ID: 778236
Cookbook: browseurl.jbs
Time: 09:07:56
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

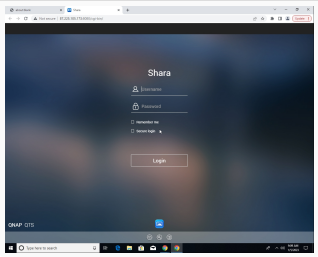
Windows Analysis Report

http://87.225.105.173

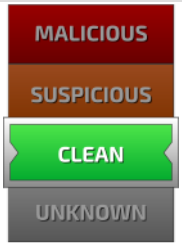
Overview

General Information

Sample URL:	http://87.225.105.173
Analysis ID:	778236
Infos:	



Detection

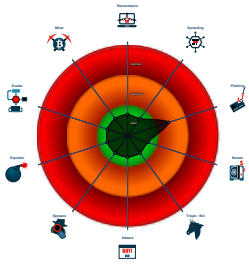


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- HTML body contains low number of …
- None HTTPS page querying sensitiv…
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4276 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4860 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1956 --field-trial-handle=1776,i,3735756616294617513,11813154491766648 81,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6180 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://87.225.105.173 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

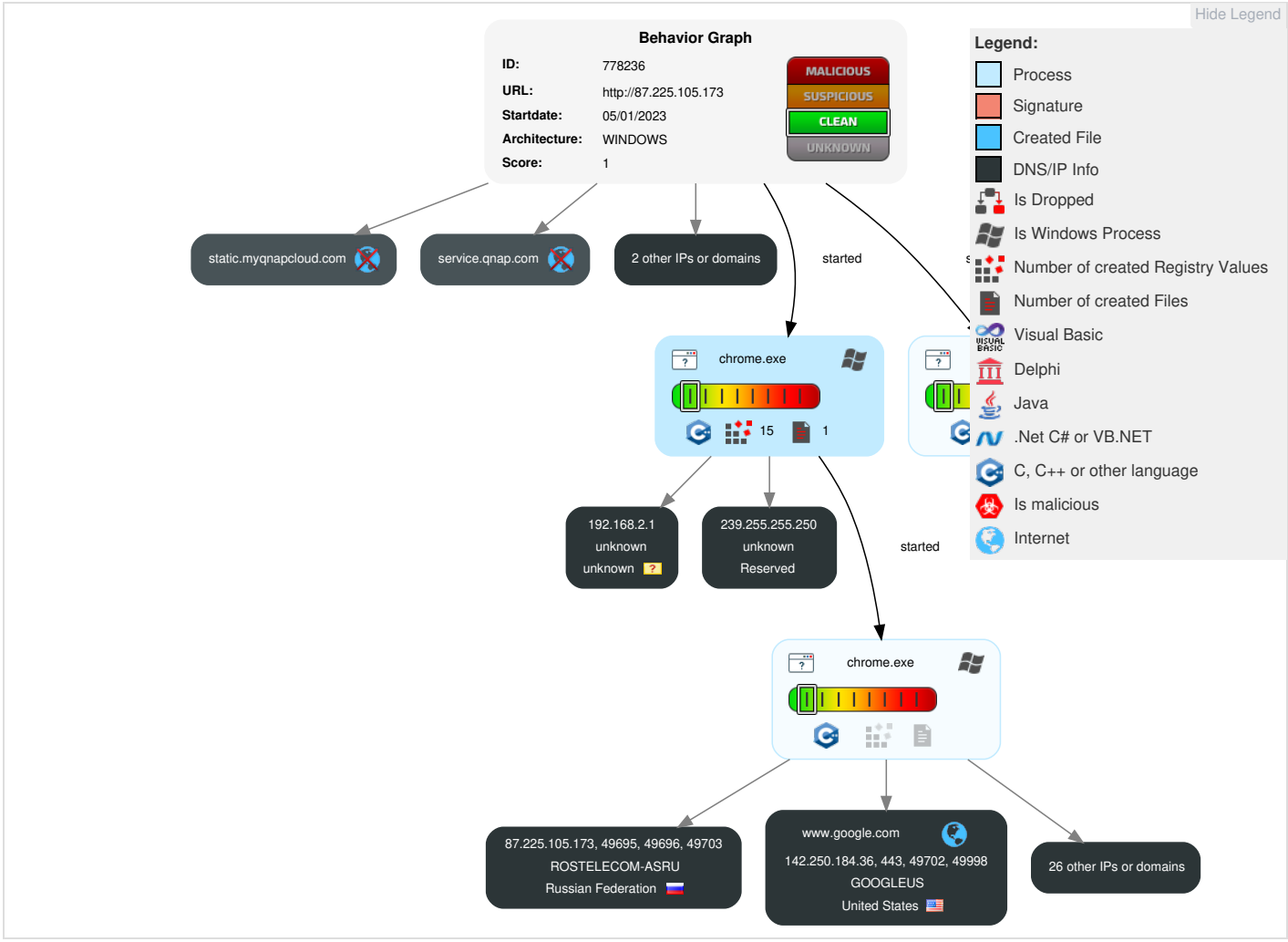
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	5 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

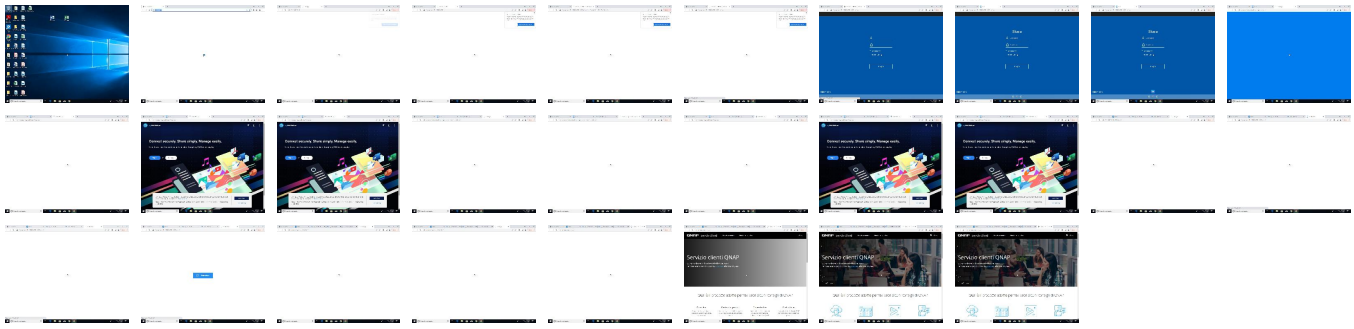
Behavior Graph

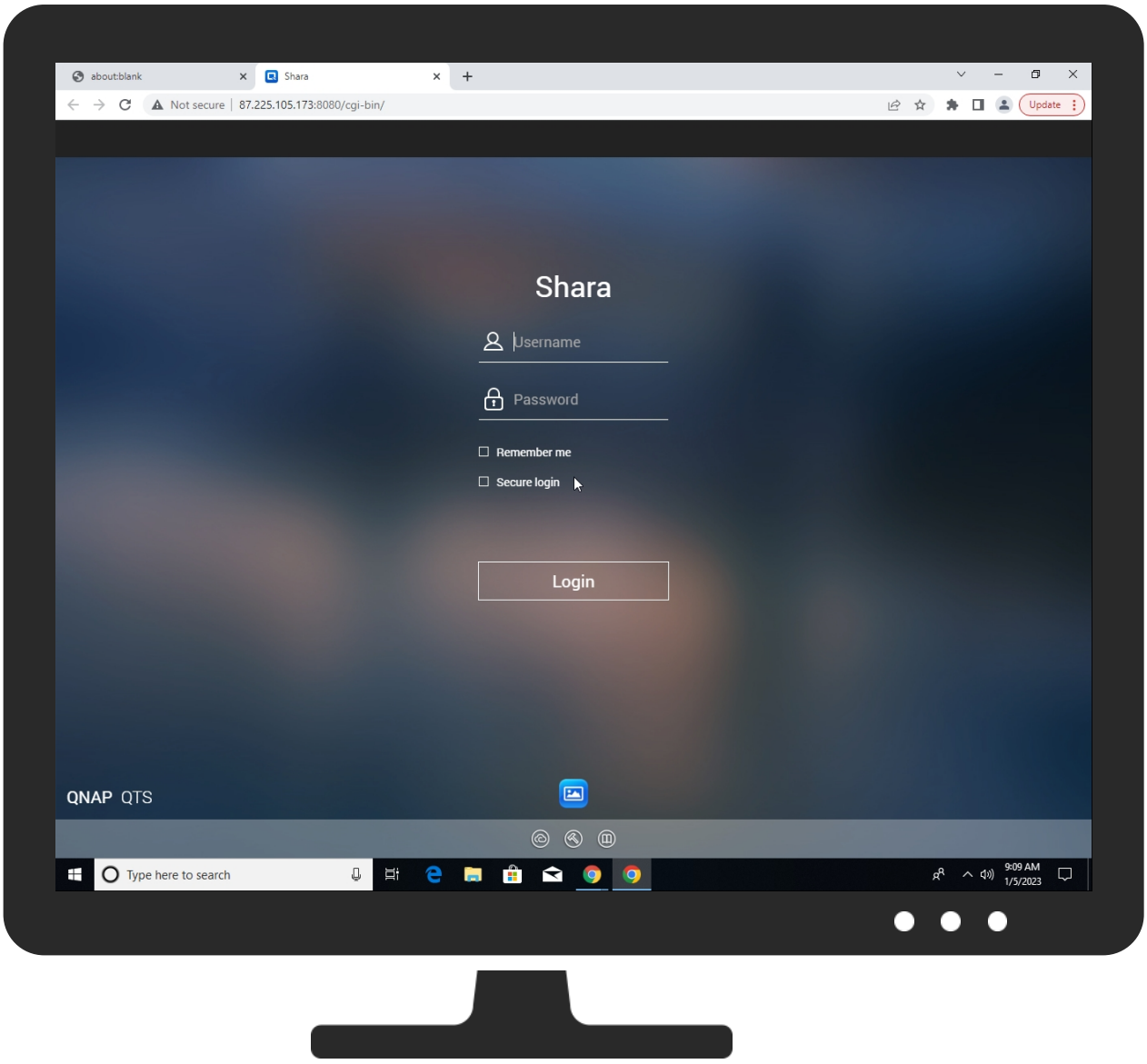


Screenshots

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
http://87.225.105.173	2%	Virustotal		Browse
http://87.225.105.173	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://87.225.105.173:8080/photo/lib/simple.css?5.4.4.20170912	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/photo/lang/ENG.js?5.4.4.20170912	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://static.myqnapcloud.com/portal/static/v3/js/OverlayScrollbars.min.js	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/js/903955a6.app-home.min.js	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/myqnapcloud-logo.svg	0%	Avira URL Cloud	safe	
http://https://www.myqnapcloud.com/static/app/0dd0612a.ga.js	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/v3_menu/fonts/Roboto/Roboto-Light.ttf	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/myqnapcloud-logo-cn.svg	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/photo/redirect.php	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/img/util/notify-warning.jpg?v=3.0.2.1050	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/cloud_app/icon/organization-center.png	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/logo_twitter_white.svg	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/js/05cce69d.lib-core.min.js	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/css/cookie-settings.css	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/header/ic-util-service-light.svg	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/photo/gallery/assets/images/4-1.Loading_slice.png?5.4.4.20170912	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/cloud_app/icon/service-afobot.png	0%	Avira URL Cloud	safe	
http://https://www.myqnapcloud.com/conf?v=3.0.2.1050	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/logo_youku.svg	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/js/angular-ga.js	0%	Avira URL Cloud	safe	
http://https://support.myqnapcloud.com/news/feeds/rss?lang=en	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/ic-pagination-next.svg	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/logo_sina_weibo.svg	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/js/qc-overlayScrollbars.js	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/css/utils.css	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/cgi-bin/language.cgi?1601949765	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/v3_menu/pic/photo.png?5.4.4.20170912	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/img/util/avatar-default.jpg?v=3.0.2.1050	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/cgi-bin/sysinfoReq.cgi?qpkg=1	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/css/fonts.css	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/css/landing.css	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/cloud_app/icon/service-service-portal.png	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/cloud_app/icon/software-store.png	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/cgi-bin/images/cmp/checkbox_radio/sprite.png?1601949765	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/cloud_app/icon/qmiix.png	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/cgi-bin/language.cgi?undefined=1601949765	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/logo_youtube_white.svg	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/illustration/illustration-landing-isometric-full.png	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/redirect.html?count=0.35395979719422654	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/cgi-bin/js/qos-core-login.js?1601949765	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/photo/p/api/utility.php?a=getSettings&_dc=1672906214184&json=1	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/header/ic-util-more-light.svg	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/RSS/images/PhotoStation.gif?5.4.4	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/v3_menu/css/qts-font.css?_dc=1601949765	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/v3_menu/pic/photo.ico?5.4.4.20170912	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/cloud_app/icon/service-license-manager.png	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/cgi-bin/loginTheme/theme1/login-max-height-768.css?r=wall&1601949765	0%	Avira URL Cloud	safe	
http://https://www.myqnapcloud.com/partials/alert	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/fonts/roboto/roboto-v20-latin-regular.woff2	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/cgi-bin/mediaGet.cgi?f=standard_bg&r=9604453	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/css/frame.css	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/v3_menu/pic/photo.png	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/css/common-page.css	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/photo/images/common/loading.png	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/v3_menu/css/qts-font.css?5.4.4.20170912	0%	Avira URL Cloud	safe	
http://https://www.myqnapcloud.com/%7B%7B%20info.send_user_avatar%20%7D%7D	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/css/OverlayScrollbars.min.css	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/china_jin_icon.png	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/photo/javascript/gallery-5.4.4.20170912.js	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/cgi-bin/mediaGet.cgi?f=standard_logo&r=9604453	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://static.myqnapcloud.com/cloud_app/icon/amiz-cloud.png	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/cgi-bin/jc.cgi?_dc=1601949765&t=js&f=jquery-1.10.2.min.js	0%	Avira URL Cloud	safe	
http://87.225.105.173:8080/cgi-bin/loginTheme/theme1/login.js?1601949765	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/js/a0218c7c.lib-basic.min.js	0%	Avira URL Cloud	safe	
http://https://static.myqnapcloud.com/portal/static/v3/img/common/common-page-background.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wiki.qnap.com	113.196.188.102	true	false		high
accounts.google.com	142.251.209.13	true	false		high
plus.l.google.com	142.251.209.46	true	false		high
d2owpi6pesstcp.cloudfront.net	13.224.92.62	true	false		high
dm3svrx1h6ahx.cloudfront.net	13.224.103.70	true	false		high
vars.hotjar.com	13.224.103.105	true	false		high
qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com	3.224.130.8	true	false		high
script.hotjar.com	13.224.103.124	true	false		high
forum.qnap.com	113.196.74.119	true	false		high
d14bb9kjiikrqu.cloudfront.net	13.224.103.40	true	false		high
www.google.com	142.250.184.36	true	false		high
clients.l.google.com	142.250.184.78	true	false		high
pro-customerportal-elb-132101016.us-west-2.elb.amazonaws.com	44.239.5.172	true	false		high
event.qnap.com	44.231.109.77	true	false		high
static-cdn.hotjar.com	13.224.103.58	true	false		high
support.myqnapcloud.com	unknown	unknown	false		unknown
static.myqnapcloud.com	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
service.qnap.com	unknown	unknown	false		high
www.myqnapcloud.com	unknown	unknown	false		unknown
static.hotjar.com	unknown	unknown	false		high
account.qnap.com	unknown	unknown	false		high
www.qnap.com	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high

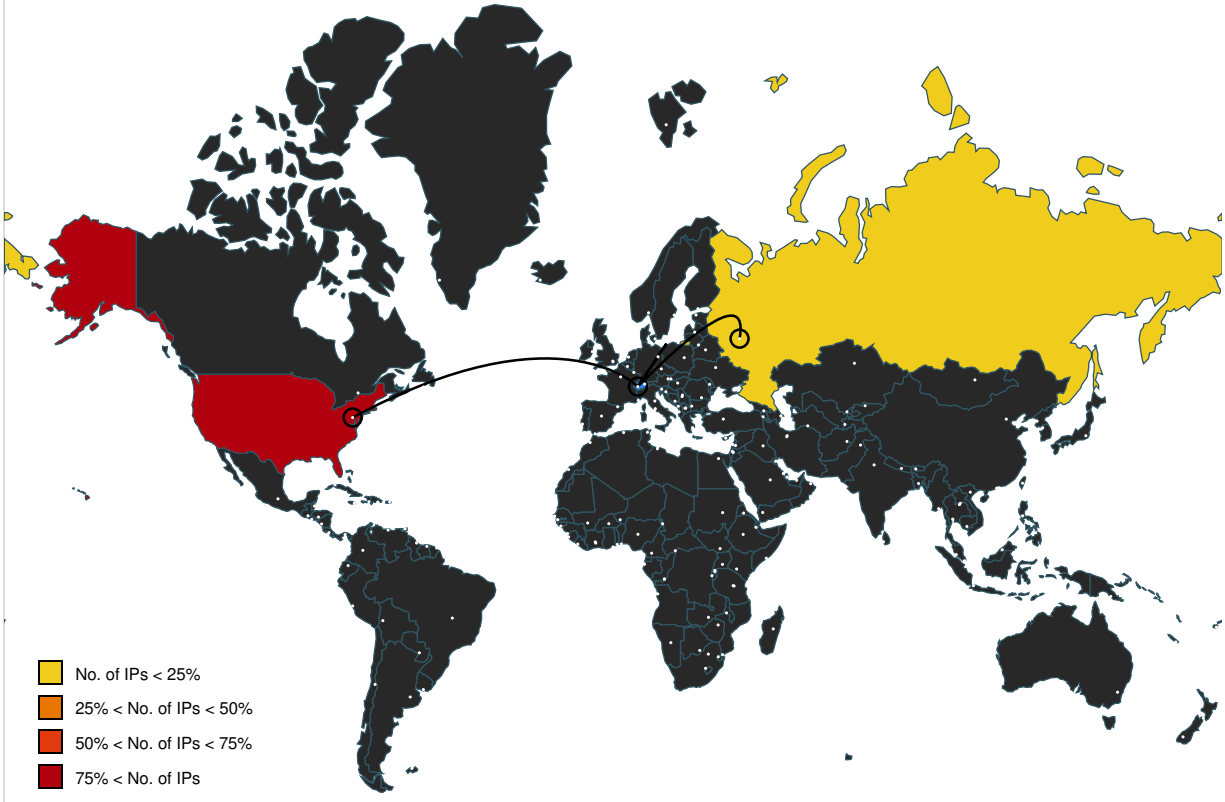
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://static.myqnapcloud.com/portal/static/js/903955a6.app-home.min.js	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/js/OverlayScrollbars.min.js	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/photo/lib/simple.css?5.4.4.20170912	false	• Avira URL Cloud: safe	unknown
http://https://vars.hotjar.com/box-5e66f98b4ee957db209dc6f63e3d59dd.html	false		high
http://https://apis.google.com/js/client.js	false		high
http://https://static.hotjar.com/c/hotjar-1642270.js?sv=6	false		high
http://https://service.qnap.com/js/clipboard.min.js	false		high
http://87.225.105.173:8080/photo/	false		unknown
http://https://www.qnap.com/en-uk/support-ticket/	false		high
http://www.qnap.com/_jump/web/myqnapcloud.php?	false		high
http://https://service.qnap.com/images/home/icon_13.png	false		high
http://87.225.105.173:8080/photo/lang/ENG.js?5.4.4.20170912	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/myqnapcloud-logo.svg	false	• Avira URL Cloud: safe	unknown
http://https://www.myqnapcloud.com/static/app/0dd0612a.ga.js	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/images/home/icon_05.png	false		high
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/myqnapcloud-logo-cn.svg	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/images/icon-03.png	false		high

Name	Malicious	Antivirus Detection	Reputation
http://87.225.105.173:8080/v3_menu/fonts/Roboto/Roboto-Light.ttf	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/photo/redirect.php	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/img/util/notify-warning.jpg?v=3.0.2.1050	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/cloud_app/icon/organization-center.png	false	• Avira URL Cloud: safe	unknown
http://https://www.qnap.com/favicon.ico	false		high
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/logo_twitter_white.svg	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/js/05cce69d.lib-core.min.js	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/css/cookie-settings.css	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/img/header/ic-util-service-light.svg	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/css/bootstrap.min.css	false		high
http://87.225.105.173:8080/photo/gallery/assets/images/4-1.Loading_slice.png?5.4.4.20170912	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/cloud_app/icon/service-afobot.png	false	• Avira URL Cloud: safe	unknown
http://https://www.myqnapcloud.com/conf?v=3.0.2.1050	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/images/home/icon_07.png	false		high
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/logo_youku.svg	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/images/home/icon_11.png	false		high
http://https://service.qnap.com/it-it	false		high
http://https://static.myqnapcloud.com/portal/static/js/angular-ga.js	false	• Avira URL Cloud: safe	unknown
http://https://support.myqnapcloud.com/news/feeds/rss?lang=en	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/photo/	false		unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/ic-pagination-next.svg	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/logo_sina_weibo.svg	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/js/qc-overlayScrollbars.js	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/css/utils.css	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/cgi-bin/language.cgi?1601949765	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/v3_menu/pic/photo.png?5.4.4.20170912	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/img/util/avatar-default.jpg?v=3.0.2.1050	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/cgi-bin/sysinfoReq.cgi?qpkg=1	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/css/fonts.css	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/css/landing.css	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/cloud_app/icon/service-service-portal.png	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/cloud_app/icon/software-store.png	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/cgi-bin/images/cmp/checkbox_radio/sprite.png?1601949765	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/images/favicon/favicon.png	false		high
http://https://static.myqnapcloud.com/cloud_app/icon/qmiix.png	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/cgi-bin/language.cgi?undefined=1601949765	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/logo_youtube_white.svg	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/img/illustration/illustration-landing-isometric-full.png	false	• Avira URL Cloud: safe	unknown
http://https://www.qnap.com/_jump/web/myqnapcloud.php?lang=undefined	false		high
http://87.225.105.173:8080/redirect.html?count=0.35395979719422654	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/cgi-bin/js/qos-core-login.js?1601949765	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/photo/p/api/utility.php?a=getSettings&_dc=1672906214184&json=1	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/img/header/ic-util-more-light.svg	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/RSS/images/PhotoStation.gif?5.4.4	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/v3_menu/css/qts-font.css?_dc=1601949765	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/v3_menu/pic/photo.ico?5.4.4.20170912	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/cloud_app/icon/service-license-manager.png	false	• Avira URL Cloud: safe	unknown
http://https://www.qnap.com/_jump/web/myqnapcloud.php?	false		high
http://87.225.105.173:8080/cgi-bin/loginTheme/theme1/login-max-height-768.css?r=wall&1601949765	false	• Avira URL Cloud: safe	unknown
http://https://www.myqnapcloud.com/partials/alert	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/css/salesforce-lightning-design-system.min.css	false		high
http://https://service.qnap.com/images/home/kv-bg.jpg	false		high
http://https://static.myqnapcloud.com/portal/static/v3/fonts/roboto/roboto-v20-latin-regular.woff2	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://service.qnap.com/js/customer_portal.js	false		high
http://87.225.105.173:8080/cgi-bin/mediaGet.cgi?f=standard_bg&r=9604453	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/css/frame.css	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/images/home/icon_03.png	false		high
http://87.225.105.173:8080/v3_menu/pic/photo.png	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/css/common-page.css	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/photo/images/common/loading.png	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/v3_menu/css/qts-font.css?5.4.4.20170912	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/photo/gallery/	false		unknown
http://https://www.myqnapcloud.com/%7B%7B%20info.send_user_avatar%20%7D%7D	false	• Avira URL Cloud: safe	unknown
http://https://vars.hotjar.com/box-5e66f98b4ee957db209dc6f63e3d59dd.html	false		high
http://https://static.myqnapcloud.com/portal/static/v3/css/OverlayScrollbars.min.css	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/images/home/icon_04.png	false		high
http://https://static.myqnapcloud.com/portal/static/v3/img/utils/china_jin_icon.png	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/js/app.js	false		high
http://87.225.105.173:8080/photo/javascript/gallery-5.4.4.20170912.js	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/cgi-bin/mediaGet.cgi?f=standard_logo&r=9604453	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/cloud_app/icon/amiz-cloud.png	false	• Avira URL Cloud: safe	unknown
http://87.225.105.173:8080/photo/gallery/	false		unknown
http://https://www.myqnapcloud.com/?lang=en	false		unknown
http://https://service.qnap.com/images/home/icon_14.png	false		high
http://https://event.qnap.com/mtc.js	false		high
http://87.225.105.173:8080/cgi-bin/jc.cgi?_dc=1601949765&t=js&f=jquery-1.10.2.min.js	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/images/home/icon_06.png	false		high
http://87.225.105.173:8080/cgi-bin/loginTheme/theme1/login.js?1601949765	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/js/a0218c7c.lib-basic.min.js	false	• Avira URL Cloud: safe	unknown
http://https://static.myqnapcloud.com/portal/static/v3/img/common/common-page-background.png	false	• Avira URL Cloud: safe	unknown
http://https://service.qnap.com/it-it	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.103.105	vars.hotjar.com	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.224.130.8	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
13.224.103.124	script.hotjar.com	United States		16509	AMAZON-02US	false
13.224.103.40	d14bb9kjiikrqu.cloudfront.net	United States		16509	AMAZON-02US	false
142.251.209.13	accounts.google.com	United States		15169	GOOGLEUS	false
13.224.103.58	static-cdn.hotjar.com	United States		16509	AMAZON-02US	false
87.225.105.173	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
142.250.184.78	clients.l.google.com	United States		15169	GOOGLEUS	false
13.224.103.70	dm3svrx1h6ahx.cloudfront.net	United States		16509	AMAZON-02US	false
142.250.184.36	www.google.com	United States		15169	GOOGLEUS	false
13.224.92.45	unknown	United States		16509	AMAZON-02US	false
142.251.209.46	plus.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
44.239.5.172	pro-customerportal-elb-132101016.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
44.231.109.77	event.qnap.com	United States		16509	AMAZON-02US	false
18.208.44.198	unknown	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	778236
Start date and time:	2023-01-05 09:07:56 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://87.225.105.173
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
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:	CLEAN
Classification:	clean1.win@34/0@25/18
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Browse: http://www.qnap.com/_jump/web/myqnapcloud.php? • Browse: http://www.qnap.com/_jump/web/myqnapcloud.php?lang=undefined • Browse: http://87.225.105.173:8080/photo/ • Browse: https://www.qnap.com/go/support-ticket/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.35, 34.104.35.123, 142.250.184.106, 142.250.180.138, 142.250.180.170, 142.251.209.10, 142.251.209.42, 216.58.209.42, 142.250.184.42, 142.250.184.74, 142.251.209.3, 142.250.184.99, 142.250.184.67
- Excluded domains from analysis (whitelisted): fonts.googleapis.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, fonts.gstatic.com, update.googleapis.com, clientservices.googleapis.com, www.gstatic.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

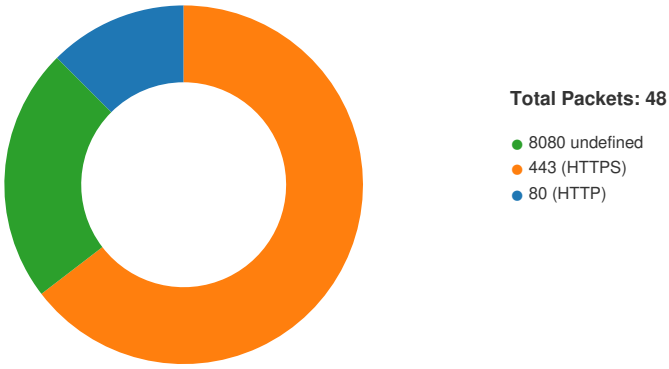
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:08:55.844831944 CET	49695	80	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:55.976603031 CET	49696	80	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:56.005932093 CET	80	49695	87.225.105.173	192.168.2.4
Jan 5, 2023 09:08:56.006129026 CET	49695	80	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:56.128829956 CET	80	49696	87.225.105.173	192.168.2.4
Jan 5, 2023 09:08:56.129069090 CET	49696	80	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:56.162837029 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.162899971 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.163001060 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.163341999 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.163372993 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.176162958 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.176218033 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.176307917 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.176609993 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.176645041 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.340123892 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.363017082 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.469656944 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.469719887 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.470074892 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.470113993 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.471051931 CET	49696	80	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:56.471508980 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.471544981 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.471620083 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.475985050 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.476011038 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.476092100 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.476129055 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.476166964 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.476196051 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.575637102 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.578726053 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.623076916 CET	80	49696	87.225.105.173	192.168.2.4
Jan 5, 2023 09:08:56.899527073 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.899610043 CET	443	49699	142.251.209.13	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:08:56.899887085 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.899904013 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.900003910 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.900166988 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.900207043 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.900335073 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.900350094 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.900620937 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.945561886 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.945765972 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.945841074 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.945893049 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.945964098 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.948832989 CET	49700	443	192.168.2.4	142.250.184.78
Jan 5, 2023 09:08:56.948869944 CET	443	49700	142.250.184.78	192.168.2.4
Jan 5, 2023 09:08:56.967508078 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.967632055 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.967658043 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.967840910 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:56.967935085 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.973089933 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 09:08:56.973128080 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 09:08:57.982703924 CET	49702	443	192.168.2.4	142.250.184.36
Jan 5, 2023 09:08:57.982779026 CET	443	49702	142.250.184.36	192.168.2.4
Jan 5, 2023 09:08:57.982928991 CET	49702	443	192.168.2.4	142.250.184.36
Jan 5, 2023 09:08:57.983242989 CET	49702	443	192.168.2.4	142.250.184.36
Jan 5, 2023 09:08:57.983278990 CET	443	49702	142.250.184.36	192.168.2.4
Jan 5, 2023 09:08:58.060019970 CET	443	49702	142.250.184.36	192.168.2.4
Jan 5, 2023 09:08:58.060403109 CET	49702	443	192.168.2.4	142.250.184.36
Jan 5, 2023 09:08:58.060461998 CET	443	49702	142.250.184.36	192.168.2.4
Jan 5, 2023 09:08:58.062094927 CET	443	49702	142.250.184.36	192.168.2.4
Jan 5, 2023 09:08:58.062221050 CET	49702	443	192.168.2.4	142.250.184.36
Jan 5, 2023 09:08:58.077941895 CET	49702	443	192.168.2.4	142.250.184.36
Jan 5, 2023 09:08:58.078002930 CET	443	49702	142.250.184.36	192.168.2.4
Jan 5, 2023 09:08:58.078180075 CET	443	49702	142.250.184.36	192.168.2.4
Jan 5, 2023 09:08:58.209742069 CET	49702	443	192.168.2.4	142.250.184.36
Jan 5, 2023 09:08:58.209798098 CET	443	49702	142.250.184.36	192.168.2.4
Jan 5, 2023 09:08:58.309724092 CET	49702	443	192.168.2.4	142.250.184.36
Jan 5, 2023 09:08:58.594156027 CET	80	49696	87.225.105.173	192.168.2.4
Jan 5, 2023 09:08:58.643877029 CET	49703	8080	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:58.662398100 CET	49704	8080	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:58.805654049 CET	8080	49703	87.225.105.173	192.168.2.4
Jan 5, 2023 09:08:58.805850983 CET	49703	8080	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:58.806787014 CET	49703	8080	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:58.810126066 CET	49696	80	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:58.812252045 CET	8080	49704	87.225.105.173	192.168.2.4
Jan 5, 2023 09:08:58.812482119 CET	49704	8080	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:58.968050957 CET	8080	49703	87.225.105.173	192.168.2.4
Jan 5, 2023 09:08:59.334126949 CET	8080	49703	87.225.105.173	192.168.2.4
Jan 5, 2023 09:08:59.415039062 CET	49703	8080	192.168.2.4	87.225.105.173
Jan 5, 2023 09:08:59.576759100 CET	8080	49703	87.225.105.173	192.168.2.4
Jan 5, 2023 09:09:00.197026968 CET	8080	49703	87.225.105.173	192.168.2.4
Jan 5, 2023 09:09:00.309860945 CET	49703	8080	192.168.2.4	87.225.105.173
Jan 5, 2023 09:09:00.431956053 CET	49703	8080	192.168.2.4	87.225.105.173
Jan 5, 2023 09:09:00.592835903 CET	8080	49703	87.225.105.173	192.168.2.4
Jan 5, 2023 09:09:01.605458975 CET	8080	49703	87.225.105.173	192.168.2.4
Jan 5, 2023 09:09:01.617294073 CET	49704	8080	192.168.2.4	87.225.105.173
Jan 5, 2023 09:09:01.710138083 CET	49703	8080	192.168.2.4	87.225.105.173
Jan 5, 2023 09:09:01.766778946 CET	8080	49704	87.225.105.173	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:09:01.919161081 CET	8080	49704	87.225.105.173	192.168.2.4
Jan 5, 2023 09:09:01.920541048 CET	8080	49704	87.225.105.173	192.168.2.4
Jan 5, 2023 09:09:01.920588970 CET	8080	49704	87.225.105.173	192.168.2.4
Jan 5, 2023 09:09:01.920645952 CET	49704	8080	192.168.2.4	87.225.105.173

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 5, 2023 09:08:55.703449011 CET	192.168.2.4	8.8.8.8	0x328e	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:08:55.705899000 CET	192.168.2.4	8.8.8.8	0x66a2	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:08:57.913631916 CET	192.168.2.4	8.8.8.8	0xd99	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:08:57.940279961 CET	192.168.2.4	8.8.8.8	0x38b0	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:04.203691006 CET	192.168.2.4	8.8.8.8	0xa1bc	Standard query (0)	wiki.qnap.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:04.204673052 CET	192.168.2.4	8.8.8.8	0x71cd	Standard query (0)	forum.qnap.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:04.208709955 CET	192.168.2.4	8.8.8.8	0xdac7	Standard query (0)	www.qnap.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:12.560970068 CET	192.168.2.4	8.8.8.8	0xe9a6	Standard query (0)	www.qnap.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:12.672840118 CET	192.168.2.4	8.8.8.8	0x3658	Standard query (0)	www.qnap.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:13.740993977 CET	192.168.2.4	8.8.8.8	0x4abf	Standard query (0)	www.myqnapcloud.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:14.558778048 CET	192.168.2.4	8.8.8.8	0xf407	Standard query (0)	static.myqnapcloud.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:14.563782930 CET	192.168.2.4	8.8.8.8	0x6ab0	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.090785027 CET	192.168.2.4	8.8.8.8	0x88e7	Standard query (0)	event.qnap.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.090872049 CET	192.168.2.4	8.8.8.8	0x9199	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.436649084 CET	192.168.2.4	8.8.8.8	0x2d16	Standard query (0)	account.qnap.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.712388039 CET	192.168.2.4	8.8.8.8	0xb5a6	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.939297915 CET	192.168.2.4	8.8.8.8	0x2fab	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:18.477092028 CET	192.168.2.4	8.8.8.8	0x826	Standard query (0)	support.myqnapcloud.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:27.617173910 CET	192.168.2.4	8.8.8.8	0xa187	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:27.617374897 CET	192.168.2.4	8.8.8.8	0x5c90	Standard query (0)	static.myqnapcloud.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:31.492747068 CET	192.168.2.4	8.8.8.8	0xbfe5	Standard query (0)	static.myqnapcloud.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:57.980515003 CET	192.168.2.4	8.8.8.8	0xa82b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:58.004089117 CET	192.168.2.4	8.8.8.8	0x1e65	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:58.702641010 CET	192.168.2.4	8.8.8.8	0x9b33	Standard query (0)	service.qnap.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:10:10.227299929 CET	192.168.2.4	8.8.8.8	0x4884	Standard query (0)	service.qnap.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:08:55.723131895 CET	8.8.8.8	192.168.2.4	0x328e	No error (0)	accounts.google.com		142.251.209.13	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:08:55.733294964 CET	8.8.8.8	192.168.2.4	0x66a2	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:08:55.733294964 CET	8.8.8.8	192.168.2.4	0x66a2	No error (0)	clients.l.google.com		142.250.184.78	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:08:57.932959080 CET	8.8.8.8	192.168.2.4	0xd99	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:08:57.979861021 CET	8.8.8.8	192.168.2.4	0x38b0	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:04.224313974 CET	8.8.8.8	192.168.2.4	0xa1bc	No error (0)	wiki.qnap.com		113.196.188.102	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:04.224833012 CET	8.8.8.8	192.168.2.4	0x71cd	No error (0)	forum.qnap.com		113.196.74.119	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:04.241789103 CET	8.8.8.8	192.168.2.4	0xdac7	No error (0)	www.qnap.com	d2owpi6pesstcp.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:04.241789103 CET	8.8.8.8	192.168.2.4	0xdac7	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.62	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:04.241789103 CET	8.8.8.8	192.168.2.4	0xdac7	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.65	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:04.241789103 CET	8.8.8.8	192.168.2.4	0xdac7	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.45	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:04.241789103 CET	8.8.8.8	192.168.2.4	0xdac7	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.56	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:12.599864960 CET	8.8.8.8	192.168.2.4	0xe9a6	No error (0)	www.qnap.com	d2owpi6pesstcp.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:12.599864960 CET	8.8.8.8	192.168.2.4	0xe9a6	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.45	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:12.599864960 CET	8.8.8.8	192.168.2.4	0xe9a6	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.62	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:12.599864960 CET	8.8.8.8	192.168.2.4	0xe9a6	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.65	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:12.599864960 CET	8.8.8.8	192.168.2.4	0xe9a6	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.56	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:12.694863081 CET	8.8.8.8	192.168.2.4	0x3658	No error (0)	www.qnap.com	d2owpi6pesstcp.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:12.694863081 CET	8.8.8.8	192.168.2.4	0x3658	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.45	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:12.694863081 CET	8.8.8.8	192.168.2.4	0x3658	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.56	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:12.694863081 CET	8.8.8.8	192.168.2.4	0x3658	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.65	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:12.694863081 CET	8.8.8.8	192.168.2.4	0x3658	No error (0)	d2owpi6pesstcp.cloudfront.net		13.224.92.62	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:13.759800911 CET	8.8.8.8	192.168.2.4	0x4abf	No error (0)	www.myqnapcloud.com	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:13.759800911 CET	8.8.8.8	192.168.2.4	0x4abf	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		3.224.130.8	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:09:13.759800911 CET	8.8.8.8	192.168.2.4	0x4abf	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		34.225.113.168	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:13.759800911 CET	8.8.8.8	192.168.2.4	0x4abf	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		54.163.54.251	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:13.759800911 CET	8.8.8.8	192.168.2.4	0x4abf	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		52.201.142.201	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:13.759800911 CET	8.8.8.8	192.168.2.4	0x4abf	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		52.201.182.103	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:13.759800911 CET	8.8.8.8	192.168.2.4	0x4abf	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		18.208.44.198	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:14.589310884 CET	8.8.8.8	192.168.2.4	0x6ab0	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:14.589310884 CET	8.8.8.8	192.168.2.4	0x6ab0	No error (0)	plus.l.google.com		142.251.209.46	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:14.601752996 CET	8.8.8.8	192.168.2.4	0xf407	No error (0)	static.myqnapcloud.com	dm3svrx1h6ahx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:14.601752996 CET	8.8.8.8	192.168.2.4	0xf407	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.70	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:14.601752996 CET	8.8.8.8	192.168.2.4	0xf407	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.81	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:14.601752996 CET	8.8.8.8	192.168.2.4	0xf407	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.86	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:14.601752996 CET	8.8.8.8	192.168.2.4	0xf407	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.32	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.111013889 CET	8.8.8.8	192.168.2.4	0x88e7	No error (0)	event.qnap.com		44.231.109.77	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.117186069 CET	8.8.8.8	192.168.2.4	0x9199	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:17.117186069 CET	8.8.8.8	192.168.2.4	0x9199	No error (0)	static-cdn.hotjar.com		13.224.103.58	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.117186069 CET	8.8.8.8	192.168.2.4	0x9199	No error (0)	static-cdn.hotjar.com		13.224.103.96	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.117186069 CET	8.8.8.8	192.168.2.4	0x9199	No error (0)	static-cdn.hotjar.com		13.224.103.43	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.117186069 CET	8.8.8.8	192.168.2.4	0x9199	No error (0)	static-cdn.hotjar.com		13.224.103.36	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.455991030 CET	8.8.8.8	192.168.2.4	0x2d16	No error (0)	account.qnap.com	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:09:17.455991030 CET	8.8.8.8	192.168.2.4	0x2d16	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		18.208.44.198	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.455991030 CET	8.8.8.8	192.168.2.4	0x2d16	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		3.224.130.8	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.455991030 CET	8.8.8.8	192.168.2.4	0x2d16	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		54.163.54.251	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.455991030 CET	8.8.8.8	192.168.2.4	0x2d16	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		52.201.142.201	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.455991030 CET	8.8.8.8	192.168.2.4	0x2d16	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		34.225.113.168	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.455991030 CET	8.8.8.8	192.168.2.4	0x2d16	No error (0)	qcloud-pr-frontend-1025300009.us-east-1.elb.amazonaws.com		52.201.182.103	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.734774113 CET	8.8.8.8	192.168.2.4	0xb5a6	No error (0)	script.hotjar.com		13.224.103.124	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.734774113 CET	8.8.8.8	192.168.2.4	0xb5a6	No error (0)	script.hotjar.com		13.224.103.115	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.734774113 CET	8.8.8.8	192.168.2.4	0xb5a6	No error (0)	script.hotjar.com		13.224.103.93	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.734774113 CET	8.8.8.8	192.168.2.4	0xb5a6	No error (0)	script.hotjar.com		13.224.103.23	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.979007959 CET	8.8.8.8	192.168.2.4	0x2fab	No error (0)	vars.hotjar.com		13.224.103.105	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.979007959 CET	8.8.8.8	192.168.2.4	0x2fab	No error (0)	vars.hotjar.com		13.224.103.129	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.979007959 CET	8.8.8.8	192.168.2.4	0x2fab	No error (0)	vars.hotjar.com		13.224.103.28	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:17.979007959 CET	8.8.8.8	192.168.2.4	0x2fab	No error (0)	vars.hotjar.com		13.224.103.38	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:18.738049984 CET	8.8.8.8	192.168.2.4	0x826	No error (0)	support.myqnapcloud.com	d14bb9kjiikrqu.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:18.738049984 CET	8.8.8.8	192.168.2.4	0x826	No error (0)	d14bb9kjiikrqu.cloudfront.net		13.224.103.40	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:18.738049984 CET	8.8.8.8	192.168.2.4	0x826	No error (0)	d14bb9kjiikrqu.cloudfront.net		13.224.103.69	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:18.738049984 CET	8.8.8.8	192.168.2.4	0x826	No error (0)	d14bb9kjiikrqu.cloudfront.net		13.224.103.39	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:18.738049984 CET	8.8.8.8	192.168.2.4	0x826	No error (0)	d14bb9kjiikrqu.cloudfront.net		13.224.103.52	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:27.639673948 CET	8.8.8.8	192.168.2.4	0x5c90	No error (0)	static.myqnapcloud.com	dm3svrx1h6ahx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false

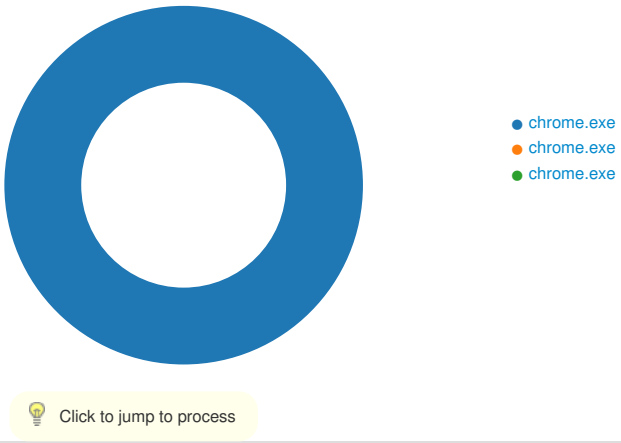
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:09:27.639673948 CET	8.8.8.8	192.168.2.4	0x5c90	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.32	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:27.639673948 CET	8.8.8.8	192.168.2.4	0x5c90	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.81	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:27.639673948 CET	8.8.8.8	192.168.2.4	0x5c90	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.86	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:27.639673948 CET	8.8.8.8	192.168.2.4	0x5c90	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.70	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:27.656929016 CET	8.8.8.8	192.168.2.4	0xa187	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:27.656929016 CET	8.8.8.8	192.168.2.4	0xa187	No error (0)	plus.l.google.com		142.251.209.46	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:31.510174990 CET	8.8.8.8	192.168.2.4	0xbfe5	No error (0)	static.myqnapcloud.com	dm3svrx1h6ahx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:31.510174990 CET	8.8.8.8	192.168.2.4	0xbfe5	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.70	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:31.510174990 CET	8.8.8.8	192.168.2.4	0xbfe5	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.81	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:31.510174990 CET	8.8.8.8	192.168.2.4	0xbfe5	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.86	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:31.510174990 CET	8.8.8.8	192.168.2.4	0xbfe5	No error (0)	dm3svrx1h6ahx.cloudfront.net		13.224.103.32	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:57.998359919 CET	8.8.8.8	192.168.2.4	0xa82b	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:58.021576881 CET	8.8.8.8	192.168.2.4	0x1e65	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:09:58.720273972 CET	8.8.8.8	192.168.2.4	0x9b33	No error (0)	service.qnap.com	pro-customerportal-elb-132101016.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:09:58.720273972 CET	8.8.8.8	192.168.2.4	0x9b33	No error (0)	pro-customerportal-elb-132101016.us-west-2.elb.amazonaws.com		44.239.5.172	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:10:10.248106003 CET	8.8.8.8	192.168.2.4	0x4884	No error (0)	service.qnap.com	pro-customerportal-elb-132101016.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:10:10.248106003 CET	8.8.8.8	192.168.2.4	0x4884	No error (0)	pro-customerportal-elb-132101016.us-west-2.elb.amazonaws.com		44.239.5.172	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- www.qnap.com
- https:
  - www.myqnapcloud.com
  - static.myqnapcloud.com
  - apis.google.com
  - static.hotjar.com
  - event.qnap.com
  - script.hotjar.com
  - vars.hotjar.com
  - account.qnap.com
  - support.myqnapcloud.com
  - service.qnap.com
- 87.225.105.173
  - 87.225.105.173:8080

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **4276**, Parent PID: **3312**

General

Target ID:	0
Start time:	09:08:51
Start date:	05/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true

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

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **4860**, Parent PID: **4276**

General

Target ID:	1
Start time:	09:08:52
Start date:	05/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1956 --field-trial-handle=1776,i,3735756616294617513,1181315449176664881,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6180**, Parent PID: **3312**

General

Target ID:	2
Start time:	09:08:53
Start date:	05/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://87.225.105.173
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true

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

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly