash	malicious	Browse	• 193.32.232.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
freegeoip.app	Purchase Order_12052021.exe	Get hash	malicious	Browse	• 104.21.19.200
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Purchase Order_12052021.exe	Get hash	malicious	Browse	• 104.21.19.200
	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
EZIT-ASHU	Purchase Order_12052021.exe	Get hash	malicious	Browse	• 193.32.232.10
	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 25022021.exe	Get hash	malicious	Browse	• 193.32.232.10
	RFQ-22100026655Q.pdf.exe	Get hash	malicious	Browse	• 193.32.232.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
DYNDNSUS	Purchase Order_12052021.exe	Get hash	malicious	Browse	• 216.146.43.71
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Purchase Order_12052021.exe	Get hash	malicious	Browse	• 172.67.188.154
	Invoice...exe	Get hash	malicious	Browse	• 172.67.188.154
	Statement of Account April-2021.exe	Get hash	malicious	Browse	• 172.67.188.154
	2070121SN-WS for Woosim i250MSR.pif.exe	Get hash	malicious	Browse	• 172.67.188.154
	FACTURA COMERCIAL_____ _____PDF__.exe	Get hash	malicious	Browse	• 172.67.188.154
	Quotation.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	• 172.67.188.154
	Account Ledger for 2020-APRIL 2021.exe	Get hash	malicious	Browse	• 172.67.188.154
	New purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO202104-543_ Inox Doan - Trading Co., Ltd,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	POI9090009.exe	Get hash	malicious	Browse	• 172.67.188.154
	SNAOUOKKOI.exe	Get hash	malicious	Browse	• 172.67.188.154
	ve #U00e7eki listesi ektedir Proforma.exe	Get hash	malicious	Browse	• 172.67.188.154
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order 12052021.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order 11052021.exe	Get hash	malicious	Browse	• 172.67.188.154
	1578D1E95037312FDBB8E0F46F086316E68BAD3B 9C8CD.exe	Get hash	malicious	Browse	• 172.67.188.154
	Due Invoices.exe	Get hash	malicious	Browse	• 172.67.188.154
	Order-PO102.exe	Get hash	malicious	Browse	• 172.67.188.154

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.433168283352283
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	e.exe
File size:	444928
MD5:	c69ddcf0dd4be5b729d10475408a468c
SHA1:	4a1113c488951852239fde30dc29d2ddcc1516bf
SHA256:	31b5237e182f6a218992e8e8ee0922665809e79f1a9050 3a39ad58da5163b04
SHA512:	5e2cea23fb92fc94732b30373a64e7b4a1a70b7b693a718 39b24897fefc7097610010ab473f2f01b114dd6d78aac42 1091c2dfba1f0c10cea520871eae77e712
SSDEEP:	3072:firqJhuNsKqZW5KgBRaq2aeKV0qW6+Kmaeq2aA 8MMscsMN+K5s8sMs8MMsY3deuG:f4SusKqZIKy3de9 IMwbMnY5EA9HEh
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...B7.`..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46defe
Entrypoint Section:	.text
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:	0x609A3742 [Tue May 11 07:50:26 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 [00402000h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6deac	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6e000	0x4b8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x70000	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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6bf04	0x6c000	False	0.19839364511	data	5.43588497553	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x4b8	0x600	False	0.369140625	data	3.67127324499	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x70000	0xc	0x200	False	0.103515625	data	0.638569002318	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x6e0a0	0x22c	data		
RT_MANIFEST	0x6e2cc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

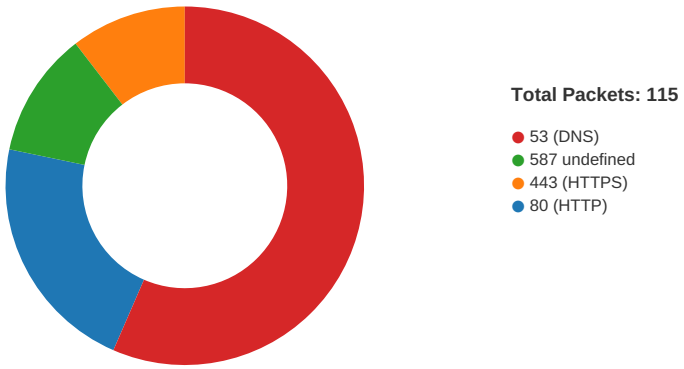
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	0.0.0.0
InternalName	e.exe
FileVersion	0.0.0.0
ProductVersion	0.0.0.0
FileDescription	
OriginalFilename	e.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:53:06.433012962 CEST	49716	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:06.566642046 CEST	80	49716	162.88.193.70	192.168.2.3
May 12, 2021 22:53:06.566862106 CEST	49716	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:06.567981958 CEST	49716	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:06.700998068 CEST	80	49716	162.88.193.70	192.168.2.3
May 12, 2021 22:53:06.701039076 CEST	80	49716	162.88.193.70	192.168.2.3
May 12, 2021 22:53:06.701076031 CEST	80	49716	162.88.193.70	192.168.2.3
May 12, 2021 22:53:06.701221943 CEST	49716	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:06.703161001 CEST	49716	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:06.789819002 CEST	49717	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:06.836289883 CEST	80	49716	162.88.193.70	192.168.2.3
May 12, 2021 22:53:06.927248001 CEST	80	49717	162.88.193.70	192.168.2.3
May 12, 2021 22:53:06.927437067 CEST	49717	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:06.927978992 CEST	49717	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:07.064970970 CEST	80	49717	162.88.193.70	192.168.2.3
May 12, 2021 22:53:07.065020084 CEST	80	49717	162.88.193.70	192.168.2.3
May 12, 2021 22:53:07.065047979 CEST	80	49717	162.88.193.70	192.168.2.3
May 12, 2021 22:53:07.065148115 CEST	49717	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:07.066042900 CEST	49717	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:07.203176022 CEST	80	49717	162.88.193.70	192.168.2.3
May 12, 2021 22:53:08.005975008 CEST	49719	443	192.168.2.3	172.67.188.154

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:53:08.046915054 CEST	443	49719	172.67.188.154	192.168.2.3
May 12, 2021 22:53:08.047050953 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:08.105524063 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:08.146339893 CEST	443	49719	172.67.188.154	192.168.2.3
May 12, 2021 22:53:08.149796009 CEST	443	49719	172.67.188.154	192.168.2.3
May 12, 2021 22:53:08.149836063 CEST	443	49719	172.67.188.154	192.168.2.3
May 12, 2021 22:53:08.149975061 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:08.159480095 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:08.200278044 CEST	443	49719	172.67.188.154	192.168.2.3
May 12, 2021 22:53:08.200527906 CEST	443	49719	172.67.188.154	192.168.2.3
May 12, 2021 22:53:08.249036074 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:08.263319969 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:08.305708885 CEST	443	49719	172.67.188.154	192.168.2.3
May 12, 2021 22:53:08.324898958 CEST	443	49719	172.67.188.154	192.168.2.3
May 12, 2021 22:53:08.373997927 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:08.426064014 CEST	49721	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:08.559999943 CEST	80	49721	162.88.193.70	192.168.2.3
May 12, 2021 22:53:08.560165882 CEST	49721	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:08.560508966 CEST	49721	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:08.693741083 CEST	80	49721	162.88.193.70	192.168.2.3
May 12, 2021 22:53:08.693784952 CEST	80	49721	162.88.193.70	192.168.2.3
May 12, 2021 22:53:08.693813086 CEST	80	49721	162.88.193.70	192.168.2.3
May 12, 2021 22:53:08.694004059 CEST	49721	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:08.695363045 CEST	49721	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:08.695960045 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:08.754417896 CEST	443	49719	172.67.188.154	192.168.2.3
May 12, 2021 22:53:08.795968056 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:08.828521967 CEST	80	49721	162.88.193.70	192.168.2.3
May 12, 2021 22:53:08.840140104 CEST	49722	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:08.974977016 CEST	80	49722	162.88.193.70	192.168.2.3
May 12, 2021 22:53:08.975127935 CEST	49722	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:08.975441933 CEST	49722	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:09.108647108 CEST	80	49722	162.88.193.70	192.168.2.3
May 12, 2021 22:53:09.108848095 CEST	80	49722	162.88.193.70	192.168.2.3
May 12, 2021 22:53:09.108880043 CEST	80	49722	162.88.193.70	192.168.2.3
May 12, 2021 22:53:09.109003067 CEST	49722	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:09.109397888 CEST	49722	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:09.109927893 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:09.164417982 CEST	443	49719	172.67.188.154	192.168.2.3
May 12, 2021 22:53:09.217828035 CEST	49719	443	192.168.2.3	172.67.188.154
May 12, 2021 22:53:09.219115973 CEST	49723	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:09.244611979 CEST	80	49722	162.88.193.70	192.168.2.3
May 12, 2021 22:53:09.353821039 CEST	80	49723	162.88.193.70	192.168.2.3
May 12, 2021 22:53:09.353909016 CEST	49723	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:09.354274035 CEST	49723	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:09.488946915 CEST	80	49723	162.88.193.70	192.168.2.3
May 12, 2021 22:53:09.488991022 CEST	80	49723	162.88.193.70	192.168.2.3
May 12, 2021 22:53:09.489017963 CEST	80	49723	162.88.193.70	192.168.2.3
May 12, 2021 22:53:09.489088058 CEST	49723	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:09.489476919 CEST	49723	80	192.168.2.3	162.88.193.70
May 12, 2021 22:53:09.624455929 CEST	80	49723	162.88.193.70	192.168.2.3
May 12, 2021 22:53:13.547951937 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:13.599044085 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:13.599179029 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:13.737692118 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:13.738184929 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:13.789324999 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:13.789886951 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:13.843952894 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:13.845506907 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:13.903120041 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:13.903182030 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:13.903219938 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:13.903389931 CEST	49729	587	192.168.2.3	193.32.232.10

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:53:13.916291952 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:13.967744112 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:13.983450890 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:14.036180019 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:14.039338112 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:14.090492010 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:14.091216087 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:14.151160955 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:14.152205944 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:14.204848051 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:14.206502914 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:14.297343016 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:14.362987041 CEST	587	49729	193.32.232.10	192.168.2.3
May 12, 2021 22:53:14.364521980 CEST	49729	587	192.168.2.3	193.32.232.10
May 12, 2021 22:53:14.415705919 CEST	587	49729	193.32.232.10	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:52:57.793086052 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 22:52:57.844779015 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 22:52:58.560045958 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 22:52:58.611998081 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 22:52:59.360487938 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 22:52:59.409188986 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 22:53:01.976490021 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:02.027128935 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 22:53:02.905586958 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:02.957254887 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 22:53:03.698676109 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:03.747711897 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 22:53:04.472368002 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:04.524100065 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 22:53:05.360712051 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:05.410540104 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 22:53:06.173043013 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:06.224760056 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 22:53:06.272114992 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:06.323497057 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 22:53:06.358006001 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:06.407160044 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 22:53:07.144892931 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:07.194111109 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 22:53:07.936170101 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:08.000313997 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 22:53:08.198333979 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:08.247191906 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 22:53:09.168943882 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:09.217719078 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 22:53:09.956726074 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:10.008492947 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 22:53:10.736010075 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:10.784725904 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 22:53:11.590265036 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:11.639256001 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 22:53:12.482506990 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:12.535531044 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 22:53:13.472529888 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:13.545953989 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 22:53:13.711410999 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:13.760402918 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 22:53:16.918060064 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:16.967279911 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 22:53:20.746395111 CEST	50713	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:53:20.803611040 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 22:53:23.918917894 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:23.967864037 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 22:53:27.135799885 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:27.195782900 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 22:53:30.285991907 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:30.336695910 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 22:53:31.081110001 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:31.140666008 CEST	53	60633	8.8.8.8	192.168.2.3
May 12, 2021 22:53:33.321083069 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:33.379771948 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 22:53:36.514879942 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:36.573599100 CEST	53	63619	8.8.8.8	192.168.2.3
May 12, 2021 22:53:37.803930044 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:37.863024950 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 22:53:39.842698097 CEST	61946	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:39.900038958 CEST	53	61946	8.8.8.8	192.168.2.3
May 12, 2021 22:53:42.843741894 CEST	64910	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:42.892656088 CEST	53	64910	8.8.8.8	192.168.2.3
May 12, 2021 22:53:43.089591026 CEST	52123	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:43.151324034 CEST	53	52123	8.8.8.8	192.168.2.3
May 12, 2021 22:53:45.816039085 CEST	56130	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:45.877115011 CEST	53	56130	8.8.8.8	192.168.2.3
May 12, 2021 22:53:48.975218058 CEST	56338	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:49.023957014 CEST	53	56338	8.8.8.8	192.168.2.3
May 12, 2021 22:53:50.838752031 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:50.911281109 CEST	53	59420	8.8.8.8	192.168.2.3
May 12, 2021 22:53:52.118401051 CEST	58784	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:52.175760031 CEST	53	58784	8.8.8.8	192.168.2.3
May 12, 2021 22:53:52.577627897 CEST	63978	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:52.639373064 CEST	53	63978	8.8.8.8	192.168.2.3
May 12, 2021 22:53:56.667988062 CEST	62938	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:56.725141048 CEST	53	62938	8.8.8.8	192.168.2.3
May 12, 2021 22:53:59.793711901 CEST	55708	53	192.168.2.3	8.8.8.8
May 12, 2021 22:53:59.843156099 CEST	53	55708	8.8.8.8	192.168.2.3
May 12, 2021 22:54:02.825144053 CEST	56803	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:02.875749111 CEST	53	56803	8.8.8.8	192.168.2.3
May 12, 2021 22:54:05.813122034 CEST	57145	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:05.861727953 CEST	53	57145	8.8.8.8	192.168.2.3
May 12, 2021 22:54:07.570676088 CEST	55359	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:07.638468027 CEST	53	55359	8.8.8.8	192.168.2.3
May 12, 2021 22:54:08.936150074 CEST	58306	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:08.987855911 CEST	53	58306	8.8.8.8	192.168.2.3
May 12, 2021 22:54:12.246995926 CEST	64124	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:12.296303034 CEST	53	64124	8.8.8.8	192.168.2.3
May 12, 2021 22:54:12.686264992 CEST	49361	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:12.744940996 CEST	53	49361	8.8.8.8	192.168.2.3
May 12, 2021 22:54:15.347206116 CEST	63150	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:15.409090996 CEST	53	63150	8.8.8.8	192.168.2.3
May 12, 2021 22:54:18.357088089 CEST	53279	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:18.406560898 CEST	53	53279	8.8.8.8	192.168.2.3
May 12, 2021 22:54:21.509905100 CEST	56881	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:21.563572884 CEST	53	56881	8.8.8.8	192.168.2.3
May 12, 2021 22:54:24.480812073 CEST	53642	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:24.533174038 CEST	53	53642	8.8.8.8	192.168.2.3
May 12, 2021 22:54:27.778995037 CEST	55667	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:27.827694893 CEST	53	55667	8.8.8.8	192.168.2.3
May 12, 2021 22:54:30.854228020 CEST	54833	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:30.905781031 CEST	53	54833	8.8.8.8	192.168.2.3
May 12, 2021 22:54:34.005455971 CEST	62476	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:34.057084084 CEST	53	62476	8.8.8.8	192.168.2.3
May 12, 2021 22:54:37.190257072 CEST	49705	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:37.248511076 CEST	53	49705	8.8.8.8	192.168.2.3
May 12, 2021 22:54:40.273678064 CEST	61477	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:54:40.322417021 CEST	53	61477	8.8.8.8	192.168.2.3
May 12, 2021 22:54:42.986082077 CEST	61633	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:43.053510904 CEST	53	61633	8.8.8.8	192.168.2.3
May 12, 2021 22:54:43.792738914 CEST	55949	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:43.842997074 CEST	53	55949	8.8.8.8	192.168.2.3
May 12, 2021 22:54:44.420928955 CEST	57601	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:44.486454010 CEST	53	57601	8.8.8.8	192.168.2.3
May 12, 2021 22:54:46.883919001 CEST	49342	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:46.935659885 CEST	53	49342	8.8.8.8	192.168.2.3
May 12, 2021 22:54:49.993673086 CEST	56253	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:50.042603016 CEST	53	56253	8.8.8.8	192.168.2.3
May 12, 2021 22:54:52.997462988 CEST	49667	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:53.046355009 CEST	53	49667	8.8.8.8	192.168.2.3
May 12, 2021 22:54:55.995349884 CEST	55439	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:56.044291019 CEST	53	55439	8.8.8.8	192.168.2.3
May 12, 2021 22:54:59.244407892 CEST	57069	53	192.168.2.3	8.8.8.8
May 12, 2021 22:54:59.303075075 CEST	53	57069	8.8.8.8	192.168.2.3
May 12, 2021 22:55:02.397352934 CEST	57659	53	192.168.2.3	8.8.8.8
May 12, 2021 22:55:02.454824924 CEST	53	57659	8.8.8.8	192.168.2.3
May 12, 2021 22:55:05.517371893 CEST	54717	53	192.168.2.3	8.8.8.8
May 12, 2021 22:55:05.567748070 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 22:53:06.272114992 CEST	192.168.2.3	8.8.8.8	0x809d	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
May 12, 2021 22:53:06.358006001 CEST	192.168.2.3	8.8.8.8	0x76a	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
May 12, 2021 22:53:07.936170101 CEST	192.168.2.3	8.8.8.8	0x2347	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)
May 12, 2021 22:53:13.472529888 CEST	192.168.2.3	8.8.8.8	0xc426	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:16.918060064 CEST	192.168.2.3	8.8.8.8	0x5f79	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:20.746395111 CEST	192.168.2.3	8.8.8.8	0x8a35	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:23.918917894 CEST	192.168.2.3	8.8.8.8	0x7495	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:27.135799885 CEST	192.168.2.3	8.8.8.8	0x579f	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:30.285991907 CEST	192.168.2.3	8.8.8.8	0xb9ff	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:33.321083069 CEST	192.168.2.3	8.8.8.8	0x8547	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:36.514879942 CEST	192.168.2.3	8.8.8.8	0x93d	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:39.842698097 CEST	192.168.2.3	8.8.8.8	0x5a2a	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:42.843741894 CEST	192.168.2.3	8.8.8.8	0x11ad	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:45.816039085 CEST	192.168.2.3	8.8.8.8	0x85e6	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:48.975218058 CEST	192.168.2.3	8.8.8.8	0xaea4	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:52.118401051 CEST	192.168.2.3	8.8.8.8	0x976e	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:56.667988062 CEST	192.168.2.3	8.8.8.8	0xf982	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:53:59.793711901 CEST	192.168.2.3	8.8.8.8	0x7258	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:02.825144053 CEST	192.168.2.3	8.8.8.8	0xabc0	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:05.813122034 CEST	192.168.2.3	8.8.8.8	0x1887	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:08.936150074 CEST	192.168.2.3	8.8.8.8	0x2999	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:12.246995926 CEST	192.168.2.3	8.8.8.8	0xba39	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:15.347206116 CEST	192.168.2.3	8.8.8.8	0x16dd	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 22:54:18.357088089 CEST	192.168.2.3	8.8.8.8	0x2d3b	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:21.509905100 CEST	192.168.2.3	8.8.8.8	0xa3e2	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:24.480812073 CEST	192.168.2.3	8.8.8.8	0xad31	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:27.778995037 CEST	192.168.2.3	8.8.8.8	0x4889	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:30.854228020 CEST	192.168.2.3	8.8.8.8	0x1b9c	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:34.005455971 CEST	192.168.2.3	8.8.8.8	0xa930	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:37.190257072 CEST	192.168.2.3	8.8.8.8	0xcd06	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:40.273678064 CEST	192.168.2.3	8.8.8.8	0xb9d1	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:43.792738914 CEST	192.168.2.3	8.8.8.8	0xc23d	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:46.883919001 CEST	192.168.2.3	8.8.8.8	0x88a1	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:49.993673086 CEST	192.168.2.3	8.8.8.8	0x4cb	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:52.997462988 CEST	192.168.2.3	8.8.8.8	0xe806	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:55.995349884 CEST	192.168.2.3	8.8.8.8	0xa77f	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:54:59.244407892 CEST	192.168.2.3	8.8.8.8	0x5751	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:55:02.397352934 CEST	192.168.2.3	8.8.8.8	0xffb2	Standard query (0)	kerekesfoto.com	A (IP address)	IN (0x0001)
May 12, 2021 22:55:05.517371893 CEST	192.168.2.3	8.8.8.8	0xdeaa	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 22:53:06.323497057 CEST	8.8.8.8	192.168.2.3	0x809d	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 22:53:06.323497057 CEST	8.8.8.8	192.168.2.3	0x809d	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
May 12, 2021 22:53:06.323497057 CEST	8.8.8.8	192.168.2.3	0x809d	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
May 12, 2021 22:53:06.323497057 CEST	8.8.8.8	192.168.2.3	0x809d	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
May 12, 2021 22:53:06.323497057 CEST	8.8.8.8	192.168.2.3	0x809d	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
May 12, 2021 22:53:06.323497057 CEST	8.8.8.8	192.168.2.3	0x809d	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
May 12, 2021 22:53:06.407160044 CEST	8.8.8.8	192.168.2.3	0x76a	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 22:53:06.407160044 CEST	8.8.8.8	192.168.2.3	0x76a	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
May 12, 2021 22:53:06.407160044 CEST	8.8.8.8	192.168.2.3	0x76a	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
May 12, 2021 22:53:06.407160044 CEST	8.8.8.8	192.168.2.3	0x76a	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
May 12, 2021 22:53:06.407160044 CEST	8.8.8.8	192.168.2.3	0x76a	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
May 12, 2021 22:53:06.407160044 CEST	8.8.8.8	192.168.2.3	0x76a	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
May 12, 2021 22:53:08.000313997 CEST	8.8.8.8	192.168.2.3	0x2347	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 22:53:08.000313997 CEST	8.8.8.8	192.168.2.3	0x2347	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
May 12, 2021 22:53:13.545953989 CEST	8.8.8.8	192.168.2.3	0xc426	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:16.967279911 CEST	8.8.8.8	192.168.2.3	0x5f79	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:20.803611040 CEST	8.8.8.8	192.168.2.3	0x8a35	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:23.967864037 CEST	8.8.8.8	192.168.2.3	0x7495	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:27.195782900 CEST	8.8.8.8	192.168.2.3	0x579f	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:30.336695910 CEST	8.8.8.8	192.168.2.3	0xb9ff	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:33.379771948 CEST	8.8.8.8	192.168.2.3	0x8547	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:36.573599100 CEST	8.8.8.8	192.168.2.3	0x93d	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:39.900038958 CEST	8.8.8.8	192.168.2.3	0x5a2a	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:42.892656088 CEST	8.8.8.8	192.168.2.3	0x11ad	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:45.877115011 CEST	8.8.8.8	192.168.2.3	0x85e6	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:49.023957014 CEST	8.8.8.8	192.168.2.3	0xaea4	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:52.175760031 CEST	8.8.8.8	192.168.2.3	0x976e	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:56.725141048 CEST	8.8.8.8	192.168.2.3	0xf982	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:53:59.843156099 CEST	8.8.8.8	192.168.2.3	0x7258	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:02.875749111 CEST	8.8.8.8	192.168.2.3	0xabc0	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:05.861727953 CEST	8.8.8.8	192.168.2.3	0x1887	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:08.987855911 CEST	8.8.8.8	192.168.2.3	0x2999	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:12.296303034 CEST	8.8.8.8	192.168.2.3	0xba39	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:15.409090996 CEST	8.8.8.8	192.168.2.3	0x16dd	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:18.406560898 CEST	8.8.8.8	192.168.2.3	0x2d3b	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:21.563572884 CEST	8.8.8.8	192.168.2.3	0xa3e2	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:24.533174038 CEST	8.8.8.8	192.168.2.3	0xad31	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:27.827694893 CEST	8.8.8.8	192.168.2.3	0x4889	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:30.905781031 CEST	8.8.8.8	192.168.2.3	0x1b9c	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 22:54:34.057084084 CEST	8.8.8.8	192.168.2.3	0xa930	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:37.248511076 CEST	8.8.8.8	192.168.2.3	0xcd06	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:40.322417021 CEST	8.8.8.8	192.168.2.3	0xb9d1	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:43.842997074 CEST	8.8.8.8	192.168.2.3	0xc23d	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:46.935659885 CEST	8.8.8.8	192.168.2.3	0x88a1	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:50.042603016 CEST	8.8.8.8	192.168.2.3	0x4cb	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:53.046355009 CEST	8.8.8.8	192.168.2.3	0xe806	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:56.044291019 CEST	8.8.8.8	192.168.2.3	0xa77f	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:54:59.303075075 CEST	8.8.8.8	192.168.2.3	0x5751	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:55:02.454824924 CEST	8.8.8.8	192.168.2.3	0xffb2	No error (0)	kerekesfoto.com		193.32.232.10	A (IP address)	IN (0x0001)
May 12, 2021 22:55:05.567748070 CEST	8.8.8.8	192.168.2.3	0xdeaa	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	49716	162.88.193.70	80	C:\Users\user\Desktop\e.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:53:06.567981958 CEST	1141	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 22:53:06.701039076 CEST	1144	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	49717	162.88.193.70	80	C:\Users\user\Desktop\e.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:53:06.927978992 CEST	1148	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

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:53:07.065020084 CEST	1149	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	49721	162.88.193.70	80	C:\Users\user\Desktop\e.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:53:08.560508966 CEST	1173	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 22:53:08.693784952 CEST	1174	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	49722	162.88.193.70	80	C:\Users\user\Desktop\e.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:53:08.975441933 CEST	1182	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 22:53:09.108848095 CEST	1184	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	49723	162.88.193.70	80	C:\Users\user\Desktop\e.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 22:53:09.354274035 CEST	1186	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 22:53:09.488991022 CEST	1191	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 22:53:08.149836063 CEST	172.67.188.154	443	192.168.2.3	49719	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 22:53:13.737692118 CEST	587	49729	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:53:13 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:13.738184929 CEST	49729	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:13.789324999 CEST	587	49729	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:13.789886951 CEST	49729	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:13.843952894 CEST	587	49729	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:17.151762962 CEST	587	49731	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:53:17 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:17.152122974 CEST	49731	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:17.203258038 CEST	587	49731	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:17.203701973 CEST	49731	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:17.257808924 CEST	587	49731	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:20.964314938 CEST	587	49732	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:53:20 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:20.964553118 CEST	49732	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:21.016235113 CEST	587	49732	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:21.016514063 CEST	49732	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:21.071008921 CEST	587	49732	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:24.162065029 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 22:53:24 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:24.162288904 CEST	49733	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:24.214493036 CEST	587	49733	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 22:53:24.218379974 CEST	49733	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:24.272486925 CEST	587	49733	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:27.344834089 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 22:53:27 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:27.345105886 CEST	49734	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:27.398219109 CEST	587	49734	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:27.398585081 CEST	49734	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:27.452563047 CEST	587	49734	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:30.488079071 CEST	587	49735	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:53:30 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:30.488555908 CEST	49735	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:30.539558887 CEST	587	49735	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:30.539793968 CEST	49735	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:30.593888044 CEST	587	49735	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:33.516235113 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 22:53:33 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:33.516571045 CEST	49738	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:33.567698956 CEST	587	49738	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:33.569546938 CEST	49738	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:33.622659922 CEST	587	49738	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:36.699047089 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 22:53:36 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:36.699295044 CEST	49741	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:36.750631094 CEST	587	49741	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:36.753571987 CEST	49741	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:36.809415102 CEST	587	49741	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:40.048444033 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 22:53:40 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:40.049027920 CEST	49743	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:40.100214005 CEST	587	49743	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:40.100477934 CEST	49743	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:40.153366089 CEST	587	49743	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 22:53:43.029694080 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 22:53:43 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:43.029922962 CEST	49744	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:43.081005096 CEST	587	49744	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:43.081242085 CEST	49744	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:43.133456945 CEST	587	49744	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:46.013276100 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 22:53:46 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:46.013580084 CEST	49746	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:46.066364050 CEST	587	49746	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:46.066626072 CEST	49746	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:46.120806932 CEST	587	49746	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:49.178059101 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 22:53:49 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:49.178313971 CEST	49747	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:49.229263067 CEST	587	49747	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:49.230911970 CEST	49747	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:49.284928083 CEST	587	49747	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:52.297692060 CEST	587	49749	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:53:52 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:52.527509928 CEST	49749	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:52.554361105 CEST	587	49749	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:53:52 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:52.580358982 CEST	587	49749	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:52.580661058 CEST	49749	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:53:52.636683941 CEST	587	49749	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:56.859334946 CEST	587	49751	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:53:56 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:56.859708071 CEST	49751	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:53:56.910834074 CEST	587	49751	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:53:56.911058903 CEST	49751	587	192.168.2.3	193.32.232.10	STARTTLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 22:53:56.965042114 CEST	587	49751	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:53:59.995628119 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 22:53:59 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:53:59.995886087 CEST	49752	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:00.046915054 CEST	587	49752	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:00.047239065 CEST	49752	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:00.101155996 CEST	587	49752	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:03.009027958 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 22:54:02 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:03.009350061 CEST	49753	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:03.060328960 CEST	587	49753	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:03.060626984 CEST	49753	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:03.114947081 CEST	587	49753	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:06.011895895 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 22:54:05 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:06.012170076 CEST	49754	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:06.063009977 CEST	587	49754	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:06.063271046 CEST	49754	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:06.116489887 CEST	587	49754	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:09.137520075 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 22:54:09 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:09.140613079 CEST	49758	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:09.191857100 CEST	587	49758	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:09.192121029 CEST	49758	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:09.246020079 CEST	587	49758	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:12.417273045 CEST	587	49759	193.32.232.10	192.168.2.3	220-s16.tarhely.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 22:54:12 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:12.417553902 CEST	49759	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:12.468481064 CEST	587	49759	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:12.468859911 CEST	49759	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:12.521049976 CEST	587	49759	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 22:54:15.546890974 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 22:54:15 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:15.547153950 CEST	49765	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:15.599287987 CEST	587	49765	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:15.599601030 CEST	49765	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:15.652318954 CEST	587	49765	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:18.566883087 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 22:54:18 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:18.569432974 CEST	49766	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:18.620553017 CEST	587	49766	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:18.621587992 CEST	49766	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:18.675333977 CEST	587	49766	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:21.698724031 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 22:54:21 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:21.698986053 CEST	49767	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:21.751804113 CEST	587	49767	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:21.752155066 CEST	49767	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:21.804410934 CEST	587	49767	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:24.700077057 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 22:54:24 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:24.700839996 CEST	49768	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:24.751827955 CEST	587	49768	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:24.752116919 CEST	49768	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:24.805804014 CEST	587	49768	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:27.963216066 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 22:54:27 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:27.963530064 CEST	49769	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:28.014477968 CEST	587	49769	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:28.014883041 CEST	49769	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:28.067079067 CEST	587	49769	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 22:54:31.027833939 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 22:54:31 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:31.028074980 CEST	49770	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:31.079250097 CEST	587	49770	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:31.079780102 CEST	49770	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:31.133804083 CEST	587	49770	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:34.180912018 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 22:54:34 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:34.181194067 CEST	49771	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:34.232280016 CEST	587	49771	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:34.232598066 CEST	49771	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:34.285563946 CEST	587	49771	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:37.384490013 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 22:54:37 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:37.384932995 CEST	49772	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:37.437901020 CEST	587	49772	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:37.438218117 CEST	49772	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:37.490459919 CEST	587	49772	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:40.447444916 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 22:54:40 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:40.447834015 CEST	49773	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:40.498879910 CEST	587	49773	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:40.499280930 CEST	49773	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:40.551425934 CEST	587	49773	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:43.990959883 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 22:54:43 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:43.991285086 CEST	49775	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:44.043951988 CEST	587	49775	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:44.044161081 CEST	49775	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:44.098206043 CEST	587	49775	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 22:54:47.104635954 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 22:54:47 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:47.105268002 CEST	49777	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:47.156411886 CEST	587	49777	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:47.156814098 CEST	49777	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:47.210796118 CEST	587	49777	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:50.165085077 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 22:54:50 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:50.165360928 CEST	49778	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:50.216360092 CEST	587	49778	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:50.216617107 CEST	49778	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:50.269978046 CEST	587	49778	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:53.207391977 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 22:54:53 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:53.207670927 CEST	49779	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:53.258485079 CEST	587	49779	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:53.258812904 CEST	49779	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:53.312436104 CEST	587	49779	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:56.165515900 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 22:54:56 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:56.165813923 CEST	49780	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:56.217128038 CEST	587	49780	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:56.217467070 CEST	49780	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:56.270625114 CEST	587	49780	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:54:59.411505938 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 22:54:59 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:54:59.411715984 CEST	49781	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:54:59.462841988 CEST	587	49781	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:54:59.463139057 CEST	49781	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:54:59.518477917 CEST	587	49781	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 22:55:02.573951006 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 22:55:02 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:55:02.574194908 CEST	49782	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:55:02.625145912 CEST	587	49782	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:55:02.625390053 CEST	49782	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:55:02.678066969 CEST	587	49782	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:55:05.704494953 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 22:55:05 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:55:05.704905987 CEST	49783	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:55:05.756325960 CEST	587	49783	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:55:05.756800890 CEST	49783	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:55:05.809911966 CEST	587	49783	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:55:08.808249950 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 22:55:08 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:55:08.808969021 CEST	49784	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:55:08.860240936 CEST	587	49784	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:55:08.860450029 CEST	49784	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:55:08.912601948 CEST	587	49784	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:55:11.767436028 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 22:55:11 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:55:11.767617941 CEST	49785	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:55:11.820185900 CEST	587	49785	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:55:11.820406914 CEST	49785	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:55:11.872878075 CEST	587	49785	193.32.232.10	192.168.2.3	220 TLS go ahead
May 12, 2021 22:55:15.650163889 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 22:55:15 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 22:55:15.650736094 CEST	49786	587	192.168.2.3	193.32.232.10	EHLO 238576
May 12, 2021 22:55:15.701859951 CEST	587	49786	193.32.232.10	192.168.2.3	250-s16.tarhely.com Hello 238576 [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 22:55:15.703850031 CEST	49786	587	192.168.2.3	193.32.232.10	STARTTLS
May 12, 2021 22:55:15.756432056 CEST	587	49786	193.32.232.10	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

System Behavior

Analysis Process: e.exe PID: 6132 Parent PID: 5688

General

Start time:	22:53:02
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\e.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\e.exe'
Imagebase:	0x300000
File size:	444928 bytes
MD5 hash:	C69DDCF0DD4BE5B729D10475408A468C
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: 00000000.00000002.461405433.0000000002661000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000000.00000000.191074513.0000000000302000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000000.191074513.0000000000302000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000000.191074513.0000000000302000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000000.00000002.458925410.0000000000302000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.458925410.0000000000302000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.458925410.0000000000302000.00000002.00020000.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	6DF3CF06	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	6DF3CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	success or wait	1	6CD86A95	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	success or wait	1	6CD86A95	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	success or wait	1	6CD86A95	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	6DF15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD81B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis