ID: 345001
Sample Name: ttrpym.exe
Cookbook: default.jbs
Time: 15:38:48
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

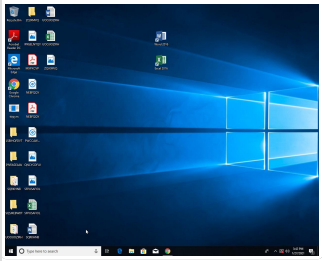
Analysis Report ttrpym.exe

Overview

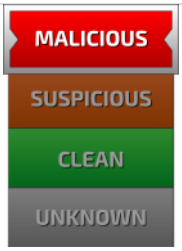
General Information

Sample Name:	ttrpym.exe
Analysis ID:	345001
MD5:	3b53c639bd8ea8..
SHA1:	af2f707e2e78787..
SHA256:	eca6a35d952f845.
Tags:	exe

Most interesting Screenshot:



Detection



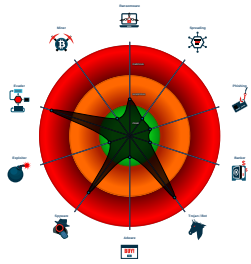
AgentTesla Telegram RAT

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected Telegram RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- .NET source code references suspic…
- Found evasive API chain (trying to d…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…

Classification



Startup

- **System is w10x64**
- ttrpym.exe (PID: 6400 cmdline: 'C:\Users\user\Desktop\ttrpym.exe' MD5: 3B53C639BD8EA883E5036A040F833415)
  - ttrpym.exe (PID: 6732 cmdline: {path} MD5: 3B53C639BD8EA883E5036A040F833415)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.619489004.000000000339 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.619489004.000000000339 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000003.00000002.614226904.0000000000F8 2000.00000020.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: ttrpym.exe PID: 6732	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: ttrpym.exe PID: 6732	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	

Click to see the 1 entries

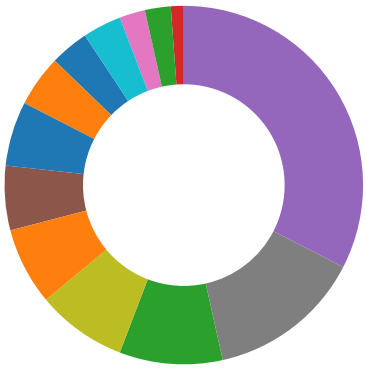
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.ttrpym.exe.f80000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

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:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

Uses the Telegram API (likely for C&C communication)

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected Telegram RAT

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

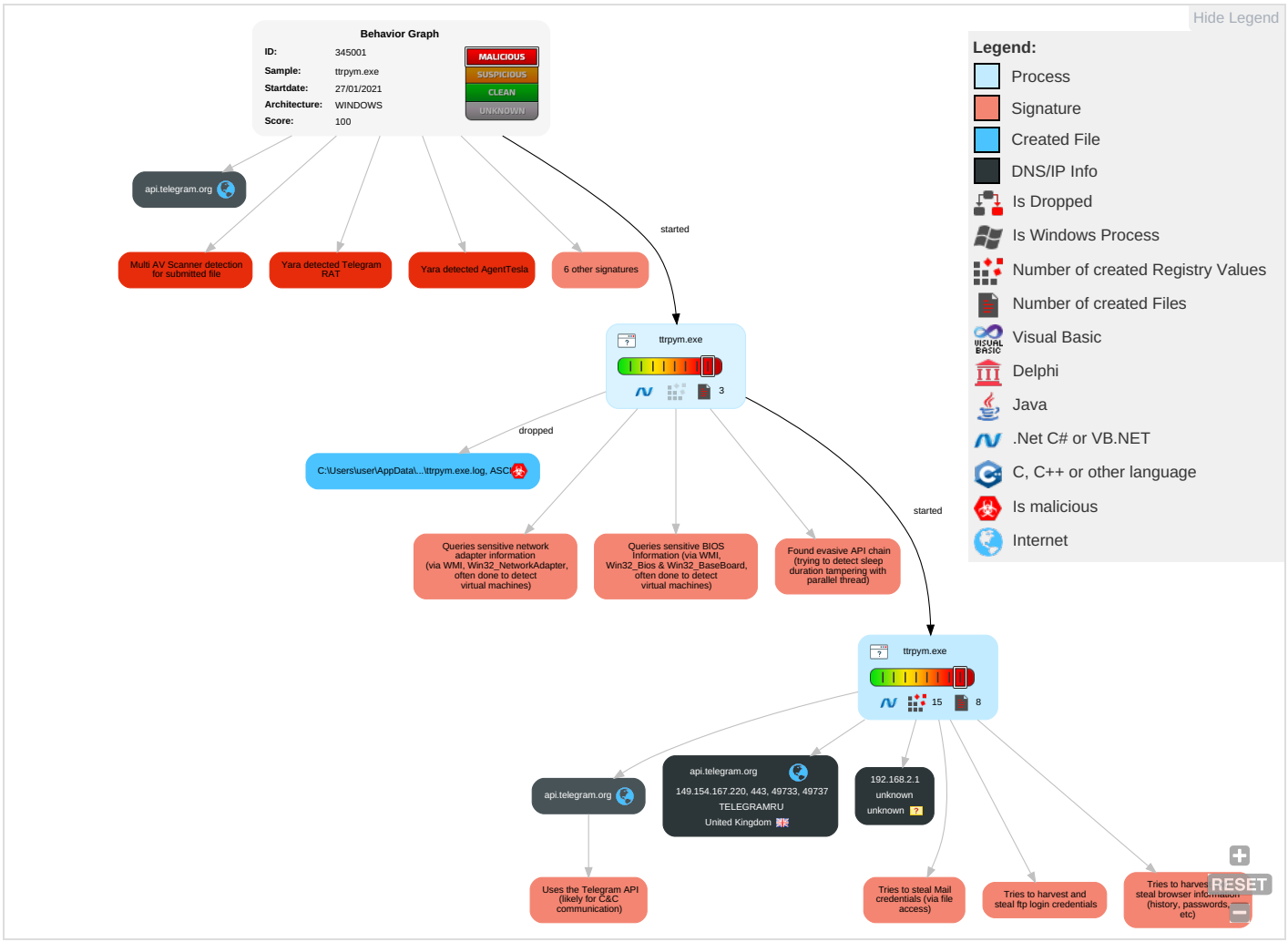
Yara detected AgentTesla

Yara detected Telegram RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	W Se
Default Accounts	Native API 2 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	In Tr
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 2	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 2 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Er Cl
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	No Ap La Pr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 2 4 1	SSH	Keylogging	Data Transfer Size Limits	Ap La Pr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr

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
ttrpym.exe	50%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
ttrpym.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.ttrpym.exe.f80000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comes	0%	Avira URL Cloud	safe	
http://www.fontbureau.comttvaZ	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnr-c	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.carterandcone.comma	0%	Avira URL Cloud	safe	
http://www.carterandcone.comamFA	0%	Avira URL Cloud	safe	
http://www.urwpp.deoi	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cnomp	0%	Avira URL Cloud	safe	
http://www.urwpp.dewa	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/m	0%	Avira URL Cloud	safe	
http://https://api.telegram.orgx&.q	0%	Avira URL Cloud	safe	
http://ocsp.godaddy.c	0%	Avira URL Cloud	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmJU	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krl	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnj	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.tiro.comrporation	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnad	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnamFA	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgritaC	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.htmlXUJl	0%	Avira URL Cloud	safe	
http://www.carterandcone.comkYF=	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cnma	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.comroa	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sandoll.co.krs-c	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnm	0%	Avira URL Cloud	safe	
http://www.sandoll.c	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.telegram.orgx&.qloN	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comad	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comes	ttrpym.exe, 00000000.00000003.239292340.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html.	ttrpym.exe, 00000000.00000003.245072326.0000000005E7B000.00000004.00000001.sdmp	false		high
http://crl.godaddy.com/gdig2s1-1823.crl0	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false		high

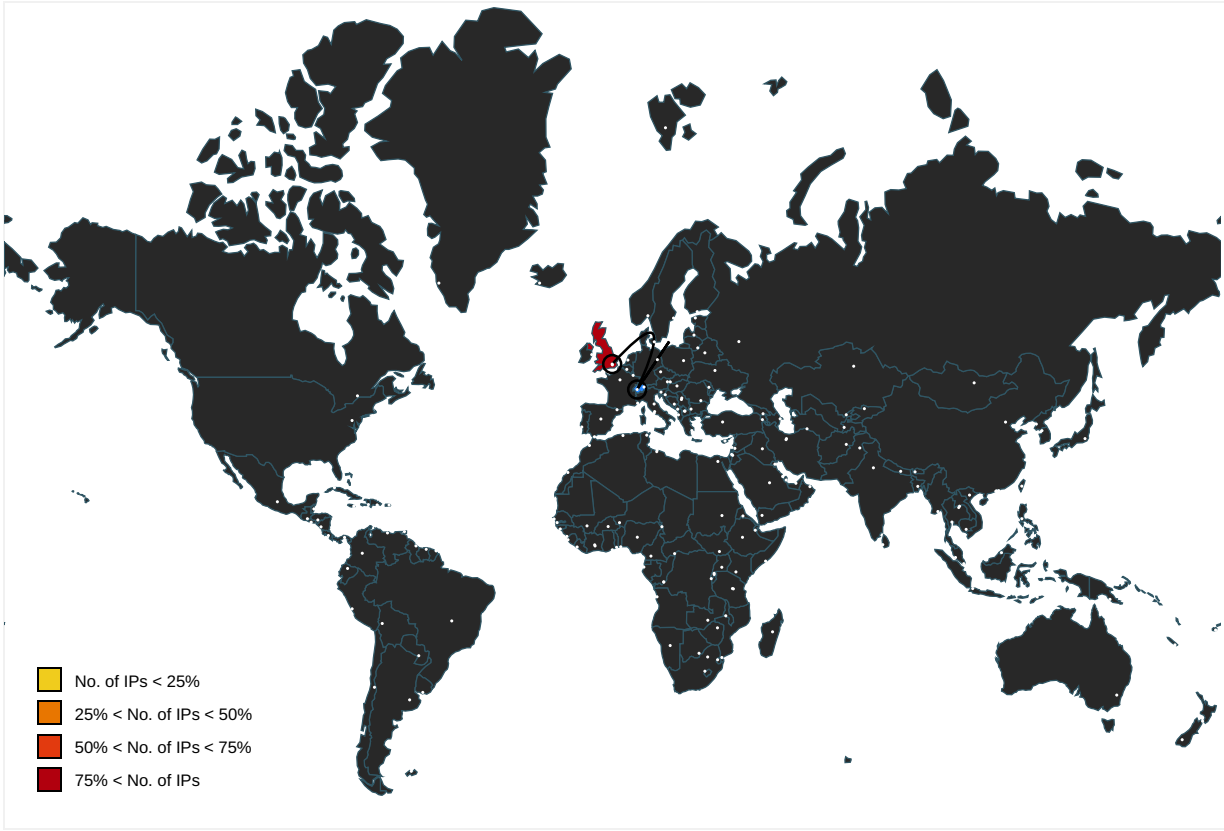
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designerskYlH	ttrpym.exe, 00000000.00000003.244441566.0000000005E7D000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comttvaZ	ttrpym.exe, 00000000.00000002.264530973.00000000016D7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnr-c	ttrpym.exe, 00000000.00000003.238783173.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	ttrpym.exe, 00000000.00000003.233656365.0000000005E62000.00000004.00000001.sdmp, ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comma	ttrpym.exe, 00000000.00000003.239779476.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers)Y	ttrpym.exe, 00000000.00000003.245883722.0000000005E7B000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comamFA	ttrpym.exe, 00000000.00000003.238931261.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deoi	ttrpym.exe, 00000000.00000003.243771789.0000000005E7D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlP	ttrpym.exe, 00000000.00000003.245112917.0000000005E9E000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot1534863067:AAHgkXiWvRLedLdzn8NhreUVQl7GIuV0U6g/	ttrpym.exe, 00000003.00000002.614226904.0000000000F82000.00000020.00000001.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	ttrpym.exe, 00000000.00000003.242053272.0000000005E83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?Y0	ttrpym.exe, 00000000.00000003.244251584.0000000005E7D000.00000004.00000001.sdmp	false		high
http://www.urwpp.deDPlease	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnomp	ttrpym.exe, 00000000.00000003.238437682.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.dewa	ttrpym.exe, 00000000.00000003.243571729.0000000005E7D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	ttrpym.exe, 00000000.00000003.238783173.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.godaddy.com/repository/gdig2.crt0	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	ttrpym.exe, 00000003.00000002.614226904.0000000000F82000.00000020.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/m	ttrpym.exe, 00000000.00000003.238160822.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.orgx&.q	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp, ttrpym.exe, 00000003.00000002.619638629.000000000343E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ocsp.godaddy.c	ttrpym.exe, 00000003.00000003.469945835.0000000007DCC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comd	ttrpym.exe, 00000000.00000003.239366599.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmJU	ttrpym.exe, 00000000.00000003.247669599.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.godaddy.com/repository/1301	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.krl	ttrpym.exe, 00000000.00000003.237159926.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://certs.godaddy.com/repository/0	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false		high
http://https://certs.godaddy.com/repositor	ttrpym.exe, 00000003.00000003.469945835.0000000007DCC000.00000004.00000001.sdmp	false		high
http://en.w	ttrpym.exe, 00000000.00000003.235365275.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cnj	ttrpym.exe, 00000000.00000003.238783173.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	ttrpym.exe, 00000000.00000003.238052266.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.godaddy.com/gdroot-g2.crl0F	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/frere-jones.html	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false		high
http://www.tiro.comrporation	ttrpym.exe, 00000000.00000003.238437682.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnad	ttrpym.exe, 00000000.00000003.239436981.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnamFA	ttrpym.exe, 00000000.00000003.238783173.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comgritaC	ttrpym.exe, 00000000.00000002.264530973.00000000016D7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.htmlXUJl	ttrpym.exe, 00000000.00000003.241273039.0000000005E83000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comkYF=	ttrpym.exe, 00000000.00000003.239436981.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comn-u	ttrpym.exe, 00000000.00000003.239779476.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersL	ttrpym.exe, 00000000.00000003.244027978.0000000005E7D000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org	ttrpym.exe, 00000003.00000002.619638629.000000000343E000.00000004.00000001.sdmp	false		high
http://certificates.godaddy.com/repository/0	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cnma	ttrpym.exe, 00000000.00000003.239436981.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comroa	ttrpym.exe, 00000000.00000003.239201394.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	ttrpym.exe, 00000000.00000003.237159926.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	ttrpym.exe, 00000000.00000003.239779476.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krs-c	ttrpym.exe, 00000000.00000003.237159926.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ttrpym.exe, 00000000.00000003.247619500.0000000005E7B000.00000004.00000001.sdmp, ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	ttrpym.exe, 00000000.00000003.234788164.0000000005E7B000.00000004.00000001.sdmp, ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnm	ttrpym.exe, 00000000.00000003.237899138.0000000005E80000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.c	ttrpym.exe, 00000000.00000003.237222343.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot1534863067:AAHgkXiWvRLedLdzn8NhreUVQl7GIuV0U6g/sendDocument	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://api.telegram.orgx&.qloN	ttrpym.exe, 00000003.00000002.619638629.000000000343E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fonts.com	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	ttrpym.exe, 00000000.00000003.237222343.0000000005E7B000.00000004.00000001.sdmp, ttrpym.exe, 00000000.00000003.237159926.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comad	ttrpym.exe, 00000000.00000003.239779476.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	ttrpym.exe, 00000000.00000003.246313205.0000000005E88000.00000004.00000001.sdmp, ttrpym.exe, 00000000.00000003.243655870.0000000005E7D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	ttrpym.exe, 00000000.00000003.242053272.0000000005E83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comexc	ttrpym.exe, 00000000.00000003.238931261.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comt	ttrpym.exe, 00000000.00000003.233656365.0000000005E62000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTC	ttrpym.exe, 00000000.00000003.240021767.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/s	ttrpym.exe, 00000000.00000003.243841900.0000000005E7D000.00000004.00000001.sdmp	false		high
http://www.tiro.comp	ttrpym.exe, 00000000.00000003.239902821.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%(	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.comlic	ttrpym.exe, 00000000.00000003.240021767.0000000005E7B000.00000004.00000001.sdmp, ttrpym.exe, 00000000.00000003.239945309.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot1534863067:AAHgkXiWvRLedLdzn8NhreUVQl7GIuV0U6g/sendDocumentdocument-----	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comdd	ttrpym.exe, 00000000.00000003.239779476.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false		high
http://pmTUNK.com	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	ttrpym.exe, 00000000.00000003.239436981.0000000005E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comhly	ttrpym.exe, 00000000.00000003.238931261.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	ttrpym.exe, 00000000.00000003.245848821.0000000005E9E000.00000004.00000001.sdmp	false		high
http://www.monotype.	ttrpym.exe, 00000000.00000003.243086872.0000000005E7D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comm	ttrpym.exe, 00000000.00000002.264530973.00000000016D7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.godaddy.com/gdroot.crl0F	ttrpym.exe, 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comEacdW	ttrpym.exe, 00000000.00000003.240021767.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	ttrpym.exe, 00000000.00000002.272513220.0000000007072000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comt;F	ttrpym.exe, 00000000.00000003.239436981.0000000005E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://cert.s	ttrpym.exe, 00000003.00000003.522255884.0000000007DEC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/m	ttrpym.exe, 00000000.00000003.243841900.0000000005E7D000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	unknown	United Kingdom		62041	TELEGRAMRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345001
Start date:	27.01.2021
Start time:	15:38:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ttrpym.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:	mal100.troj.spyw.evad.winEXE@3/2@26/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.9% (good quality ratio 5.8%) • Quality average: 90.8% • Quality standard deviation: 21%
HCA Information:	• Successful, ratio: 75% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 168.61.161.212, 40.88.32.150, 23.210.248.85, 51.104.144.132, 67.26.81.254, 8.248.121.254, 8.241.123.254, 67.27.159.254, 67.27.158.126, 93.184.221.240, 51.103.5.159, 52.155.217.156, 20.54.26.129, 95.101.22.224, 95.101.22.216, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/345001/sample/ttrpym.exe

Simulations

Behavior and APIs

Time	Type	Description
15:39:49	API Interceptor	1008x Sleep call for process: ttrpym.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.154.167.220	SecuriteInfo.com.Trojan.PackedNET.519.21836.exe	Get hash	malicious	Browse	
	RFQ RPM202011-776JD.jpg.lnk	Get hash	malicious	Browse	
	commercial invoice packing list.xlsx	Get hash	malicious	Browse	
	Updated Invoice{swift..exe	Get hash	malicious	Browse	
	RFQ #6553928_PDF.exe	Get hash	malicious	Browse	
	MTD INVOICE.exe	Get hash	malicious	Browse	
	Payment Confirmation Paper - Customer Copy_pdf.exe	Get hash	malicious	Browse	
	MDS5932RFQ.exe	Get hash	malicious	Browse	
	TJyVCvjegT.exe	Get hash	malicious	Browse	
	Simulteanous-Project.exe	Get hash	malicious	Browse	
	PO 012658.exe	Get hash	malicious	Browse	
	RQN0004266.exe	Get hash	malicious	Browse	
	tnD89iJ2Vx.exe	Get hash	malicious	Browse	
	zff.exe	Get hash	malicious	Browse	
	trr.exe	Get hash	malicious	Browse	
	4dVgkhY953.exe	Get hash	malicious	Browse	
	CI_PL_BL.xlsx	Get hash	malicious	Browse	
	RFQ 130121.exe	Get hash	malicious	Browse	
	PO 130121.exe	Get hash	malicious	Browse	
	ttr.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.telegram.org	SecuriteInfo.com.Trojan.PackedNET.519.21836.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ RPM202011-776JD.jpg.lnk	Get hash	malicious	Browse	• 149.154.167.220
	commercial invoice packing list.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Updated Invoice{swift..exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ #6553928_PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	MTD INVOICE.exe	Get hash	malicious	Browse	• 149.154.167.220
	Payment Confirmation Paper - Customer Copy_pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	MDS5932RFQ.exe	Get hash	malicious	Browse	• 149.154.167.220
	Simulteanous-Project.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 012658.exe	Get hash	malicious	Browse	• 149.154.167.220
	RQN0004266.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Trojan.PackedNET.500.8394.exe	Get hash	malicious	Browse	• 149.154.167.220
	tnD89iJ2Vx.exe	Get hash	malicious	Browse	• 149.154.167.220
	zff.exe	Get hash	malicious	Browse	• 149.154.167.220
	trr.exe	Get hash	malicious	Browse	• 149.154.167.220
	4dVgkhY953.exe	Get hash	malicious	Browse	• 149.154.167.220
	CI_PL_BL.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	RFQ 130121.exe	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO 130121.exe	Get hash	malicious	Browse	• 149.154.167.220
	ttr.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEGRAMRU	SecuriteInfo.com.Trojan.PackedNET.519.21836.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ RPM202011-776JD.jpg.lnk	Get hash	malicious	Browse	• 149.154.167.220
	commercial invoice packing list.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Updated Invoice{swift..exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ #6553928_PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	MTD INVOICE.exe	Get hash	malicious	Browse	• 149.154.167.220
	Payment Confirmation Paper - Customer Copy_pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	MDS5932RFQ.exe	Get hash	malicious	Browse	• 149.154.167.220
	TJyVCvjegT.exe	Get hash	malicious	Browse	• 149.154.167.220
	Simulteanous-Project.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 012658.exe	Get hash	malicious	Browse	• 149.154.167.220
	RQN0004266.exe	Get hash	malicious	Browse	• 149.154.167.220
	tnD89iJ2Vx.exe	Get hash	malicious	Browse	• 149.154.167.220
	zff.exe	Get hash	malicious	Browse	• 149.154.167.220
	trr.exe	Get hash	malicious	Browse	• 149.154.167.220
	4dVgkhY953.exe	Get hash	malicious	Browse	• 149.154.167.220
	CI_PL_BL.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	RFQ 130121.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 130121.exe	Get hash	malicious	Browse	• 149.154.167.220
	ttr.exe	Get hash	malicious	Browse	• 149.154.167.220

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	roboforex4multisetup.exe	Get hash	malicious	Browse	• 149.154.167.220
	MV TAN BINH 135.pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Variant.Zusy.363976.7571.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Trojan.PackedNET.519.21836.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ RPM202011-776JD.jpg.lnk	Get hash	malicious	Browse	• 149.154.167.220
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ-Strip Casting Line.exe	Get hash	malicious	Browse	• 149.154.167.220
	NEW ORDER PO 20200909.exe	Get hash	malicious	Browse	• 149.154.167.220
	U1G3qA2l4I.exe	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file.exe	Get hash	malicious	Browse	• 149.154.167.220
	file.exe	Get hash	malicious	Browse	• 149.154.167.220
	Updated Invoice{swift..exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.BehavesLike.Win32.Generic.mh.exe	Get hash	malicious	Browse	• 149.154.167.220
	file.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ #6553928_PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	SPpfYOx5Ju.exe	Get hash	malicious	Browse	• 149.154.167.220
	MTD INVOICE.exe	Get hash	malicious	Browse	• 149.154.167.220
	file.exe	Get hash	malicious	Browse	• 149.154.167.220
	Online_doc20.01.exe	Get hash	malicious	Browse	• 149.154.167.220
	090008000000000000.exe	Get hash	malicious	Browse	• 149.154.167.220

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\ttrpym.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\nozq152y.bbo\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\ttrpym.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6969296358976265
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBo2+tYeF+X:T5LLOpEO5J/Kn7U1uBo2UYeQ
MD5:	A9DBC7B8E523ABE3B02D77DBF2FCD645
SHA1:	DF5EE16ECF4B3B02E312F935AE81D4C5D2E91CA8
SHA-256:	39B4E45A062DEA6F541C18FA1A15C5C0DB43A59673A26E2EB5B8A4345EE767AE
SHA-512:	3CF87455263E395313E779D4F440D8405D86244E04B5F577BB9FA2F4A2069DE019D340F6B2F6EF420DEE3D3DEEFD4B58DA3FCA3BB802DE348E1A810D6379CC3B
Malicious:	false

C:\Users\user\AppData\Roaming\nozq152y.bbo\Chrome\Default\Cookies	
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.961464624984834
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:	ttrpym.exe
File size:	907776
MD5:	3b53c639bd8ea883e5036a040f833415
SHA1:	af2f707e2e787879a67994fbad96c3e2f418dd3a
SHA256:	eca6a35d952f84597c3917f4c77f8c0e2cdeea6101caa97906dc1904e6f9e0ea
SHA512:	d4788d45a4d9f240b1a1a39662af2e2ade354d8d2b2d6ac0488536f5e0f24531457fdba5ab2c8ea89cb359616ef83d774d52655e2281d46f63870972522b833
SSDEEP:	24576:5pVLHCXj6FjdUXDvOTmNjfUeNp8b/1TR01bNP8VZ:53LH+uddUTvOEzUC21TROb98V
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....*.... .....@.. .....@.....@..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4def2a
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:	0x6010ACC3 [Tue Jan 26 23:58:59 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0xdeed8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe0000	0x58c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	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	0xdcf30	0xdd000	False	0.963299367223	data	7.96541170313	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe0000	0x58c	0x600	False	0.414713541667	data	4.04029792959	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe0090	0x2fc	data		
RT_MANIFEST	0xe039c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

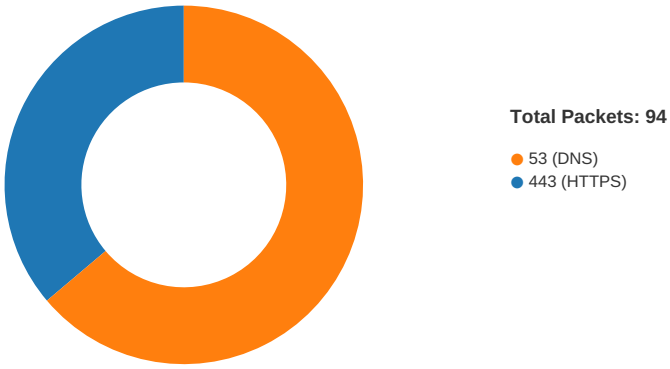
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	o.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	MathLib
ProductVersion	1.0.0.0
FileDescription	MathLib
OriginalFilename	o.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:40:28.687222004 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:28.737272978 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:28.737596035 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:28.793538094 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:28.843585014 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:28.843657970 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:28.843683004 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:28.843707085 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:28.843724012 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:28.843780994 CET	49733	443	192.168.2.7	149.154.167.220

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:40:28.843802929 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:28.844851971 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:28.844871044 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:28.844955921 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:28.851510048 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:28.901681900 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:28.982672930 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:29.034112930 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.037432909 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:29.087413073 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.087440014 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.087450027 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.087477922 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.087596893 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:29.087645054 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:29.135551929 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.136955023 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:29.138926029 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.138961077 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.138972998 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.138984919 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.138995886 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.139010906 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.139024019 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.139036894 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:29.139053106 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.139132977 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:29.189526081 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.191422939 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.191474915 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.191508055 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.191533089 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.191557884 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.191582918 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:29.191606998 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:30.302746058 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:30.302782059 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:30.302870989 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:31.300745010 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:31.350812912 CET	443	49733	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:31.350900888 CET	49733	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.070513010 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.120078087 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.120181084 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.121416092 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.170907021 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.171019077 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.171075106 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.171106100 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.171130896 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.171142101 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.171180964 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.172120094 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.172161102 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.172204018 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.174921989 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.224741936 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.244679928 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.294336081 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.295227051 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.344839096 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.344877958 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.344893932 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.344907999 CET	443	49737	149.154.167.220	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:40:32.345141888 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.345217943 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.396123886 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.396148920 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.396157980 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.396163940 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.396178961 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.396294117 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.396374941 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:32.396724939 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.396738052 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.396752119 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.447319984 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.447346926 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.447364092 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.447376966 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.447402954 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.447448969 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.447463989 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.612437010 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.612463951 CET	443	49737	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:32.612569094 CET	49737	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:36.677257061 CET	49744	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:36.728257895 CET	443	49744	149.154.167.220	192.168.2.7
Jan 27, 2021 15:40:36.728379011 CET	49744	443	192.168.2.7	149.154.167.220
Jan 27, 2021 15:40:36.729243040 CET	49744	443	192.168.2.7	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:39:33.715507984 CET	54329	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:33.763349056 CET	53	54329	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:34.669538021 CET	58052	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:34.717581034 CET	53	58052	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:35.843195915 CET	54008	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:35.892709017 CET	53	54008	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:38.025835991 CET	59451	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:38.082242966 CET	53	59451	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:39.053725004 CET	52914	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:39.101902008 CET	53	52914	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:40.089294910 CET	64569	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:40.139744043 CET	53	64569	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:41.635791063 CET	52816	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:41.694269896 CET	53	52816	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:42.905051947 CET	50781	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:42.952841997 CET	53	50781	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:44.429778099 CET	54230	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:44.479804039 CET	53	54230	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:45.867139101 CET	54911	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:45.917840004 CET	53	54911	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:46.875595093 CET	49958	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:46.923955917 CET	53	49958	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:47.852305889 CET	50860	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:47.900228024 CET	53	50860	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:49.135725021 CET	50452	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:49.186652899 CET	53	50452	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:50.156994104 CET	59730	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:50.221220016 CET	53	59730	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:51.147923946 CET	59310	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:51.207005978 CET	53	59310	8.8.8.8	192.168.2.7
Jan 27, 2021 15:39:54.711616993 CET	51919	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:39:54.772500038 CET	53	51919	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:04.847881079 CET	64296	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:04.898616076 CET	53	64296	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:40:22.687508106 CET	56680	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:22.736802101 CET	53	56680	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:22.843063116 CET	58820	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:22.893771887 CET	53	58820	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:23.025090933 CET	60983	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:23.072978020 CET	53	60983	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:26.948806047 CET	49247	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:27.724040985 CET	52286	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:28.005475998 CET	49247	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:28.658900976 CET	53	49247	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:28.659524918 CET	53	49247	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:28.690206051 CET	53	52286	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:29.574579000 CET	56064	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:29.636046886 CET	53	56064	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:30.392115116 CET	63744	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:30.474877119 CET	53	63744	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:31.338669062 CET	61457	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:31.390422106 CET	53	61457	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:32.106720924 CET	58367	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:32.163254023 CET	53	58367	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:32.832277060 CET	60599	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:32.891266108 CET	53	60599	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:33.527162075 CET	59571	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:33.584872007 CET	53	59571	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:33.710160971 CET	52689	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:33.773241043 CET	53	52689	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:34.985593081 CET	50290	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:35.044379950 CET	53	50290	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:36.149755001 CET	60427	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:36.205991030 CET	53	60427	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:36.624577045 CET	56209	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:36.675945044 CET	53	56209	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:37.106697083 CET	59582	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:37.165129900 CET	53	59582	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:37.999283075 CET	60949	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:38.055941105 CET	53	60949	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:38.533976078 CET	58542	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:38.596560955 CET	53	58542	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:42.044061899 CET	59179	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:42.094304085 CET	53	59179	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:47.259381056 CET	60927	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:47.310029984 CET	53	60927	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:52.646893978 CET	57854	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:52.697794914 CET	53	57854	8.8.8.8	192.168.2.7
Jan 27, 2021 15:40:58.084070921 CET	62026	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:40:58.134624004 CET	53	62026	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:03.597238064 CET	59453	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:03.645111084 CET	53	59453	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:09.098335028 CET	62468	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:09.146516085 CET	53	62468	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:09.195938110 CET	52563	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:09.243799925 CET	53	52563	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:10.637166023 CET	54721	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:10.693717957 CET	53	54721	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:14.693689108 CET	62826	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:14.746314049 CET	53	62826	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:20.273941994 CET	62046	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:20.332885981 CET	53	62046	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:30.856502056 CET	51223	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:30.914367914 CET	53	51223	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:31.014096022 CET	63908	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:31.070439100 CET	53	63908	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:35.566085100 CET	49226	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:35.624517918 CET	53	49226	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:41:40.251019001 CET	60212	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:40.301875114 CET	53	60212	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:44.977015972 CET	58867	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:45.026854038 CET	53	58867	8.8.8.8	192.168.2.7
Jan 27, 2021 15:41:55.161653042 CET	50864	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:56.198138952 CET	50864	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:41:56.248830080 CET	53	50864	8.8.8.8	192.168.2.7
Jan 27, 2021 15:42:03.052429914 CET	61504	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:42:03.101008892 CET	53	61504	8.8.8.8	192.168.2.7
Jan 27, 2021 15:42:11.725560904 CET	60231	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:42:11.773346901 CET	53	60231	8.8.8.8	192.168.2.7
Jan 27, 2021 15:42:20.497102022 CET	50095	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:42:20.547625065 CET	53	50095	8.8.8.8	192.168.2.7
Jan 27, 2021 15:42:29.290561914 CET	59654	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:42:30.305404902 CET	59654	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:42:31.301431894 CET	59654	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:42:31.349600077 CET	53	59654	8.8.8.8	192.168.2.7
Jan 27, 2021 15:42:37.549274921 CET	58233	53	192.168.2.7	8.8.8.8
Jan 27, 2021 15:42:37.599611998 CET	53	58233	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:40:26.948806047 CET	192.168.2.7	8.8.8.8	0x3f26	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:28.005475998 CET	192.168.2.7	8.8.8.8	0x3f26	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:31.338669062 CET	192.168.2.7	8.8.8.8	0x4202	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:36.624577045 CET	192.168.2.7	8.8.8.8	0x8bad	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:42.044061899 CET	192.168.2.7	8.8.8.8	0x307b	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:47.259381056 CET	192.168.2.7	8.8.8.8	0xc18c	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:52.646893978 CET	192.168.2.7	8.8.8.8	0xc3dc	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:58.084070921 CET	192.168.2.7	8.8.8.8	0x399f	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:03.597238064 CET	192.168.2.7	8.8.8.8	0x47a	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:09.098335028 CET	192.168.2.7	8.8.8.8	0x8b7b	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:14.693689108 CET	192.168.2.7	8.8.8.8	0x2aa9	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:20.273941994 CET	192.168.2.7	8.8.8.8	0x6dd9	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:30.856502056 CET	192.168.2.7	8.8.8.8	0xfd15	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:31.014096022 CET	192.168.2.7	8.8.8.8	0xdb27	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:35.566085100 CET	192.168.2.7	8.8.8.8	0x3a3c	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:40.251019001 CET	192.168.2.7	8.8.8.8	0x5d07	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:44.977015972 CET	192.168.2.7	8.8.8.8	0x9502	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:55.161653042 CET	192.168.2.7	8.8.8.8	0x93ca	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:56.198138952 CET	192.168.2.7	8.8.8.8	0x93ca	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:03.052429914 CET	192.168.2.7	8.8.8.8	0xcb65	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:11.725560904 CET	192.168.2.7	8.8.8.8	0x5bdd	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:20.497102022 CET	192.168.2.7	8.8.8.8	0x6a7e	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:29.290561914 CET	192.168.2.7	8.8.8.8	0xc759	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:30.305404902 CET	192.168.2.7	8.8.8.8	0xc759	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:42:31.301431894 CET	192.168.2.7	8.8.8.8	0xc759	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:37.549274921 CET	192.168.2.7	8.8.8.8	0xc568	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:40:28.658900976 CET	8.8.8.8	192.168.2.7	0x3f26	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:28.659524918 CET	8.8.8.8	192.168.2.7	0x3f26	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:31.390422106 CET	8.8.8.8	192.168.2.7	0x4202	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:36.675945044 CET	8.8.8.8	192.168.2.7	0x8bad	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:42.094304085 CET	8.8.8.8	192.168.2.7	0x307b	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:47.310029984 CET	8.8.8.8	192.168.2.7	0xc18c	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:52.697794914 CET	8.8.8.8	192.168.2.7	0xc3dc	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:58.134624004 CET	8.8.8.8	192.168.2.7	0x399f	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:03.645111084 CET	8.8.8.8	192.168.2.7	0x47a	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:09.146516085 CET	8.8.8.8	192.168.2.7	0x8b7b	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:14.746314049 CET	8.8.8.8	192.168.2.7	0x2aa9	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:20.332885981 CET	8.8.8.8	192.168.2.7	0x6dd9	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:30.914367914 CET	8.8.8.8	192.168.2.7	0xfd15	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:31.070439100 CET	8.8.8.8	192.168.2.7	0xdb27	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:35.624517918 CET	8.8.8.8	192.168.2.7	0x3a3c	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:40.301875114 CET	8.8.8.8	192.168.2.7	0x5d07	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:45.026854038 CET	8.8.8.8	192.168.2.7	0x9502	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:56.248830080 CET	8.8.8.8	192.168.2.7	0x93ca	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:03.101008892 CET	8.8.8.8	192.168.2.7	0xcb65	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:11.773346901 CET	8.8.8.8	192.168.2.7	0x5bdd	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:20.547625065 CET	8.8.8.8	192.168.2.7	0x6a7e	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:31.349600077 CET	8.8.8.8	192.168.2.7	0xc759	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 27, 2021 15:42:37.599611998 CET	8.8.8.8	192.168.2.7	0xc568	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

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
Jan 27, 2021 15:40:28.844851971 CET	149.154.167.220	443	192.168.2.7	49733	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 15:40:32.172120094 CET	149.154.167.220	443	192.168.2.7	49737	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:40:36.780297041 CET	149.154.167.220	443	192.168.2.7	49744	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 15:40:42.199759960 CET	149.154.167.220	443	192.168.2.7	49752	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:40:47.413180113 CET	149.154.167.220	443	192.168.2.7	49753	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 15:40:52.801297903 CET	149.154.167.220	443	192.168.2.7	49754	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:40:58.239384890 CET	149.154.167.220	443	192.168.2.7	49755	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 15:41:03.753128052 CET	149.154.167.220	443	192.168.2.7	49756	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:41:09.253482103 CET	149.154.167.220	443	192.168.2.7	49757	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 15:41:14.850255013 CET	149.154.167.220	443	192.168.2.7	49760	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:41:20.446326017 CET	149.154.167.220	443	192.168.2.7	49761	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 15:41:31.024688005 CET	149.154.167.220	443	192.168.2.7	49762	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:41:35.728291988 CET	149.154.167.220	443	192.168.2.7	49764	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 15:41:40.411825895 CET	149.154.167.220	443	192.168.2.7	49765	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:41:45.141561031 CET	149.154.167.220	443	192.168.2.7	49766	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 15:41:56.357264996 CET	149.154.167.220	443	192.168.2.7	49767	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:42:03.210078001 CET	149.154.167.220	443	192.168.2.7	49768	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 15:42:11.882802963 CET	149.154.167.220	443	192.168.2.7	49769	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

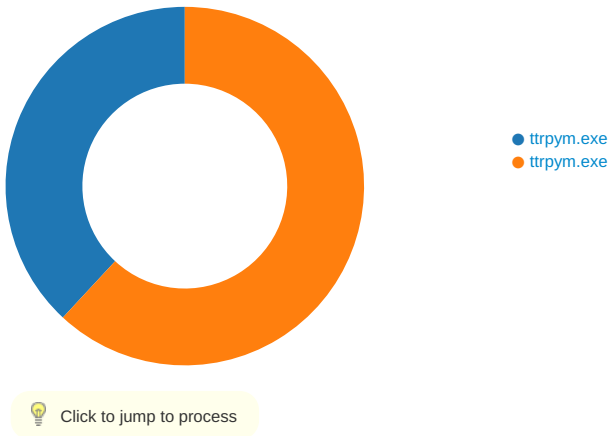
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:42:20.660326004 CET	149.154.167.220	443	192.168.2.7	49770	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jan 27, 2021 15:42:31.467353106 CET	149.154.167.220	443	192.168.2.7	49771	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 15:42:37.710154057 CET	149.154.167.220	443	192.168.2.7	49772	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ttrpym.exe PID: 6400 Parent PID: 5768

General

Start time:	15:39:38
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\ttrpym.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ttrpym.exe'
Imagebase:	0xb80000
File size:	907776 bytes
MD5 hash:	3B53C639BD8EA883E5036A040F833415
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6D3CCF06	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	6D3CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ttrpym.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ttrpym.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D6DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile

Analysis Process: ttrpym.exe PID: 6732 Parent PID: 6400

General

Start time:	15:39:52
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\ttrpym.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xaa0000
File size:	907776 bytes
MD5 hash:	3B53C639BD8EA883E5036A040F833415
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.619489004.0000000003391000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.614226904.0000000000F82000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	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	724660AC	unknown
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	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Roaming\nozq152y.bbo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5565BBD	CreateDirectoryW
C:\Users\user\AppData\Roaming\nozq152y.bbo\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5565BBD	CreateDirectoryW
C:\Users\user\AppData\Roaming\nozq152y.bbo\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5565BBD	CreateDirectoryW
C:\Users\user\AppData\Roaming\nozq152y.bbo\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5565C80	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nozq152y.bbo\Chrome\Default\Cookies	success or wait	1	5565D3A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nozq152y.bbo\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	5565C80	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5562143	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5562143	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5562143	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5562143	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5562143	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5562143	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	5562143	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\10ef7afe-b1dc-4901-88a7-8747a2b626a4	unknown	4096	success or wait	1	5562143	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	5562143	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5562143	ReadFile
C:\Users\user\AppData\Roaming\nozq152y.bbo\Chrome\Default\Cookies	unknown	16384	success or wait	2	5562143	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis