ID: 356448
Sample Name: Payment Confirmation.exe
Cookbook: default.jbs
Time: 08:06:50
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright null 2021

Copyright null 2021

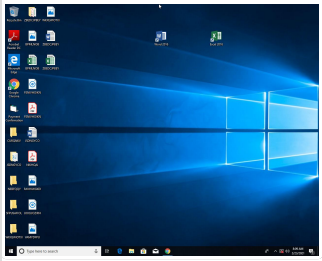
Analysis Report Payment Confirmation.exe

Overview

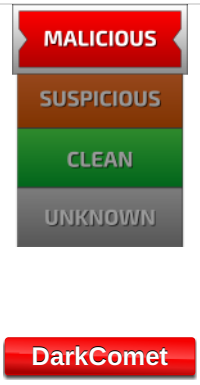
General Information

Sample Name:	Payment Confirmation.exe
Analysis ID:	356448
MD5:	800b9d7f3a47c5a.
SHA1:	67c825ca6d8f430..
SHA256:	e6edf54375a1431.
Tags:	DarkComet exe nVpn RAT

Most interesting Screenshot:



Detection



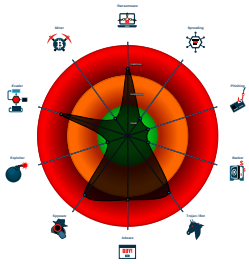
DarkComet

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Potential malicious icon found
- Yara detected DarkComet
- Contains functionality to capture and…
- Contains functionality to inject code …
- Contains functionality to log keystro…
- Contains functionality to log keystro…
- Contains functionality to register a lo…
- Drops PE files to the startup folder
- Initial sample is a PE file and has a …

Classification



Startup

- **System is w10x64**
- Payment Confirmation.exe (PID: 7012 cmdline: 'C:\Users\user\Desktop\Payment Confirmation.exe' MD5: 800B9D7F3A47C5A18DA78CB6A54F90BE)
  - cvcvsdf.exe (PID: 7064 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe MD5: 800B9D7F3A47C5A18DA78CB6A54F90BE)
    - cvcvsdf.exe (PID: 7148 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe MD5: 800B9D7F3A47C5A18DA78CB6A54F90BE)
- cvcvsdf.exe (PID: 6340 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe' MD5: 800B9D7F3A47C5A18DA78CB6A54F90BE)
  - cvcvsdf.exe (PID: 4820 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe MD5: 800B9D7F3A47C5A18DA78CB6A54F90BE)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000003.365577575.00000000023BA000.00000004.00000001.sdmp	DarkComet_2	DarkComet	Jean-Philippe Teissier / @Jipe_	• 0x928:$c: DC_MUTEX- • 0x9c8:$c: DC_MUTEX-
00000008.00000002.365956885.000000000400000.00000040.00000001.sdmp	Malware_QA_update	VT Research QA uploaded malware - file update.exe	Florian Roth	• 0x7be68:$x1: UnActiveOfflineKeylogger • 0x7c92c:$x2: BTRESULTDownload File|Mass Download : File Downloaded , Executing new one in temp dir...| • 0x7bdcc:$x3: ActiveOnlineKeylogger • 0x7c814:$x6: BTRESULTUpdate from URL|Update : File Downloaded , Executing new one in temp dir...| • 0x7c6b5:$s2: Command successfully executed!\| • 0x6e6f4:$s4: I wasn't able to open the hosts file, maybe because UAC is enabled in remote computer !

Source	Rule	Description	Author	Strings
00000008.00000002.365956885.000000000400000.00000040.00000001.sdmp	RAT_DarkComet	Detects DarkComet RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7c79c:$a1: #BOT#URLUpdate • 0x7c6b5:$a2: Command successfully executed! • 0x13f8:$b1: FastMM Borland Edition • 0x2b884:$b2: %s, ClassID: %s • 0x6e6f4:$b3: I wasn't able to open the hosts file • 0x7c5a0:$b4: #BOT#VisitUrl • 0x62bec:$b5: #KCMDDC
00000008.00000002.365956885.000000000400000.00000040.00000001.sdmp	JoeSecurity_DarkCometRat	Yara detected DarkComet	Kevin Breen <kevin@techanarchy.net>	
00000008.00000002.365956885.000000000400000.00000040.00000001.sdmp	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
Click to see the 19 entries				

Unpacked PEs

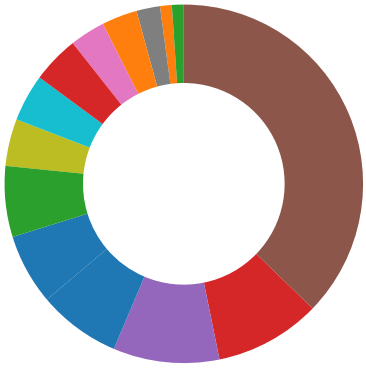
Source	Rule	Description	Author	Strings
8.2.cvcvsdf.exe.400000.0.raw.unpack	Malware_QA_update	VT Research QA uploaded malware - file update.exe	Florian Roth	• 0x7be68:$x1: UnActiveOfflineKeylogger • 0x7c92c:$x2: BTRESULTDownload File|Mass Download : File Downloaded , Executing new one in temp dir...| • 0x7bdcc:$x3: ActiveOnlineKeylogger • 0x7c814:$x6: BTRESULTUpdate from URL|Update : File Downloaded , Executing new one in temp dir...| • 0x7c6b5:$s2: Command successfully executed!\| • 0x6e6f4:$s4: I wasn't able to open the hosts file, maybe because UAC is enabled in remote computer !
8.2.cvcvsdf.exe.400000.0.raw.unpack	RAT_DarkComet	Detects DarkComet RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7c79c:$a1: #BOT#URLUpdate • 0x7c6b5:$a2: Command successfully executed! • 0x13f8:$b1: FastMM Borland Edition • 0x2b884:$b2: %s, ClassID: %s • 0x6e6f4:$b3: I wasn't able to open the hosts file • 0x7c5a0:$b4: #BOT#VisitUrl • 0x62bec:$b5: #KCMDDC
8.2.cvcvsdf.exe.400000.0.raw.unpack	JoeSecurity_DarkCometRat	Yara detected DarkComet	Kevin Breen <kevin@techanarchy.net>	
8.2.cvcvsdf.exe.400000.0.raw.unpack	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
8.2.cvcvsdf.exe.400000.0.raw.unpack	DarkComet_1	DarkComet RAT	botherder https://github.com/botherder	• 0x7c5b8:$bot1: #BOT#OpenUrl • 0x7c634:$bot2: #BOT#Ping • 0x7c67c:$bot3: #BOT#RunPrompt • 0x7c73c:$bot4: #BOT#SvrUninstall • 0x7c874:$bot5: #BOT#URLDownload • 0x7c79c:$bot6: #BOT#URLUpdate • 0x7c5a0:$bot7: #BOT#VisitUrl • 0x7c6e0:$bot8: #BOT#CloseServer • 0x7caec:$ddos1: DDOSHTTPFLOOD • 0x7cb04:$ddos2: DDOSSYNFLOOD • 0x7cb1c:$ddos3: DDOSUDPFLOOD • 0x7bdcc:$keylogger1: ActiveOnlineKeylogger • 0x7bdee:$keylogger1: ActiveOnlineKeylogger • 0x7bdec:$keylogger2: UnActiveOnlineKeylogger • 0x7be48:$keylogger3: ActiveOfflineKeylogger • 0x7be6a:$keylogger3: ActiveOfflineKeylogger • 0x7be68:$keylogger4: UnActiveOfflineKeylogger
Click to see the 19 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection



- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Uses 32bit PE files

Networking:

- Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Contains functionality to capture and log keystrokes
- Contains functionality to log keystrokes
- Contains functionality to log keystrokes
- Contains functionality to register a low level keyboard hook

System Summary:

- Malicious sample detected (through community Yara rule)
- Potential malicious icon found
- Yara detected DarkComet
- Initial sample is a PE file and has a suspicious name

Boot Survival:

- Drops PE files to the startup folder

HIPS / PFW / Operating System Protection Evasion:

- Contains functionality to inject code into remote processes

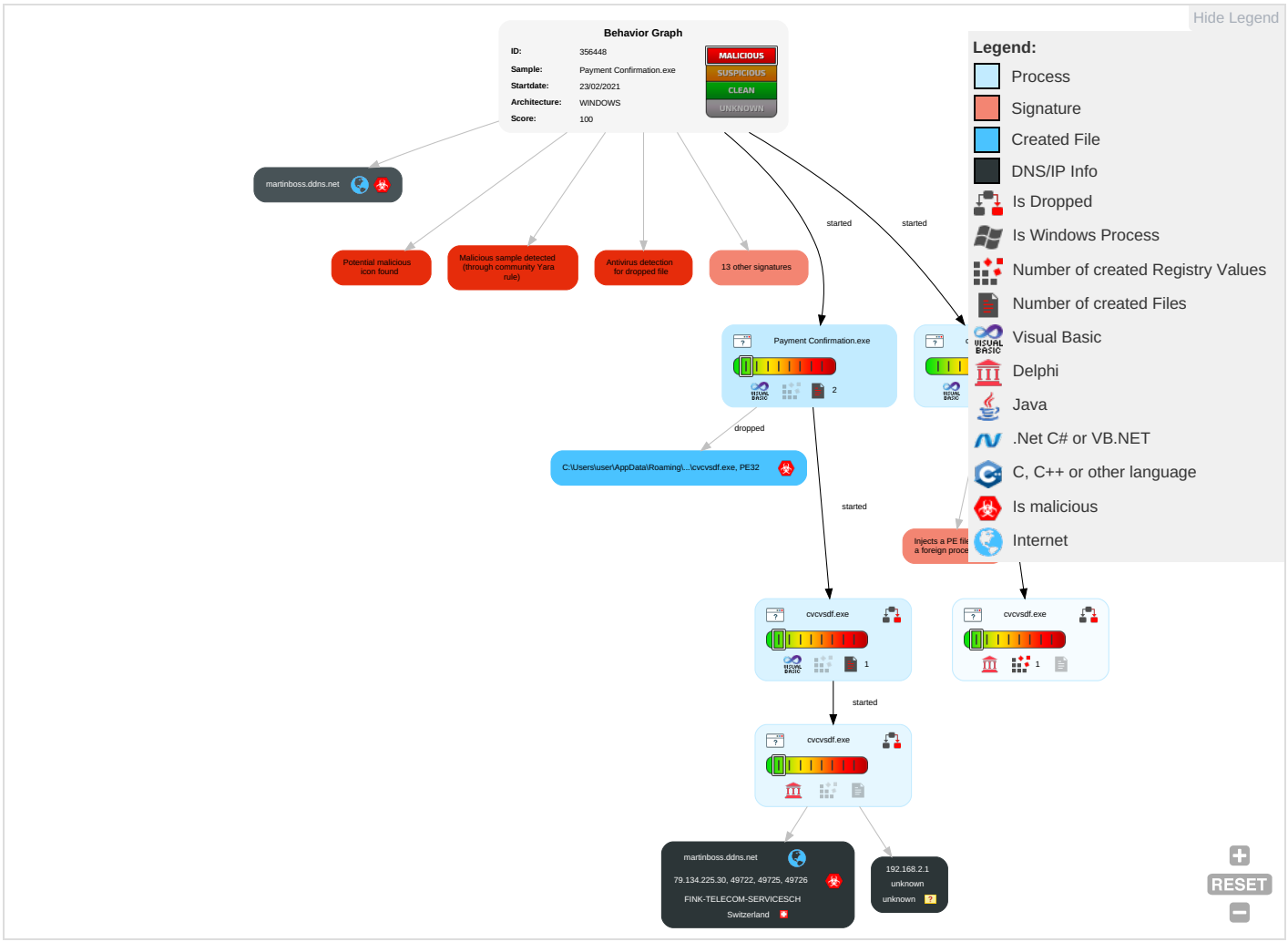
Copyright null 2021

Injects a PE file into a foreign processes

Mitre Att&ck Matrix

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

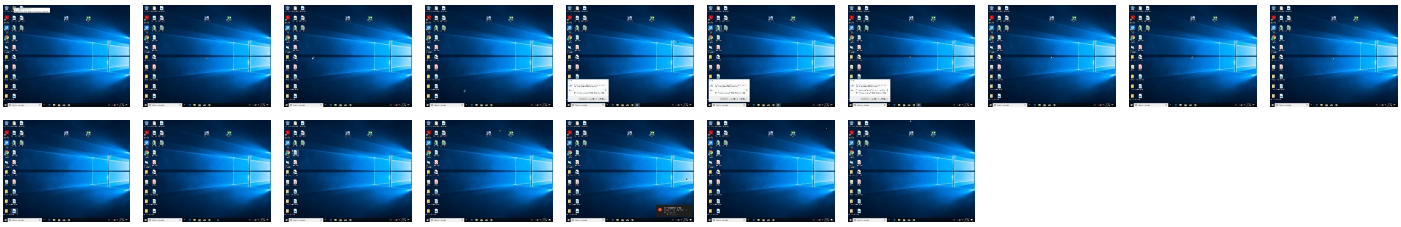
Behavior Graph



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
Payment Confirmation.exe	100%	Avira	TR/Dropper.Gen	
Payment Confirmation.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe	48%	ReversingLabs	Win32.Backdoor.DarkComet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.cvcvsdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.2.cvcvsdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
1.0.cvcvsdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.Payment Confirmation.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.cvcvsdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.2.cvcvsdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.cvcvsdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Copyright null 2021

Source	Detection	Scanner	Label	Link	Download
8.0.cvcvsdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.1.cvcvsdf.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
8.1.cvcvsdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Payment Confirmation.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.2.cvcvsdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://technohub.in	0%	Avira URL Cloud	safe	
http://www.technohub.in/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
martinboss.ddns.net	79.134.225.30	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://technohub.in	Payment Confirmation.exe	false	• Avira URL Cloud: safe	unknown
http://www.technohub.in/	Payment Confirmation.exe	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.30	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356448
Start date:	23.02.2021
Start time:	08:06:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Confirmation.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:	25
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.rans.troj.adwa.spyw.evad.winEXE@8/1@84/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.8% (good quality ratio 27.1%) • Quality average: 74.8% • Quality standard deviation: 27.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Copyright null 2021

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 51.104.139.180, 104.43.139.144, 204.79.197.200, 13.107.21.200, 52.255.188.83, 168.61.161.212, 92.122.145.220, 52.147.198.201, 93.184.221.240, 52.155.217.156, 51.103.5.186, 20.54.26.129, 92.122.213.247, 92.122.213.194, 184.30.24.56, 51.132.208.181 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, vip2-par02p.wns.notify.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:07:43	API Interceptor	1030x Sleep call for process: cvcvsdf.exe modified
08:07:43	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.30	JOIN.exe	Get hash	malicious	Browse	
	Itinerary.pdf.exe	Get hash	malicious	Browse	
	vVH0wIFYFd.exe	Get hash	malicious	Browse	
	GWee9QSphp.exe	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.dc.exe	Get hash	malicious	Browse	
	Import and Export Regulation.xlsx	Get hash	malicious	Browse	
	BBdzKOGQ36.exe	Get hash	malicious	Browse	
	BL.exe	Get hash	malicious	Browse	
	Payment Invoice.exe	Get hash	malicious	Browse	
	Payment Invoice.pdf.exe	Get hash	malicious	Browse	
	Inquiries_scan_011023783591374376585.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
martinboss.ddns.net	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	rjHlt1zz28.exe	Get hash	malicious	Browse	• 79.134.225.49
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 79.134.225.49
	document.exe	Get hash	malicious	Browse	• 79.134.225.122
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 79.134.225.105
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30
	Delivery pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 79.134.225.105
	fnfqzfwC44.exe	Get hash	malicious	Browse	• 79.134.225.25
	Solicitud de oferta 6100003768.exe	Get hash	malicious	Browse	• 79.134.225.96
	Nrfgylra.exe	Get hash	malicious	Browse	• 79.134.225.96
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	HTQ19-P0401-Q0539 NE-Q22940 GR2P5 TYPBLDG-NASER AL FERDAN.exe	Get hash	malicious	Browse	• 79.134.225.62
	Form pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	Quotation 3342688.exe	Get hash	malicious	Browse	• 79.134.225.120
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 79.134.225.76
	Orden.exe	Get hash	malicious	Browse	• 79.134.225.6
	Ordine.exe	Get hash	malicious	Browse	• 79.134.225.11

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe

Process:	C:\Users\user\Desktop\Payment Confirmation.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	909312
Entropy (8bit):	5.739183525709254
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe	
SSDEEP:	12288:c1N7GYtRi6Hczy4QufM4zr9H7NH8rxRYAjjUIPg:c7wzyxuU4zZbNM1jUIPg
MD5:	800B9D7F3A47C5A18DA78CB6A54F90BE
SHA1:	67C825CA6D8F430FDFC4CBCA78C442600DB7CCF0
SHA-256:	E6EDF54375A14314AA44DB9FE8CDD48368338E7ED873F25BA2A6A5FF4381D233
SHA-512:	3F36217FC2E0AFD41D16EA8E35628B00BD8E094194B892E551BA2B39FFFAF16E67ECE937ADE136FE03286FEF59718A76FC83081A7CB1DD2F8A7EFA811A992E87
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 48%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z.....Rich.....PE..L...Y..._..... .@.....X,.....@.....D.....D...(.....8... .....T.....text...T..... ..`.data.....@....rsrc.....0.....@..@I.[J.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.739183525709254
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Payment Confirmation.exe
File size:	909312
MD5:	800b9d7f3a47c5a18da78cb6a54f90be
SHA1:	67c825ca6d8f430fdfc4cbca78c442600db7ccf0
SHA256:	e6edf54375a14314aa44db9fe8cdd48368338e7ed873f25ba2a6a5ff4381d233
SHA512:	3f36217fc2e0afd41d16ea8e35628b00bd8e094194b892e551ba2b39fffaf16e67ece937ade136fe03286fef59718a76fc83081a7cb1dd2f8a7efa811a992e87
SSDEEP:	12288:c1N7GYtRi6Hczy4QufM4zr9H7NH8rxRYAjjUIPg:c7wzyxuU4zZbNM1jUIPg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z.....Rich.....PE..L...Y..._.....@.....X,.....@

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x402c58
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5FD9DF59 [Wed Dec 16 10:20:09 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General

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:	d9b63245519b223a1f7026d72643602b

Entrypoint Preview

Instruction
push 00406B94h
call 00007F8D9C9835F5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
js 00007F8D9C98362Eh
aam 53h
clc
jp 00007F8D9C9835CEh
dec esi
mov ebx, 97158BF6h
int1
not dword ptr [ebp+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi+41h], cl
push ebx
dec eax
inc esi
push esp
push eax
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
pop es
fadd st(0), st(2)
xor eax, 139DB88Eh
inc edx
test al, 0Eh
inc edx
or esp, ecx
stosd
enter BAC4h, F3h
jl 00007F8D9C9835EAh
sub byte ptr [ecx+47B444AEh], ah
inc ecx
jc 00007F8D9C9835C4h
wait
into
cmp cl, byte ptr [edi-53h]

Copyright null 2021

Instruction
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add 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
pop ss
cmp eax, 00720000h
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [esi+72h], ah
insd
inc ecx
bound ebp, dword ptr [edi+75h]
je 00007F8D9C983602h
or eax, 41001A01h
bound ebp, dword ptr [edi+75h]
je 00007F8D9C983622h
dec esi
inc ecx
push ebx
dec eax
and byte ptr [esi+72h], 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	0x38844	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3c000	0xa2ea8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x254	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Copyright null 2021

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x38254	0x39000	False	0.297581722862	data	5.76638922611	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x3a000	0x1ff0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x3c000	0xa2ea8	0xa3000	False	0.369846086561	data	5.12810599289	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
BSDK	0x3c1dc	0xa24cc	data		
BSDK	0xde6a8	0x29	ASCII text, with CRLF line terminators		
RT_ICON	0xde6d4	0x130	data		
RT_ICON	0xde804	0x2e8	data		
RT_ICON	0xdeaec	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xdec14	0x30	data		
RT_VERSION	0xdec44	0x264	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	__vbaVarSub, __vbaStrI2, _CIcos, _adj_fptan, __vbaVarMove, __vbaStrI4, __vbaAryMove, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaLateIdCall, __vbaEnd, __vbaFreeVarList, _adj_fdiv_m64, __vbaPut4, __vbaRaiseEvent, __vbaNextEachVar, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaStrCat, __vbaLsetFixstr, __vbaRecDestruct, __vbaSetSystemError, __vbaHresultCheckObj, __vbaLenVar, _adj_fdiv_m32, __vbaAryVar, __vbaAryDestruct, __vbaVarForInit, __vbaExitProc, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaStrFixstr, __vbaBoolVarNull, _CIsin, __vbaVarCmpGt, __vbaChkstk, __vbaFileClose, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaPutOwner3, __vbaAryConstruct2, __vbaVarTstEq, __vbaI2I4, __vbaObjVar, DllFunctionCall, __vbaVarLateMemSt, __vbaCastObjVar, __vbaRedimPreserve, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, __vbaRecUniToAnsi, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, __vbaObjIs, __vbaVarAnd, EVENT_SINK_QueryInterface, __vbaUI1I4, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaInStrVar, __vbaUbound, __vbaGetOwner3, __vbaStrVarVal, __vbaVarCat, __vbaI2Var, _CIlog, __vbaErrorOverflow, __vbaFileOpen, __vbaR8Str, __vbaVar2Vec, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarSetVar, __vbaI4Var, __vbaVarCmpEq, __vbaAryLock, __vbaLateMemCall, __vbaVarAdd, __vbaVarDup, __vbaStrToAnsi, __vbaFpI4, __vbaVarCopy, __vbaVarLateMemCallLd, __vbaRecDestructAnsi, _CIatan, __vbaUI1Str, __vbaAryCopy, __vbaCastObj, __vbaStrMove, __vbaR8IntI4, __vbaForEachVar, _allmul, __vbaLateIdSt, _CItan, __vbaAryUnlock, __vbaVarForNext, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

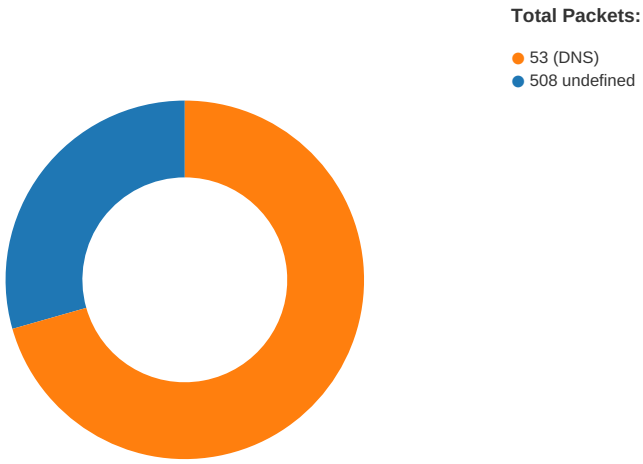
Description	Data
Translation	0x0409 0x04b0
InternalName	1
FileVersion	1.00
CompanyName	TECHNOHUB TECHNOLOGIES
Comments	NASH FTP VERSION 1.0.0
ProductName	NASH FREE FTP
ProductVersion	1.00
OriginalFilename	1.exe

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:07:45.274120092 CET	49722	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:45.351197004 CET	508	49722	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:45.955323935 CET	49722	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:46.032562971 CET	508	49722	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:46.646625996 CET	49722	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:46.725698948 CET	508	49722	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:46.829035044 CET	49725	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:46.908900023 CET	508	49725	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:47.517852068 CET	49725	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:47.600960016 CET	508	49725	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:48.253881931 CET	49725	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:48.333935022 CET	508	49725	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:48.493331909 CET	49726	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:48.572839022 CET	508	49726	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:49.127384901 CET	49726	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:49.204401016 CET	508	49726	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:49.830650091 CET	49726	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:49.907689095 CET	508	49726	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:50.043519974 CET	49728	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:50.120651960 CET	508	49728	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:50.644663095 CET	49728	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:50.722227097 CET	508	49728	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:51.252656937 CET	49728	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:51.329705954 CET	508	49728	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:51.433896065 CET	49730	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:51.511483908 CET	508	49730	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:52.018292904 CET	49730	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:52.095400095 CET	508	49730	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:52.627715111 CET	49730	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:52.704982996 CET	508	49730	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:52.840053082 CET	49731	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:52.922589064 CET	508	49731	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:53.424676895 CET	49731	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:53.504687071 CET	508	49731	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:54.018486977 CET	49731	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:54.098535061 CET	508	49731	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:54.207840919 CET	49732	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:54.285154104 CET	508	49732	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:54.799772978 CET	49732	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:54.878434896 CET	508	49732	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:55.396162033 CET	49732	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:55.474953890 CET	508	49732	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:55.574055910 CET	49733	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:55.655462027 CET	508	49733	79.134.225.30	192.168.2.6

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:07:56.159270048 CET	49733	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:56.239308119 CET	508	49733	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:56.878067970 CET	49733	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:56.958292007 CET	508	49733	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:57.140614986 CET	49734	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:57.217694044 CET	508	49734	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:57.878218889 CET	49734	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:57.955197096 CET	508	49734	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:58.487585068 CET	49734	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:58.566756964 CET	508	49734	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:58.668698072 CET	49735	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:58.745752096 CET	508	49735	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:59.378397942 CET	49735	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:07:59.455717087 CET	508	49735	79.134.225.30	192.168.2.6
Feb 23, 2021 08:07:59.956434965 CET	49735	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:00.034888029 CET	508	49735	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:00.121334076 CET	49736	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:00.200638056 CET	508	49736	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:00.711935043 CET	49736	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:00.789062977 CET	508	49736	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:01.301961899 CET	49736	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:01.379132032 CET	508	49736	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:01.481987953 CET	49737	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:01.562107086 CET	508	49737	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:02.066109896 CET	49737	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:02.146181107 CET	508	49737	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:02.659811974 CET	49737	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:02.742487907 CET	508	49737	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:02.826824903 CET	49738	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:02.903831005 CET	508	49738	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:03.409893990 CET	49738	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:03.487040997 CET	508	49738	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:03.988044024 CET	49738	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:04.073004007 CET	508	49738	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:04.153270006 CET	49739	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:04.235135078 CET	508	49739	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:04.738221884 CET	49739	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:04.820008993 CET	508	49739	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:05.332009077 CET	49739	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:05.413285971 CET	508	49739	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:05.500704050 CET	49740	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:05.582556009 CET	508	49740	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:06.097687960 CET	49740	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:06.178369045 CET	508	49740	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:06.691385031 CET	49740	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:06.771500111 CET	508	49740	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:06.859509945 CET	49741	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:06.936503887 CET	508	49741	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:07.441503048 CET	49741	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:07.521667004 CET	508	49741	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:08.035310030 CET	49741	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:08.112411022 CET	508	49741	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:08.203289986 CET	49742	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:08.281152010 CET	508	49742	79.134.225.30	192.168.2.6
Feb 23, 2021 08:08:08.785429001 CET	49742	508	192.168.2.6	79.134.225.30
Feb 23, 2021 08:08:08.862402916 CET	508	49742	79.134.225.30	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:07:31.546785116 CET	55074	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:31.546822071 CET	53	49283	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:31.569567919 CET	53	58377	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:31.595554113 CET	53	55074	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:07:32.532334089 CET	54513	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:32.581161022 CET	53	54513	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:33.356961012 CET	62044	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:33.406233072 CET	53	62044	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:34.305083036 CET	63791	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:34.356946945 CET	53	63791	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:34.987416029 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:35.047049046 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:35.247118950 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:35.299757004 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:36.451236010 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:36.514520884 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:37.377928019 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:37.430246115 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:38.374042988 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:38.422550917 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:39.172760010 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:39.221329927 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:39.998399973 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:40.052440882 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:41.539827108 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:41.591310978 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:42.617219925 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:42.674478054 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:43.793068886 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:43.844515085 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:44.619919062 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:44.669038057 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:45.206157923 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:45.266907930 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:45.539908886 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:45.597114086 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:46.536823034 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:46.589545965 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:46.766422033 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:46.827474117 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:48.432107925 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:48.491969109 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:49.686492920 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:49.738003969 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:49.969152927 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:50.028769016 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:50.607882023 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:50.656481981 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:51.367156982 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:51.431777954 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:52.781282902 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:52.838727951 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:54.145982027 CET	50010	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:54.205889940 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:55.510709047 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:55.571289062 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:57.053105116 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:57.111020088 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 08:07:58.610317945 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:07:58.667474031 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:00.063472986 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:00.120590925 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:01.420938015 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:01.480880976 CET	53	62208	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:02.774080038 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:02.825578928 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:04.102524996 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:04.152319908 CET	53	51818	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:08:05.439734936 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:05.499820948 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:06.808162928 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:06.858426094 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:08.144113064 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:08.202327967 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:08.285270929 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:08.336926937 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:09.473737955 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:09.530750990 CET	53	59329	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:10.930634975 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:10.987613916 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:12.319010019 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:12.376049042 CET	53	56129	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:14.125897884 CET	58177	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:14.188676119 CET	53	58177	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:15.721072912 CET	50700	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:15.780385971 CET	53	50700	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:17.264655113 CET	54069	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:17.316565990 CET	53	54069	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:18.647496939 CET	61178	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:18.696165085 CET	53	61178	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:19.964416027 CET	57017	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:20.020870924 CET	53	57017	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:21.351953030 CET	56327	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:21.412421942 CET	53	56327	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:22.707381964 CET	50243	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:22.767571926 CET	53	50243	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:24.057987928 CET	62055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:24.118077993 CET	53	62055	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:25.395737886 CET	61249	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:25.454222918 CET	53	61249	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:26.731435061 CET	65252	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:26.781805992 CET	53	65252	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:26.800857067 CET	64367	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:26.863466024 CET	53	64367	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:27.491439104 CET	55066	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:27.581167936 CET	53	55066	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:27.945303917 CET	60211	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:27.995989084 CET	53	60211	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:28.170456886 CET	56570	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:28.233465910 CET	53	56570	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:28.241755009 CET	58454	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:28.298862934 CET	53	58454	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:28.806243896 CET	55180	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:28.863424063 CET	53	55180	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:29.268851042 CET	58721	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:29.358316898 CET	53	58721	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:29.447592974 CET	57691	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:29.521596909 CET	53	57691	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:29.757359028 CET	52943	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:29.803540945 CET	59489	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:29.816936970 CET	53	52943	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:29.865108013 CET	53	59489	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:30.362148046 CET	64022	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:30.420394897 CET	53	64022	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:31.150052071 CET	60023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:31.200783014 CET	53	60023	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:31.305212975 CET	57193	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:31.365034103 CET	53	57193	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:32.359426022 CET	50248	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:32.410923958 CET	53	50248	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:33.486183882 CET	64413	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:33.546222925 CET	53	64413	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:08:34.813810110 CET	60429	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:34.865504026 CET	53	60429	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:34.949865103 CET	60345	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:35.001399040 CET	53	60345	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:35.441658974 CET	58730	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:35.500091076 CET	53	58730	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:36.518665075 CET	53830	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:36.570158005 CET	53	53830	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:38.047070026 CET	57226	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:38.095921993 CET	53	57226	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:38.622483969 CET	57880	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:38.680929899 CET	53	57880	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:39.627697945 CET	60850	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:39.687787056 CET	53	60850	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:41.073613882 CET	53187	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:41.122194052 CET	53	53187	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:42.702431917 CET	55830	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:42.761286020 CET	53	55830	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:44.271133900 CET	55145	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:44.328437090 CET	53	55145	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:45.681833029 CET	64091	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:45.741550922 CET	53	64091	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:47.037139893 CET	55728	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:47.088871002 CET	53	55728	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:48.411649942 CET	55694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:48.471918106 CET	53	55694	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:49.770519972 CET	53926	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:49.829307079 CET	53	53926	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:51.140413046 CET	65531	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:51.200211048 CET	53	65531	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:52.501919985 CET	65437	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:52.559010029 CET	53	65437	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:53.880294085 CET	54590	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:53.929353952 CET	53	54590	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:55.225248098 CET	51318	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:55.287211895 CET	53	51318	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:56.594271898 CET	60888	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:56.655138016 CET	53	60888	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:57.936106920 CET	58474	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:57.995523930 CET	53	58474	8.8.8.8	192.168.2.6
Feb 23, 2021 08:08:59.288147926 CET	64575	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:08:59.348825932 CET	53	64575	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:00.650860071 CET	59092	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:00.699660063 CET	53	59092	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:01.998353958 CET	57483	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:02.060837984 CET	53	57483	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:03.361493111 CET	53830	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:03.421380997 CET	53	53830	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:04.711440086 CET	49809	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:04.770749092 CET	53	49809	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:06.059376955 CET	52814	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:06.107952118 CET	53	52814	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:07.439800024 CET	51069	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:07.491424084 CET	53	51069	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:11.888250113 CET	56526	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:11.949131966 CET	53	56526	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:14.215146065 CET	50512	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:14.274820089 CET	53	50512	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:15.589412928 CET	51679	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:15.646821022 CET	53	51679	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:16.988843918 CET	56071	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:17.040496111 CET	53	56071	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:17.342309952 CET	58950	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:17.393151045 CET	53	58950	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:09:18.359960079 CET	57035	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:18.422797918 CET	53	57035	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:19.847336054 CET	54122	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:19.907733917 CET	53	54122	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:21.211339951 CET	56759	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:21.270256996 CET	53	56759	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:22.623347044 CET	59220	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:22.674866915 CET	53	59220	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:24.028367043 CET	62211	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:24.088788033 CET	53	62211	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:25.404438972 CET	62033	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:25.453197002 CET	53	62033	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:26.753979921 CET	61244	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:26.810834885 CET	53	61244	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:28.154974937 CET	53696	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:28.206527948 CET	53	53696	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:29.502564907 CET	50733	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:29.562889099 CET	53	50733	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:30.856758118 CET	55770	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:30.915587902 CET	53	55770	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:32.198609114 CET	54525	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:32.256922007 CET	53	54525	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:33.567120075 CET	61760	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:33.624037027 CET	53	61760	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:34.927153111 CET	63822	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:34.986808062 CET	53	63822	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:36.342387915 CET	50957	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:36.401557922 CET	53	50957	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:37.706017017 CET	59666	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:37.760108948 CET	53	59666	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:39.064377069 CET	52223	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:39.123634100 CET	53	52223	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:40.407258034 CET	60136	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:40.464591026 CET	53	60136	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:41.762677908 CET	55649	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:41.819736004 CET	53	55649	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:43.145524979 CET	51524	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:43.194669008 CET	53	51524	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:44.451947927 CET	59141	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:44.511965990 CET	53	59141	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:45.776679039 CET	49682	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:45.826669931 CET	53	49682	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:47.092387915 CET	49709	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:47.149457932 CET	53	49709	8.8.8.8	192.168.2.6
Feb 23, 2021 08:09:48.404412031 CET	59384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:09:48.462491989 CET	53	59384	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:07:45.206157923 CET	192.168.2.6	8.8.8.8	0xd9b2	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:46.766422033 CET	192.168.2.6	8.8.8.8	0x4cfc	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:48.432107925 CET	192.168.2.6	8.8.8.8	0x7b0b	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:49.969152927 CET	192.168.2.6	8.8.8.8	0x2dc4	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:51.367156982 CET	192.168.2.6	8.8.8.8	0x4881	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:52.781282902 CET	192.168.2.6	8.8.8.8	0x1d0e	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:54.145982027 CET	192.168.2.6	8.8.8.8	0x44f3	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:55.510709047 CET	192.168.2.6	8.8.8.8	0x5e4c	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:07:57.053105116 CET	192.168.2.6	8.8.8.8	0xb8bd	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:58.610317945 CET	192.168.2.6	8.8.8.8	0xda71	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:00.063472986 CET	192.168.2.6	8.8.8.8	0x1e15	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:01.420938015 CET	192.168.2.6	8.8.8.8	0x6514	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:02.774080038 CET	192.168.2.6	8.8.8.8	0x7f53	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:04.102524996 CET	192.168.2.6	8.8.8.8	0xa722	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:05.439734936 CET	192.168.2.6	8.8.8.8	0x3ff4	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:06.808162928 CET	192.168.2.6	8.8.8.8	0x30ca	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:08.144113064 CET	192.168.2.6	8.8.8.8	0x337b	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:09.473737955 CET	192.168.2.6	8.8.8.8	0x982e	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:10.930634975 CET	192.168.2.6	8.8.8.8	0xc475	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:12.319010019 CET	192.168.2.6	8.8.8.8	0xcbf7	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:14.125897884 CET	192.168.2.6	8.8.8.8	0xe579	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:15.721072912 CET	192.168.2.6	8.8.8.8	0x4ad8	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:17.264655113 CET	192.168.2.6	8.8.8.8	0xdd90	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:18.647496939 CET	192.168.2.6	8.8.8.8	0x9949	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:19.964416027 CET	192.168.2.6	8.8.8.8	0x4fb6	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:21.351953030 CET	192.168.2.6	8.8.8.8	0xe93	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:22.707381964 CET	192.168.2.6	8.8.8.8	0x419a	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:24.057987928 CET	192.168.2.6	8.8.8.8	0xdb1a	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:25.395737886 CET	192.168.2.6	8.8.8.8	0xe2f3	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:26.731435061 CET	192.168.2.6	8.8.8.8	0x578e	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:28.241755009 CET	192.168.2.6	8.8.8.8	0x9933	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:29.757359028 CET	192.168.2.6	8.8.8.8	0xb6c4	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:31.305212975 CET	192.168.2.6	8.8.8.8	0xb961	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:33.486183882 CET	192.168.2.6	8.8.8.8	0x49df	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:34.949865103 CET	192.168.2.6	8.8.8.8	0xf99a	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:36.518665075 CET	192.168.2.6	8.8.8.8	0x6d0b	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:38.047070026 CET	192.168.2.6	8.8.8.8	0x6c72	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:39.627697945 CET	192.168.2.6	8.8.8.8	0x2355	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:41.073613882 CET	192.168.2.6	8.8.8.8	0xfb39	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:42.702431917 CET	192.168.2.6	8.8.8.8	0xf8e6	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:44.271133900 CET	192.168.2.6	8.8.8.8	0x4b22	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:45.681833029 CET	192.168.2.6	8.8.8.8	0xf653	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:47.037139893 CET	192.168.2.6	8.8.8.8	0xc499	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:48.411649942 CET	192.168.2.6	8.8.8.8	0x70af	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:49.770519972 CET	192.168.2.6	8.8.8.8	0x5a34	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:08:51.140413046 CET	192.168.2.6	8.8.8.8	0xb366	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:52.501919985 CET	192.168.2.6	8.8.8.8	0x81af	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:53.880294085 CET	192.168.2.6	8.8.8.8	0x712b	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:55.225248098 CET	192.168.2.6	8.8.8.8	0x38c9	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:56.594271898 CET	192.168.2.6	8.8.8.8	0x622d	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:57.936106920 CET	192.168.2.6	8.8.8.8	0xb17e	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:59.288147926 CET	192.168.2.6	8.8.8.8	0x3e14	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:00.650860071 CET	192.168.2.6	8.8.8.8	0x6718	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:01.998353958 CET	192.168.2.6	8.8.8.8	0x967b	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:03.361493111 CET	192.168.2.6	8.8.8.8	0xc85c	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:04.711440086 CET	192.168.2.6	8.8.8.8	0xbc83	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:06.059376955 CET	192.168.2.6	8.8.8.8	0xa3bf	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:07.439800024 CET	192.168.2.6	8.8.8.8	0xf7c8	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:14.215146065 CET	192.168.2.6	8.8.8.8	0xd9b8	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:15.589412928 CET	192.168.2.6	8.8.8.8	0x1a8d	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:16.988843918 CET	192.168.2.6	8.8.8.8	0x92d1	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:18.359960079 CET	192.168.2.6	8.8.8.8	0xeef5	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:19.847336054 CET	192.168.2.6	8.8.8.8	0x3ba0	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:21.211339951 CET	192.168.2.6	8.8.8.8	0xf3d8	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:22.623347044 CET	192.168.2.6	8.8.8.8	0x91	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:24.028367043 CET	192.168.2.6	8.8.8.8	0x80fe	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:25.404438972 CET	192.168.2.6	8.8.8.8	0x5d60	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:26.753979921 CET	192.168.2.6	8.8.8.8	0x34fe	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:28.154974937 CET	192.168.2.6	8.8.8.8	0x6d93	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:29.502564907 CET	192.168.2.6	8.8.8.8	0xf992	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:30.856758118 CET	192.168.2.6	8.8.8.8	0xa178	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:32.198609114 CET	192.168.2.6	8.8.8.8	0x7019	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:33.567120075 CET	192.168.2.6	8.8.8.8	0xa690	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:34.927153111 CET	192.168.2.6	8.8.8.8	0xf1b9	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:36.342387915 CET	192.168.2.6	8.8.8.8	0x69a	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:37.706017017 CET	192.168.2.6	8.8.8.8	0x11da	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:39.064377069 CET	192.168.2.6	8.8.8.8	0xeaa5	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:40.407258034 CET	192.168.2.6	8.8.8.8	0x65a3	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:41.762677908 CET	192.168.2.6	8.8.8.8	0xf859	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:43.145524979 CET	192.168.2.6	8.8.8.8	0xea50	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:44.451947927 CET	192.168.2.6	8.8.8.8	0x70ab	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:45.776679039 CET	192.168.2.6	8.8.8.8	0x6010	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:09:47.092387915 CET	192.168.2.6	8.8.8.8	0x1c90	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:48.404412031 CET	192.168.2.6	8.8.8.8	0x1b03	Standard query (0)	martinboss .ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:07:45.266907930 CET	8.8.8.8	192.168.2.6	0xd9b2	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:46.827474117 CET	8.8.8.8	192.168.2.6	0x4cfc	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:48.491969109 CET	8.8.8.8	192.168.2.6	0x7b0b	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:50.028769016 CET	8.8.8.8	192.168.2.6	0x2dc4	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:51.431777954 CET	8.8.8.8	192.168.2.6	0x4881	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:52.838727951 CET	8.8.8.8	192.168.2.6	0x1d0e	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:54.205889940 CET	8.8.8.8	192.168.2.6	0x44f3	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:55.571289062 CET	8.8.8.8	192.168.2.6	0x5e4c	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:57.111020088 CET	8.8.8.8	192.168.2.6	0xb8bd	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:07:58.667474031 CET	8.8.8.8	192.168.2.6	0xda71	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:00.120590925 CET	8.8.8.8	192.168.2.6	0x1e15	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:01.480880976 CET	8.8.8.8	192.168.2.6	0x6514	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:02.825578928 CET	8.8.8.8	192.168.2.6	0x7f53	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:04.152319908 CET	8.8.8.8	192.168.2.6	0xa722	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:05.499820948 CET	8.8.8.8	192.168.2.6	0x3ff4	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:06.858426094 CET	8.8.8.8	192.168.2.6	0x30ca	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:08.202327967 CET	8.8.8.8	192.168.2.6	0x337b	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:09.530750990 CET	8.8.8.8	192.168.2.6	0x982e	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:10.987613916 CET	8.8.8.8	192.168.2.6	0xc475	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:12.376049042 CET	8.8.8.8	192.168.2.6	0xcbf7	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:14.188676119 CET	8.8.8.8	192.168.2.6	0xe579	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:15.780385971 CET	8.8.8.8	192.168.2.6	0x4ad8	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:17.316565990 CET	8.8.8.8	192.168.2.6	0xdd90	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:08:18.696165085 CET	8.8.8.8	192.168.2.6	0x9949	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:20.020870924 CET	8.8.8.8	192.168.2.6	0x4fb6	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:21.412421942 CET	8.8.8.8	192.168.2.6	0xe93	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:22.767571926 CET	8.8.8.8	192.168.2.6	0x419a	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:24.118077993 CET	8.8.8.8	192.168.2.6	0xdb1a	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:25.454222918 CET	8.8.8.8	192.168.2.6	0xe2f3	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:26.781805992 CET	8.8.8.8	192.168.2.6	0x578e	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:28.298862934 CET	8.8.8.8	192.168.2.6	0x9933	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:29.816936970 CET	8.8.8.8	192.168.2.6	0xb6c4	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:31.365034103 CET	8.8.8.8	192.168.2.6	0xb961	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:33.546222925 CET	8.8.8.8	192.168.2.6	0x49df	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:35.001399040 CET	8.8.8.8	192.168.2.6	0xf99a	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:36.570158005 CET	8.8.8.8	192.168.2.6	0x6d0b	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:38.095921993 CET	8.8.8.8	192.168.2.6	0x6c72	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:39.687787056 CET	8.8.8.8	192.168.2.6	0x2355	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:41.122194052 CET	8.8.8.8	192.168.2.6	0xfb39	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:42.761286020 CET	8.8.8.8	192.168.2.6	0xf8e6	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:44.328437090 CET	8.8.8.8	192.168.2.6	0x4b22	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:45.741550922 CET	8.8.8.8	192.168.2.6	0xf653	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:47.088871002 CET	8.8.8.8	192.168.2.6	0xc499	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:48.471918106 CET	8.8.8.8	192.168.2.6	0x70af	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:49.829307079 CET	8.8.8.8	192.168.2.6	0x5a34	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:51.200211048 CET	8.8.8.8	192.168.2.6	0xb366	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:52.559010029 CET	8.8.8.8	192.168.2.6	0x81af	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:53.929353952 CET	8.8.8.8	192.168.2.6	0x712b	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:55.287211895 CET	8.8.8.8	192.168.2.6	0x38c9	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)

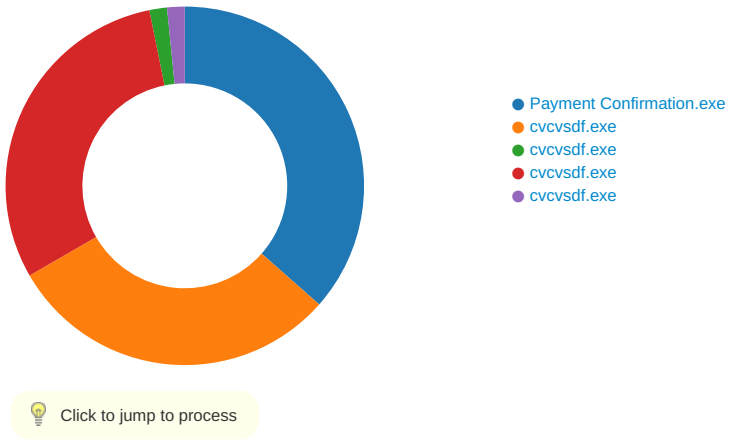
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:08:56.655138016 CET	8.8.8.8	192.168.2.6	0x622d	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:57.995523930 CET	8.8.8.8	192.168.2.6	0xb17e	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:08:59.348825932 CET	8.8.8.8	192.168.2.6	0x3e14	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:00.699660063 CET	8.8.8.8	192.168.2.6	0x6718	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:02.060837984 CET	8.8.8.8	192.168.2.6	0x967b	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:03.421380997 CET	8.8.8.8	192.168.2.6	0xc85c	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:04.770749092 CET	8.8.8.8	192.168.2.6	0xbc83	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:06.107952118 CET	8.8.8.8	192.168.2.6	0xa3bf	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:07.491424084 CET	8.8.8.8	192.168.2.6	0xf7c8	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:14.274820089 CET	8.8.8.8	192.168.2.6	0xd9b8	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:15.646821022 CET	8.8.8.8	192.168.2.6	0x1a8d	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:17.040496111 CET	8.8.8.8	192.168.2.6	0x92d1	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:18.422797918 CET	8.8.8.8	192.168.2.6	0xeef5	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:19.907733917 CET	8.8.8.8	192.168.2.6	0x3ba0	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:21.270256996 CET	8.8.8.8	192.168.2.6	0xf3d8	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:22.674866915 CET	8.8.8.8	192.168.2.6	0x91	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:24.088788033 CET	8.8.8.8	192.168.2.6	0x80fe	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:25.453197002 CET	8.8.8.8	192.168.2.6	0x5d60	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:26.810834885 CET	8.8.8.8	192.168.2.6	0x34fe	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:28.206527948 CET	8.8.8.8	192.168.2.6	0x6d93	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:29.562889099 CET	8.8.8.8	192.168.2.6	0xf992	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:30.915587902 CET	8.8.8.8	192.168.2.6	0xa178	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:32.256922007 CET	8.8.8.8	192.168.2.6	0x7019	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:33.624037027 CET	8.8.8.8	192.168.2.6	0xa690	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:34.986808062 CET	8.8.8.8	192.168.2.6	0xf1b9	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:36.401557922 CET	8.8.8.8	192.168.2.6	0x69a	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:09:37.760108948 CET	8.8.8.8	192.168.2.6	0x11da	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:39.123634100 CET	8.8.8.8	192.168.2.6	0xeaa5	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:40.464591026 CET	8.8.8.8	192.168.2.6	0x65a3	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:41.819736004 CET	8.8.8.8	192.168.2.6	0xf859	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:43.194669008 CET	8.8.8.8	192.168.2.6	0xea50	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:44.511965990 CET	8.8.8.8	192.168.2.6	0x70ab	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:45.826669931 CET	8.8.8.8	192.168.2.6	0x6010	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:47.149457932 CET	8.8.8.8	192.168.2.6	0x1c90	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)
Feb 23, 2021 08:09:48.462491989 CET	8.8.8.8	192.168.2.6	0x1b03	No error (0)	martinboss .ddns.net		79.134.225.30	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Payment Confirmation.exe PID: 7012 Parent PID: 5880

General

Start time:	08:07:38
Start date:	23/02/2021

Path:	C:\Users\user\Desktop\Payment Confirmation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment Confirmation.exe'
Imagebase:	0x400000
File size:	909312 bytes
MD5 hash:	800B9D7F3A47C5A18DA78CB6A54F90BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe	unknown	65024	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 bd 95 ee 82 f9 f4 80 d1 f9 f4 80 d1 f9 f4 80 d1 7a e8 8e d1 f8 f4 80 d1 90 eb 89 d1 f2 f4 80 d1 10 eb 8d d1 f8 f4 80 d1 52 69 63 68 f9 f4 80 d1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 59 df d9 5f 00 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 90 03 00 00 40 0a 00 00 00 00 00 58 2c 00 00 00 10 00 00 00 a0 03 00 00 00 40	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......................z..... ....Rich........ ...................PE..L...Y. ._....................@...... X,............@	success or wait	14	660ED8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\Public\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\Public\Desktop\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	660D92AC	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	660D92AC	unknown
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	660D92AC	unknown
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	660D92AC	unknown
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	660D92AC	unknown
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	660D92AC	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini	unknown	742	success or wait	1	660D92AC	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Windows\Fonts\desktop.ini	unknown	67	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini	unknown	696	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini	unknown	266	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\user\Favorites\desktop.ini	unknown	404	success or wait	1	660D92AC	unknown
C:\Users\user\Desktop\Payment Confirmation.exe	unknown	65024	success or wait	14	660ED50F	ReadFile
C:\Users\user\Desktop\Payment Confirmation.exe	unknown	65024	end of file	1	660ED50F	ReadFile

Analysis Process: cvcvsdf.exe PID: 7064 Parent PID: 7012

General

Start time:	08:07:40
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe
Imagebase:	0x400000
File size:	909312 bytes
MD5 hash:	800B9D7F3A47C5A18DA78CB6A54F90BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 48%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	660D92AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\Public\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\Public\Desktop\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	660D92AC	unknown
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	660D92AC	unknown
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	660D92AC	unknown
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	660D92AC	unknown
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	660D92AC	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	660D92AC	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini	unknown	742	success or wait	1	660D92AC	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Windows\Fonts\desktop.ini	unknown	67	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini	unknown	696	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini	unknown	266	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\user\Favorites\desktop.ini	unknown	404	success or wait	1	660D92AC	unknown

Analysis Process: cvcvsdf.exe PID: 7148 Parent PID: 7064

General

Start time:	08:07:42
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcv sdf.exe
Imagebase:	0x400000
File size:	909312 bytes
MD5 hash:	800B9D7F3A47C5A18DA78CB6A54F90BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Malware_QA_update, Description: VT Research QA uploaded malware - file update.exe, Source: 00000003.00000002.590959377.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: RAT_DarkComet, Description: Detects DarkComet RAT, Source: 00000003.00000002.590959377.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DarkCometRat, Description: Yara detected DarkComet, Source: 00000003.00000002.590959377.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000003.00000002.590959377.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: DarkComet_1, Description: DarkComet RAT, Source: 00000003.00000002.590959377.0000000000400000.00000040.00000001.sdmp, Author: botherder https://github.com/botherder • Rule: DarkComet_3, Description: unknown, Source: 00000003.00000002.590959377.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: DarkComet_2, Description: DarkComet, Source: 00000003.00000002.592032143.000000000238A000.00000004.00000001.sdmp, Author: Jean-Philippe Teissier / @Jipe_
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\DC3_FEXEC	success or wait	1	4211BC	RegCreateKeyExA

Analysis Process: cvcvsdf.exe PID: 6340 Parent PID: 3440

General

Start time:	08:07:52
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe'
Imagebase:	0x400000
File size:	909312 bytes
MD5 hash:	800B9D7F3A47C5A18DA78CB6A54F90BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	660D92AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\Public\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\Public\Desktop\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\user\Desktop\desktop.ini	unknown	284	success or wait	1	660D92AC	unknown
C:\Users\user\Documents\desktop.ini	unknown	404	success or wait	1	660D92AC	unknown
C:\Users\user\Music\desktop.ini	unknown	506	success or wait	1	660D92AC	unknown
C:\Users\user\Pictures\desktop.ini	unknown	506	success or wait	1	660D92AC	unknown
C:\Users\user\Videos\desktop.ini	unknown	506	success or wait	1	660D92AC	unknown
C:\Users\user\Downloads\desktop.ini	unknown	284	success or wait	1	660D92AC	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini	unknown	742	success or wait	1	660D92AC	unknown
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Windows\Fonts\desktop.ini	unknown	67	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini	unknown	696	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini	unknown	266	success or wait	1	660D92AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini	unknown	176	success or wait	1	660D92AC	unknown
C:\Users\user\Favorites\desktop.ini	unknown	404	success or wait	1	660D92AC	unknown

Analysis Process: cvcvsdf.exe PID: 4820 Parent PID: 6340

General

Start time:	08:07:56
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcvsdf.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cvcv sdf.exe
Imagebase:	0x400000
File size:	909312 bytes
MD5 hash:	800B9D7F3A47C5A18DA78CB6A54F90BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: DarkComet_2, Description: DarkComet, Source: 00000008.00000003.365577575.00000000023BA000.00000004.00000001.sdmp, Author: Jean-Philippe Teissier / @Jipe_ • Rule: Malware_QA_update, Description: VT Research QA uploaded malware - file update.exe, Source: 00000008.00000002.365956885.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: RAT_DarkComet, Description: Detects DarkComet RAT, Source: 00000008.00000002.365956885.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DarkCometRat, Description: Yara detected DarkComet, Source: 00000008.00000002.365956885.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000008.00000002.365956885.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: DarkComet_1, Description: DarkComet RAT, Source: 00000008.00000002.365956885.0000000000400000.00000040.00000001.sdmp, Author: botherder https://github.com/botherder • Rule: DarkComet_3, Description: unknown, Source: 00000008.00000002.365956885.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\DC3_FEXEC	2/23/2021 at 8:07:57 AM	unicode	{e6e9dfa8-98f2-11e9-90ce-806e6f6e6963-}	success or wait	1	421AF7	RegSetValueExA

Disassembly

Code Analysis