ID: 708252
Cookbook: browseurl.jbs
Time: 08:13:19
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

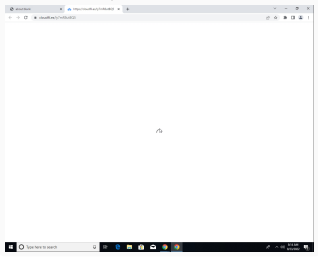
Windows Analysis Report

https://cloudfil.es/ly7mR8utBQ5

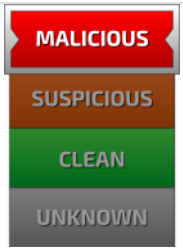
Overview

General Information

Sample URL:	http://https://cloudfil.es/ly7mR8utBQ5
Analysis ID:	708252
Infos:	



Detection



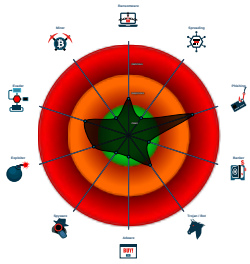
HTMLPhisher

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish44
- Found inlined nop instructions (likely…
- Found iframes
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- No HTML title found
- Detected potential crypto function
- HTTP GET or POST without a user …
- Creates a process in suspended mo…
- Contains long sleeps (>= 3 min)

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5928 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 1572 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1936 --field-trial-handle=1772,i,13935456055298204775,6851687727719502408,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - unarchiver.exe (PID: 2768 cmdline: C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip MD5: 9DE2E060A2985A232D8B96F9EC847A19)
    - 7za.exe (PID: 5912 cmdline: C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
      - conhost.exe (PID: 7004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - chrome.exe (PID: 3560 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=3636 --field-trial-handle=1772,i,13935456055298204775,6851687727719502408,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6268 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=6236 --field-trial-handle=1772,i,13935456055298204775,6851687727719502408,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - unarchiver.exe (PID: 1768 cmdline: C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip MD5: 9DE2E060A2985A232D8B96F9EC847A19)
    - 7za.exe (PID: 4852 cmdline: C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\oluilyf2.xu4" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
      - conhost.exe (PID: 6420 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - unarchiver.exe (PID: 4788 cmdline: C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip MD5: 9DE2E060A2985A232D8B96F9EC847A19)
    - 7za.exe (PID: 7164 cmdline: C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\evppz250.yan" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
      - conhost.exe (PID: 5772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- chrome.exe (PID: 760 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://cloudfil.es/ly7mR8utBQ5 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\oluilyf2.xu4\SARS OUTSTANDING LETTER OF DEMAND.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	
C:\Users\user\AppData\Local\Temp\evppz250.yan\SARS OUTSTANDING LETTER OF DEMAND.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	
C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e\SARS OUTSTANDING LETTER OF DEMAND.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

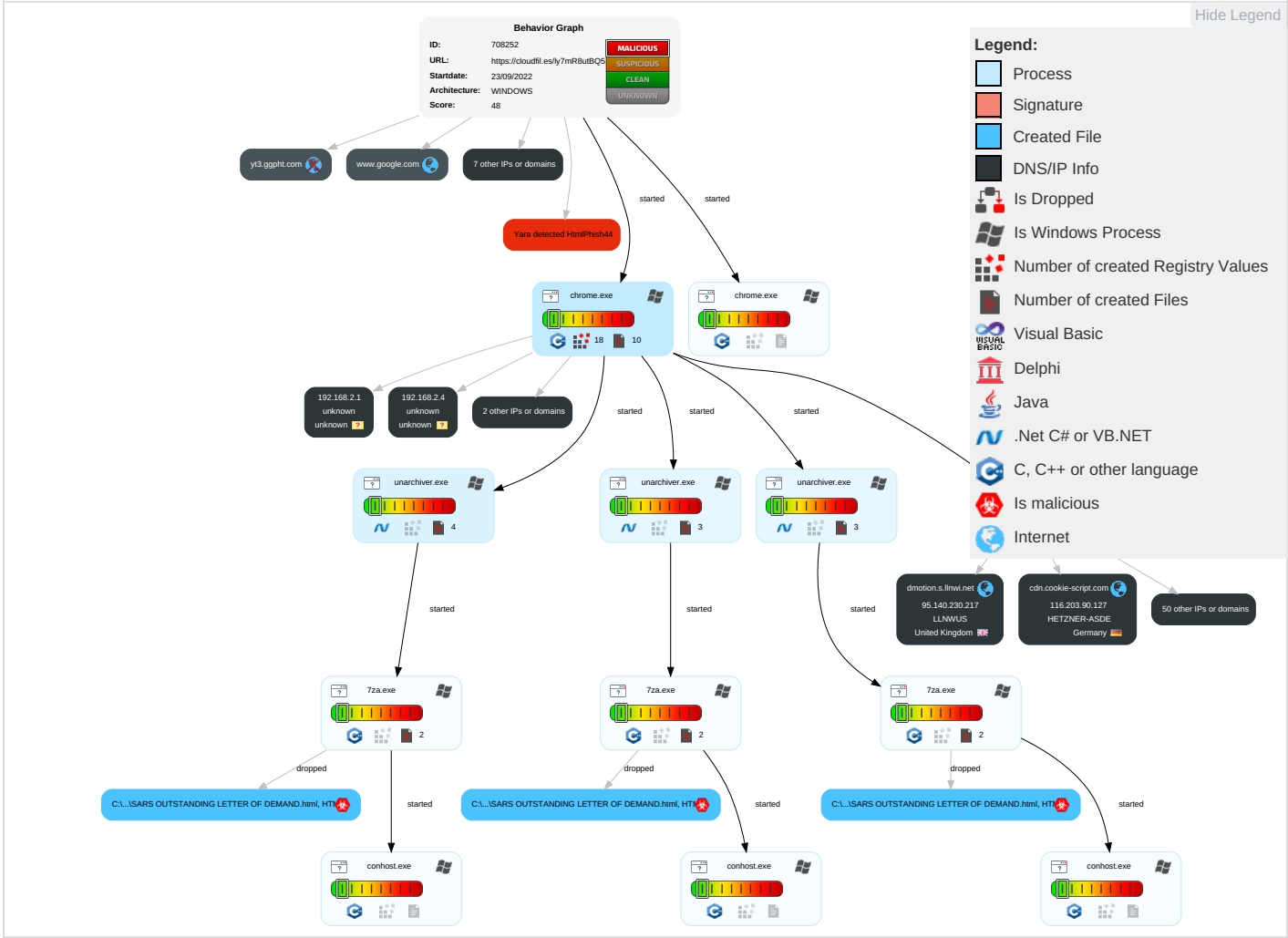
Phishing

Yara detected HtmlPhish44

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
1 Drive-by Compromise	Windows Management Instrumentation	Path Interception	1 1 Process Injection	3 Masquerading	OS Credential Dumping	2 1 Virtualization/Sandbox Evasion	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 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 Disable or Modify Tools	LSASS Memory	3 System Information 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)	2 1 Virtualization/Sandbox Evasion	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)	1 1 Process Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

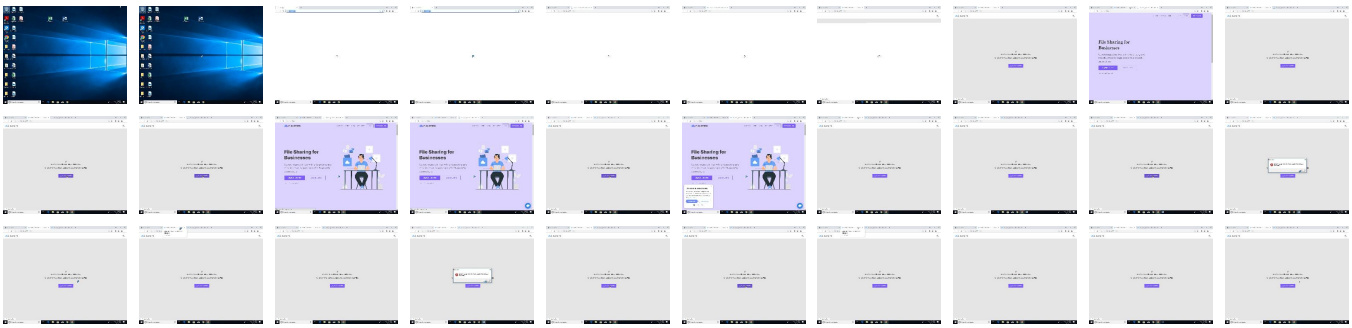
Behavior Graph

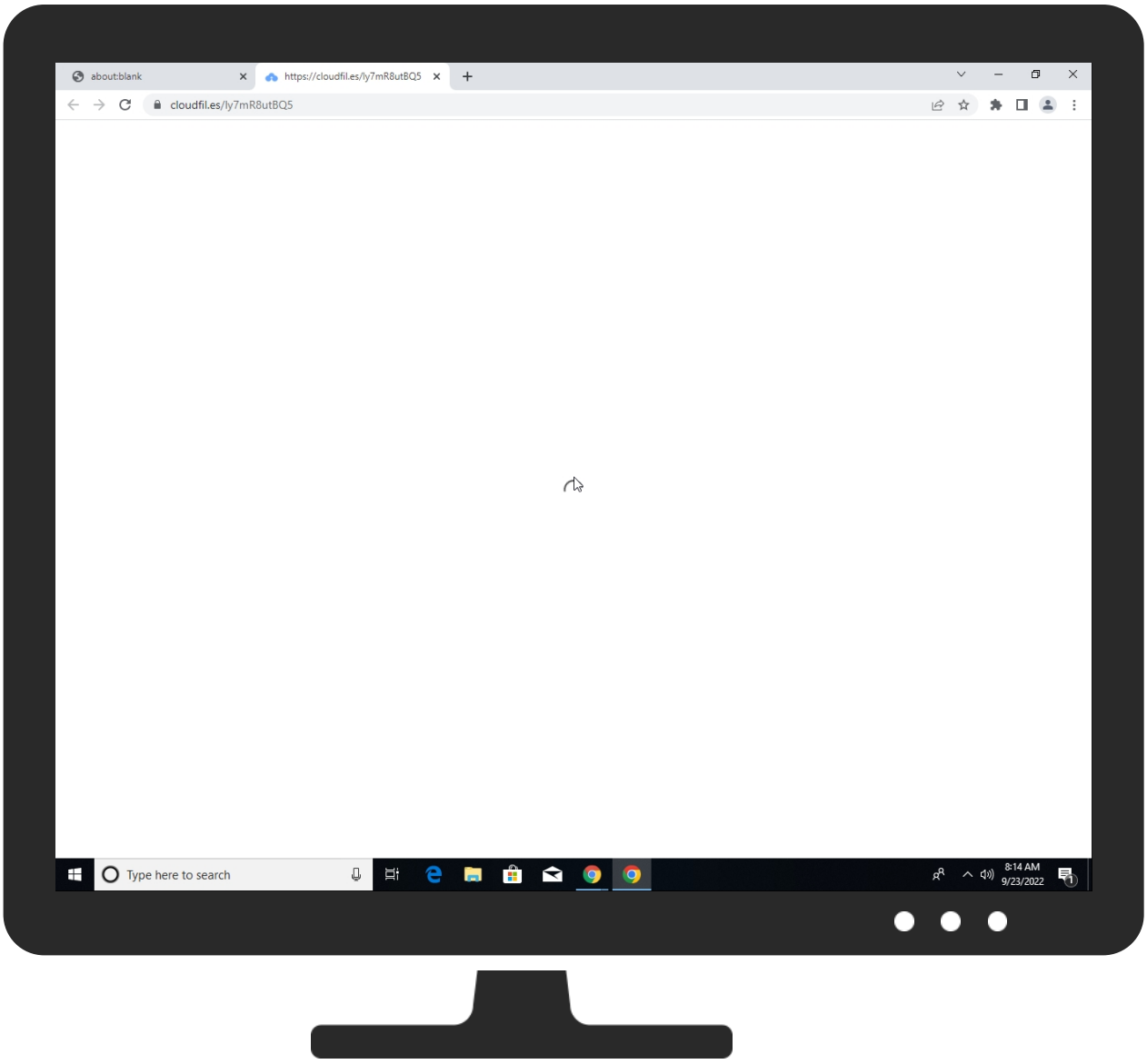


Screenshots

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://https://cloudfil.es/ly7mR8utBQ5	0%	Virustotal		Browse
http://https://cloudfil.es/ly7mR8utBQ5	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://https://js.usemessages.com/conversations-embed.js	0%	URL Reputation	safe	
http://https://js.hsadspixel.net/fb.js	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cloudfiles.io/_next/image?url=%2Fimages%2Fpages%2Fhome%2Ftestimonials%2Fhs-logo.png&w=1920&q=75	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/testimonials/Jordan-Harris.jpeg	0%	Avira URL Cloud	safe	
http://https://cloudfil.es/_next/static/chunks/main-96fa8ae7c24c9725.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/logos/security/gdpr.png	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/icons/twitter.png	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/YJeXlCCpqKEI4BNvP_rQi/_buildManifest.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/testimonials/neighbourhood-logo.jpeg	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/testimonials/Architecture-Social.jpeg	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/icons/linkedin.png	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/testimonials/1920px-HubSpot_Logo.svg.png	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/testimonials/Chris-Moore.png	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/ads/ga-audiences?v=1&t=sr&slf_rd=1&_r=4&tid=G-HB9Z4JLXX4&cid=604035153.1663946092>m=2oe9l0&aip=1&z=1923764674	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/YJeXlCCpqKEI4BNvP_rQi/_ssgManifest.js	0%	Avira URL Cloud	safe	
http://https://js.hs-banner.com/20182553.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/pages/%5Bslug%5D-987d9e7f5dfae2bd.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/423-c466c32b0761d1c5.js	0%	Avira URL Cloud	safe	
http://https://api.cloudfil.es/api/views/632d4ec5c3d2310bbf142ae1/download	0%	Avira URL Cloud	safe	
http://https://api.cloudfil.es/api/ly7mR8utBQ5	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/197-c096a3bf80407be8.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/features/file-links.svg	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/testimonials/goreact-logo.svg	0%	Avira URL Cloud	safe	
http://https://cloudfil.es/favicon.ico	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/buddha-banner.jpg	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/pagead/1p-user-list/10783125194/?random=1663946097443&cv=9&fst=1663945200000&num=1&bg=ffffff&guid=ON&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=0&u_nmime=0>m=2oa9l0&sendb=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fcloudfiles.io%2F&tiba=File%20Sharing%20Platform%20%7C%20Share%20Documents%20Online%20%7C%20CloudFiles&async=1&fmt=3&is_vtc=1&random=1027656747&resp=GooglemKTybQhCsO&rmt_tld=1&ipr=y	0%	Avira URL Cloud	safe	
http://https://cloudfil.es/_next/static/chunks/pages/%5Bhash%5D-da6732468a64e9d9.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/features/detailed-analytics.png	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/pages/_app-f171edb1f3175855.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/logos/FullLogo-new.svg	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/hubspot-dlb/static-1.318/bundle.production.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/image?url=%2Fimages%2Fpages%2Fhome%2Ftestimonials%2Fg2-logo.png&w=3840&q=75	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/icons/angellist.png	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/390-8a0eaf13ec9db927.js	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-188936264-1&cid=604035153.1663946092&jid=1865915276&_u=YADAAUAAAAAAAC~&z=1702222027	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/545f34e4-eb701074efab5973.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/hog/decide?v=2&ip=1&_=1663946086126	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/data/YJeXlCCpqKEI4BNvP_rQi/pricing.json?slug=pricing	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/pagead/1p-user-list/10790155329/?random=1663946097413&cv=9&fst=1663945200000&num=1&bg=ffffff&guid=ON&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=0&u_nmime=0>m=2oa9l0&sendb=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fcloudfiles.io%2F&tiba=File%20Sharing%20Platform%20%7C%20Share%20Documents%20Online%20%7C%20CloudFiles&async=1&fmt=3&is_vtc=1&random=346257282&resp=GooglemKTybQhCsO&rmt_tld=1&ipr=y	0%	Avira URL Cloud	safe	
http://https://api.cloudfil.es/api/ly7mR8utBQ5/files	0%	Avira URL Cloud	safe	
http://https://cloudfil.es/_next/static/css/761d08517528cd55.css	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/features/secure-file-sharing.svg	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/logos/security/soc2.webp	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/5ca00d41-f80dcc02233c86a3.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/framework-5f4595e5518b5600.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/pages/index-54a1471851cf647f.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/fc20e1c4-9e1761e40e9bca31.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/hog/e?ip=1&_=1663946086204	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/testimonials/Travis-White.jpg	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/testimonials/5-star-rating.svg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://cloudfiles.io/_next/static/chunks/28-8667e3219650ddd1.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/features/cloud-copy.svg	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/951-9933cd60a769c984.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/43a99af2-6a652ea0e41564d0.js	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/head-dlb/static-1.233/bundle.production.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/images/pages/home/hero-image.svg	0%	Avira URL Cloud	safe	
http://https://cloudfil.es/_next/static/chunks/838-e577e7ded876b417.js	0%	Avira URL Cloud	safe	
http://https://cloudfiles.io/_next/static/chunks/b16bd182-2fce6d9e40c8c943.js	0%	Avira URL Cloud	safe	
http://https://cloudfil.es/images/logoWordmark.svg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.16.195	true	false		high
i.ytimg.com	142.250.186.182	true	false		high
js.hs-analytics.net	104.17.69.176	true	false		unknown
cloudfil.es	76.76.21.21	true	false		unknown
d296je7bbdd650.cloudfront.net	108.138.32.174	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
track.hubspot.com	104.19.154.83	true	false		high
avatars.hubspot.net	104.17.240.204	true	false		high
dmotion.s.llnwi.net	95.140.230.217	true	false		unknown
photos-ugc.l.googleusercontent.com	142.250.186.161	true	false		high
www.google.com	142.250.185.164	true	false		high
js.usemessages.com	104.17.239.204	true	false		unknown
api.cloudfil.es	172.67.199.56	true	false		unknown
js.hs-banner.com	104.18.33.171	true	false		unknown
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
a.nel.cloudflare.com	35.190.80.1	true	false		high
static.hsappstatic.net	104.17.6.210	true	false		unknown
accounts.google.com	216.58.212.173	true	false		high
stats.l.doubleclick.net	108.177.15.156	true	false		high
app.hubspot.com	104.19.155.83	true	false		high
www-googletagmanager.l.google.com	172.217.18.8	true	false		high
js.hsadspixel.net	104.17.112.176	true	false		unknown
region1.analytics.google.com	216.239.32.36	true	false		high
static-doubleclick-net.l.google.com	142.250.185.166	true	false		high
youtube-ui.l.google.com	172.217.23.110	true	false		high
js-na1.hs-scripts.com	104.17.213.204	true	false		high
api.hubspot.com	104.19.154.83	true	false		high
googleads.g.doubleclick.net	142.250.184.226	true	false		high
play.google.com	142.250.185.110	true	false		high
api-na1.hubspot.com	104.19.154.83	true	false		high
api.hubapi.com	104.17.202.204	true	false		high
www.google.co.uk	172.217.18.3	true	false		unknown
cloudfiles.io	76.76.21.21	true	false		unknown
clients.l.google.com	142.250.186.46	true	false		high
cdn.cookie-script.com	116.203.90.127	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
cdn.segment.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
api.dmcdn.net	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
bam-cell.nr-data.net	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.facebook.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
js-agent.newrelic.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
static.doubleclick.net	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high

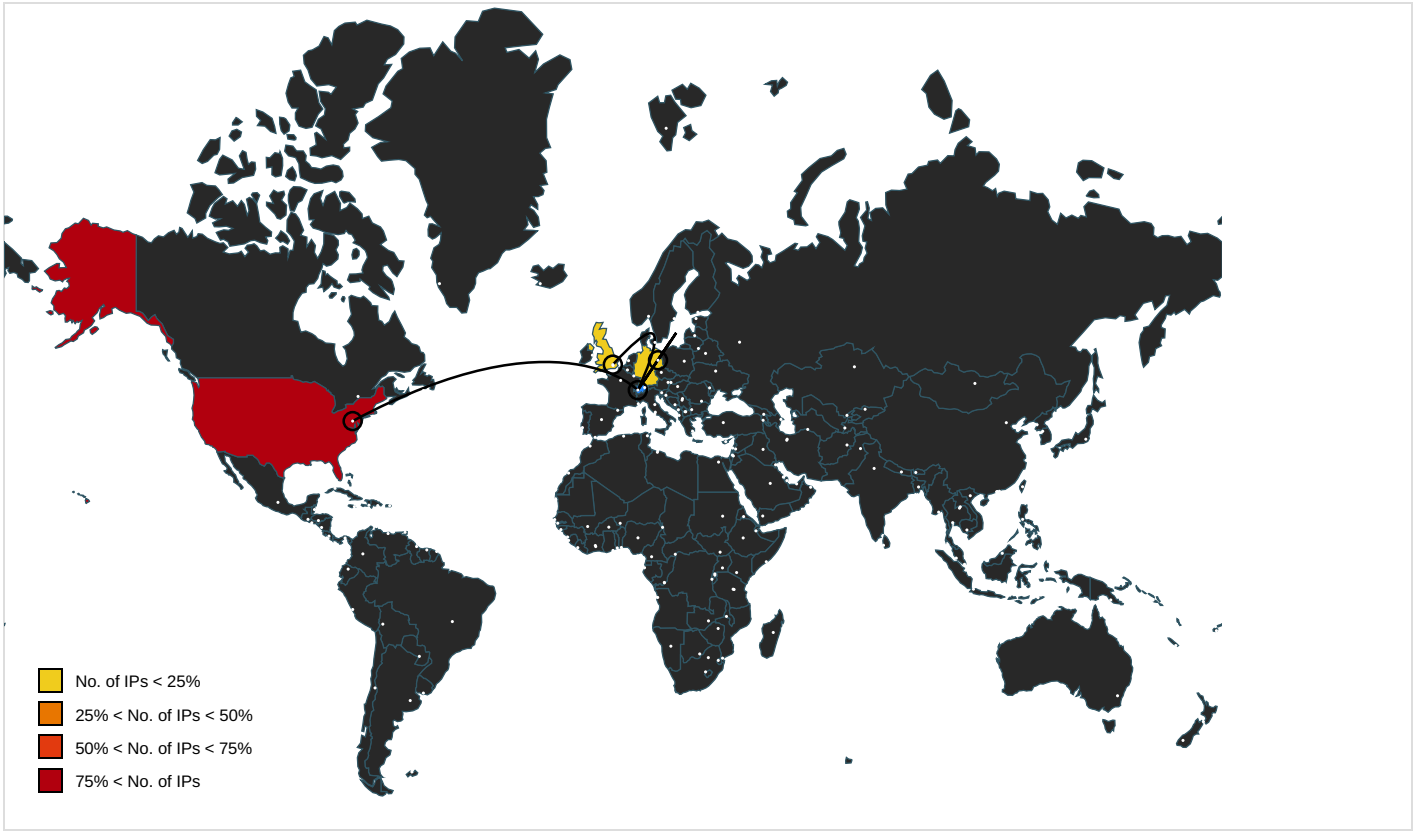
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cloudfiles.io/_next/image?url=%2Fimages%2Fpages%2Fhome%2Ftestimonials%2Fhs-logo.png&w=1920&q=75	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/logos/security/gdpr.png	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/s/player/abfb84fe/player_ias.vflset/en_US/base.js	false		high
http://https://region1.analytics.google.com/g/collect?v=2&tid=G-HB9Z4JLXX4>m=2oe9l0&_p=932923266&cid=604035153.1663946092&ul=en-us&sr=1280x1024&_z=ccd.v9B&_s=2&sid=1663946091&sct=1&seg=1&dl=https%3A%2F%2Fcloudfiles.io%2F&dt=File%20Sharing%20Platform%20%7C%20Share%20Documents%20Online%20%7C%20CloudFiles&en=page_view&_ee=1	false		high
http://https://api-na1.hubspot.com/userpreferences/v1/avatar/9da96031556358e4754625e37320e787/100	false		high
http://https://www.google.com/pagead/1p-user-list/10790155329/?random=1663946097413&cv=9&fst=1663945200000&num=1&bg=ffffff&guid=ON&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=0&u_nmime=0>m=2oa9l0&sendb=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fcloudfiles.io%2F&tiba=File%20Sharing%20Platform%20%7C%20Share%20Documents%20Online%20%7C%20CloudFiles&async=1&fmt=3&is_vtc=1&random=346257282&resp=GooglemKTybQhCsO&rmt_tld=0&ipr=y	false		high
http://https://cloudfiles.io/images/pages/home/testimonials/Jordan-Harris.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://cloudfil.es/_next/static/chunks/main-96fa8ae7c24c9725.js	false	• Avira URL Cloud: safe	unknown
http://https://js.usemessages.com/conversations-embed.js	false	• URL Reputation: safe	unknown
http://https://cloudfiles.io/icons/twitter.png	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/YJeXlCCpqKEI4BNvP_rQi/_buildManifest.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/images/pages/home/testimonials/neighbourhood-logo.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://cdn.segment.com/analytics-next/bundles/870.bundle.323974846b6d45afb45e.js	false		high
http://https://www.youtube.com/s/player/abfb84fe/player_ias.vflset/en_US/embed.js	false		high
http://https://avatars.hubspot.net/9da96031556358e4754625e37320e787-100	false		high
http://https://www.youtube.com/iframe_api	false		high
http://https://cloudfiles.io/images/pages/home/testimonials/Architecture-Social.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://cdn.segment.com/v1/projects/KUs1gEeIVanAKts76f3NenLgmETEQxxr/settings	false		high
http://https://www.youtube.com/youtubei/v1/log_event?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y9_11qcW8	false		high
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j97&tid=UA-188936264-1&cid=604035153.1663946092&jid=1865915276&gjid=1491550274&_gid=405113668.1663946093&_u=YADAAUAAAAAAAC~&z=1482416094	false		high
http://https://cloudfiles.io/images/pages/home/testimonials/Chris-Moore.png	false	• Avira URL Cloud: safe	unknown
http://https://connect.facebook.net/en_US/fbevents.js	false		high
http://https://cloudfiles.io/icons/linkedin.png	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/images/pages/home/testimonials/1920px-HubSpot_Logo.svg.png	false	• Avira URL Cloud: safe	unknown
http://https://www.google.co.uk/ads/ga-audiences?v=1&t=sr&slf_rd=1&_r=4&tid=G-HB9Z4JLXX4&cid=604035153.1663946092>m=2oe9l0&aip=1&z=1923764674	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/YJeXlCCpqKEI4BNvP_rQi/_ssgManifest.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/chunks/pages/%5Bslug%5D-987d9e7f5dfae2bd.js	false	• Avira URL Cloud: safe	unknown
http://https://js.hs-banner.com/20182553.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/chunks/197-c096a3bf80407be8.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/chunks/423-c466c32b0761d1c5.js	false	• Avira URL Cloud: safe	unknown
http://https://app.hubspot.com/conversations-visitor/20182553/threads/utk/e86f3294fabf4298bfb6731338a898f9?uuid=9cb37ca1f6ae46778bde47f4ac4692ca&mobile=false&mobileSafari=false&hideWelcomeMessage=false&hstc=null&domain=cloudfiles.io&inApp53=false&messagesUtk=e86f3294fabf4298bfb6731338a898f9&url=https%3A%2F%2Fcloudfiles.io%2F&inline=false&isFullscreen=false&globalCookieOptOut=null&isFirstVisitorSession=true&isAttachmentDisabled=false&enableWidgetCookieBanner=false&isInCMS=false	false		high
http://https://api.cloudfil.es/api/ly7mR8utBQ5	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/images/pages/home/features/file-links.svg	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://api.cloudfil.es/api/views/632d4ec5c3d2310bbf142ae1/download	false	• Avira URL Cloud: safe	unknown
http://https://i.ytimg.com/vi_webp/1rkTwk6PKdY/sddefault.webp	false		high
http://https://cloudfiles.io/images/pages/home/testimonials/goreact-logo.svg	false	• Avira URL Cloud: safe	unknown
http://https://cloudfil.es/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/images/pages/home/buddha-banner.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.co.uk/pagead/1p-user-list/10783125194/?random=1663946097443&cv=9&fst=1663945200000&num=1&bg=ffffff&guid=ON&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=0&u_nmime=0>m=2oa9l0&sendb=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fcloudfiles.io%2F&tiba=File%20Sharing%20Platform%20%7C%20Share%20Documents%20Online%20%7C%20CloudFiles&async=1&fmt=3&is_vtc=1&random=1027656747&resp=GooglemKTybQhCsO&rmt_tld=1&ipr=y	false	• Avira URL Cloud: safe	unknown
http://https://app.hubspot.com/conversations-visitor/20182553/threads/utk/e86f3294fabf4298bfb6731338a898f9?uuid=9cb37ca1f6ae46778bde47f4ac4692ca&mobile=false&mobileSafari=false&hideWelcomeMessage=false&hstc=null&domain=cloudfiles.io&inApp53=false&messagesUtk=e86f3294fabf4298bfb6731338a898f9&url=https%3A%2F%2Fcloudfiles.io%2F&inline=false&isFullscreen=false&globalCookieOptOut=null&isFirstVisitorSession=true&isAttachmentDisabled=false&enableWidgetCookieBanner=false&isInCMS=false&hubspotUtk=222eafc23c17f2f1f20b9c762dc2bdcf	false		high
http://https://static.hsappstatic.net/hubspot-dlb/static-1.318/bundle.production.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/images/pages/home/features/detailed-analytics.png	false	• Avira URL Cloud: safe	unknown
http://https://static.doubleclick.net/instream/ad_status.js	false		high
http://https://cloudfil.es/_next/static/chunks/pages/%5Bhash%5D-da6732468a64e9d9.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/chunks/pages/_app-f171edb1f3175855.js	false	• Avira URL Cloud: safe	unknown
http://https://js.hsadspixel.net/fb.js	false	• URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/id	false		high
http://https://cdn.segment.com/analytics.js/v1/KUs1gEeIVanAKts76f3NenLgmETEQxxr/analytics.min.js	false		high
http://https://api.hubapi.com/hs-script-loader-public/v1/config/pixel/json?portalId=20182553	false		high
http://https://www.facebook.com/tr/?id=749116996109032&ev=Microdata&dl=https%3A%2F%2Fcloudfiles.io%2F&rl=&if=false&ts=1663946095810&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22File%20Sharing%20Platform%20%7C%20Share%20Documents%20Online%20%7C%20CloudFiles%22%2C%22meta%3Adescription%22%3A%22CloudFiles%20is%20a%20modern%20file%20sharing%20platform%20for%20businesses%20designed%20to%20reduce%20mundane%20tasks.%20Sign%20up%20and%20put%20your%20energy%20to%20things%20that%20matter.%22%7D&cd[OpenGraph]=%7B%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1280&sh=1024&v=2.9.83&r=stable&ec=1&o=30&fbp=fb.1.1663946093092.1064301508&it=1663946090710&coo=false&es=automatic&tm=3&rqm=GET	false		high
http://https://cloudfiles.io/logos/FullLogo-new.svg	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/icons/angellist.png	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/image?url=%2Fimages%2Fpages%2Fhome%2Ftestimonials%2Fg2-logo.png&w=3840&q=75	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/chunks/390-8a0eaf13ec9db927.js	false	• Avira URL Cloud: safe	unknown
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-188936264-1&cid=604035153.1663946092&jid=1865915276&_u=YADAAUAAAAAAAC~&z=1702222027	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/pagead/1p-user-list/10783125194/?random=1663946097443&cv=9&fst=1663945200000&num=1&bg=ffffff&guid=ON&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=0&u_nmime=0>m=2oa9l0&sendb=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fcloudfiles.io%2F&tiba=File%20Sharing%20Platform%20%7C%20Share%20Documents%20Online%20%7C%20CloudFiles&async=1&fmt=3&is_vtc=1&random=1027656747&resp=GooglemKTybQhCsO&rmt_tld=0&ipr=y	false		high
http://https://api-na1.hubspot.com/userpreferences/v1/avatar/af37eb0cf85adf85d80f9fda4baa0b45/100	false		high
http://https://cloudfiles.io/_next/static/chunks/545f34e4-eb701074efab5973.js	false	• Avira URL Cloud: safe	unknown
http://https://cdn.cookie-script.com/s/61cbca8494eb3ac19b8548ecc52b65d8.js	false		high
http://https://cloudfiles.io/hog/decide?v=2&ip=1&_=1663946086126	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/data/YJeXlCCpqKEI4BNvP_rQi/pricing.json?slug=pricing	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-188936264-1&cid=604035153.1663946092&jid=1865915276&_u=YADAAUAAAAAAAC~&z=1702222027	false		high
http://https://api.dmcdn.net/all.js	false		high
http://https://www.google.co.uk/pagead/1p-user-list/10790155329/?random=1663946097413&cv=9&fst=1663945200000&num=1&bg=ffffff&guid=ON&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=0&u_nmime=0>m=2oa9l0&sendb=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fcloudfiles.io%2F&tiba=File%20Sharing%20Platform%20%7C%20Share%20Documents%20Online%20%7C%20CloudFiles&async=1&fmt=3&is_vtc=1&random=346257282&resp=GooglemKTybQhCsO&rmt_tld=1&ipr=y	false	• Avira URL Cloud: safe	unknown
http://https://api.cloudfil.es/api/ly7mR8utBQ5/files	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://www.youtube.com/s/player/abfb84fe/fetch-polyfill.vflset/fetch-polyfill.js	false		high
http://https://www.youtube.com/generate_204?uf-mSA	false		high
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-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://cloudfil.es/_next/static/css/761d08517528cd55.css	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/images/pages/home/features/secure-file-sharing.svg	false	• Avira URL Cloud: safe	unknown
http://https://cdn.segment.com/analytics-next/bundles/schemaFilter.bundle.debb169c1abb431faaa6.js	false		high
http://https://www.youtube.com/embed/1rkTwk6PKdY?autoplay=0&mute=0&controls=0&origin=https%3A%2F%2Fcloudfiles.io&playsinline=1&showinfo=0&rel=0&iv_load_policy=3&modestbranding=1&enablejsapi=1&widgetid=1	false		high
http://https://connect.facebook.net/signals/config/749116996109032?v=2.9.83&r=stable	false		high
http://https://app.hubspot.com/api/cartographer/v1/rhumb?hs_static_app=conversations-visitor-ui&hs_static_app_version=1.13284	false		high
http://https://cloudfiles.io/_next/static/chunks/5ca00d41-f80dcc02233c86a3.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/logos/security/soc2.webp	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/	false		unknown
http://https://cloudfiles.io/_next/static/chunks/framework-5f4595e5518b5600.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/chunks/pages/index-54a1471851cf647f.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/chunks/fc20e1c4-9e1761e40e9bca31.js	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/s/player/abfb84fe/www-embed-player.vflset/www-embed-player.js	false		high
http://https://app.hubspot.com/api/cartographer/v1/performance?hs_static_app=conversations-visitor-ui&hs_static_app_version=1.13284	false		high
http://https://cloudfiles.io/hog/e?ip=1&_=1663946086204	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/images/pages/home/testimonials/Travis-White.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/js/th/A6NiJ4FpWdYb46YkL14Gb7YSsd_Y0OEDYbyMmxwlYE4.js	false		high
http://https://yt3.ggpht.com/ytc/AMLnZu-FWsVbF8aAR_gls7ecgPiqYZt6-nIMTeclblUc=s68-c-k-c0x00ffffff-no-rj	false		high
http://https://avatars.hubspot.net/7baf5799201cac38d1c7a19dc11b89b1-100	false		high
http://https://cloudfiles.io/_next/static/chunks/28-8667e3219650ddd1.js	false	• Avira URL Cloud: safe	unknown
http://https://track.hubspot.com/__ptq.gif?k=1&sd=1280x1024&cd=24-bit&cs=UTF-8&ln=en-us&bfp=4285505810&v=1.1&a=20182553&pu=https%3A%2F%2Fcloudfiles.io%2F&t=File+Sharing+Platform+%7C+Share+Documents+Online+%7C+CloudFiles&cts=1663946098472&vi=222eafc23c17f2f1f20b9c762dc2bdcf&nc=true&u=218584006.222eafc23c17f2f1f20b9c762dc2bdcf.1663946098461.1663946098461.1663946098461.1&b=218584006.1.1663946098463&cc=15	false		high
http://https://cloudfiles.io/images/pages/home/testimonials/5-star-rating.svg	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/images/pages/home/features/cloud-copy.svg	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/chunks/951-9933cd60a769c984.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/chunks/43a99af2-6a652ea0e41564d0.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfil.es/ly7mR8utBQ5	false		unknown
http://https://cloudfiles.io/images/pages/home/hero-image.svg	false	• Avira URL Cloud: safe	unknown
http://https://static.hsappstatic.net/head-dlb/static-1.233/bundle.production.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/	false		unknown
http://https://cloudfil.es/_next/static/chunks/838-e577e7ded876b417.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.io/_next/static/chunks/b16bd182-2fce6d9e40c8c943.js	false	• Avira URL Cloud: safe	unknown
http://https://cloudfil.es/images/logoWordmark.svg	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.19.155.83	app.hubspot.com	United States		13335	CLOUDFLARENETUS	false
108.177.15.156	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
95.140.230.217	dmotion.s.llnwi.net	United Kingdom		22822	LLNWUS	false
104.18.33.171	js.hs-banner.com	United States		13335	CLOUDFLARENETUS	false
104.17.213.204	js-na1.hs-scripts.com	United States		13335	CLOUDFLARENETUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
104.17.239.204	js.usemessages.com	United States		13335	CLOUDFLARENETUS	false
142.250.184.226	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
104.17.6.210	static.hsappstatic.net	United States		13335	CLOUDFLARENETUS	false
76.76.21.21	cloudfil.es	United States		16509	AMAZON-02US	false
104.17.240.204	avatars.hubspot.net	United States		13335	CLOUDFLARENETUS	false
104.21.52.125	unknown	United States		13335	CLOUDFLARENETUS	false
104.19.154.83	track.hubspot.com	United States		13335	CLOUDFLARENETUS	false
172.217.18.8	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.182	i.ytimg.com	United States		15169	GOOGLEUS	false
172.217.18.3	www.google.co.uk	United States		15169	GOOGLEUS	false
142.250.185.110	play.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.17.112.176	js.hsadspixel.net	United States		13335	CLOUDFLARENETUS	false
172.217.16.195	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.46	clients.l.google.com	United States		15169	GOOGLEUS	false
108.138.32.174	d296je7bbdd650.cloudfront.net	United States		16509	AMAZON-02US	false
142.250.185.166	static-doubleclick-net.l.google.com	United States		15169	GOOGLEUS	false
216.239.32.36	region1.analytics.google.com	United States		15169	GOOGLEUS	false
172.217.23.110	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
142.250.185.164	www.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.212.173	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.186.161	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.17.202.204	api.hubapi.com	United States		13335	CLOUDFLARENETUS	false
116.203.90.127	cdn.cookie-script.com	Germany		24940	HETZNER-ASDE	false
172.67.199.56	api.cloudfil.es	United States		13335	CLOUDFLARENETUS	false
104.17.69.176	js.hs-analytics.net	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.4
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708252
Start date and time:	2022-09-23 08:13:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://cloudfil.es/ly7mR8utBQ5
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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.win@53/12@49/38
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://cloudfiles.io/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.185.163, 34.104.35.123, 142.250.185.234, 80.67.82.235, 80.67.82.240, 13.107.42.14, 216.239.32.178, 216.239.38.178, 216.239.36.178, 216.239.34.178, 142.250.74.194, 142.250.184.202, 142.250.184.234, 172.217.18.10, 172.217.16.138, 172.217.23.106, 172.217.18.106, 142.250.185.74, 142.250.185.106, 142.250.185.138, 142.250.185.170, 142.250.185.202, 142.250.181.234, 172.217.16.202, 216.58.212.170, 142.250.74.202, 151.101.2.137, 151.101.66.137, 151.101.130.137, 151.101.194.137, 162.247.241.2, 142.250.186.131
- Excluded domains from analysis (whitelisted): www-linkedin-com.l-0005.l-msedge.net, fonts.googleapis.com, fs.microsoft.com, www.googleadservices.com, fonts.gstatic.com, tls12.newrelic.com.cdn.cloudflare.net, www-alv.google-analytics.com, clientservices.googleapis.com, od.linkedin.edgesuite.net, jnn-pa.googleapis.com, k.sni.global.fastly.net, l-0005.l-msedge.net, edgedl.me.gvt1.com, www.googletagmanager.com, update.googleapis.com, a1916.dscg2.akamai.net, www.google-analytics.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 NtWriteFile calls found.
- 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

C:\Users\user\AppData\Local\Temp\evppz250.yan\SARS OUTSTANDING LETTER OF DEMAND.html

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	607486
Entropy (8bit):	5.2236882570919505
Encrypted:	false
SSDEEP:	6144:IgudndlMFDNrPmbRo0oGPmgE+fgx5b1ZugL6kVxV7HX756inXK4C3ambG0OUy5j9:JAWeXE+AIgmmxWina4C3DJOUmzDa7y
MD5:	6C7C272ABC28BF1E856F0B55908EFDF8
SHA1:	C59D77633692929D62CE37C7C505B6B16D93F1DC
SHA-256:	95C9619234E4C0FEB72CD913280552B2DFA9CE6B1B8422FB31696917B880F4ED
SHA-512:	8C31B996DA89C2F5396A9D8EABDDEBF239771B51D5B17E350B9BE9B9EA8EA6C2FF99FF0499F5A5C098AA59BA5CF8740983D27B8F4AE8413C14674736702FD6EA
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_44, Description: Yara detected HtmlPhish_44, Source: C:\Users\user\AppData\Local\Temp\evppz250.yan\SARS OUTSTANDING LETTER OF DEMAND.html, Author: Joe Security
Reputation:	low
Preview:	<script language=javascript>document.write(unescape('%3Cscript%20language%3Djavascript%3Edocument.write%28unescape%28%27%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%253Chtml%2520xmlns%253D%2522http%253A//www.w3.org/1999/xhtml%2522%253E%250A%253Chead%253E%250A%253Cscript%2520type%253D%2522text/javascript%2522%253Efunction%2520showDiv%2528%2529%2520%257B%2520%2520%2520document.getElementById%2528%2527welcomeDiv%2527%2529.style.display%2520%253D%2520%2522block%2522%253B%2520%2520%2520document.getElementById%2528

C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e\SARS OUTSTANDING LETTER OF DEMAND.html

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	607486
Entropy (8bit):	5.2236882570919505
Encrypted:	false
SSDEEP:	6144:IgudndlMFDNrPmbRo0oGPmgE+fgx5b1ZugL6kVxV7HX756inXK4C3ambG0OUy5j9:JAWeXE+AlgmmxWina4C3DJOUmzDa7y
MD5:	6C7C272ABC28BF1E856F0B55908EFDF8
SHA1:	C59D77633692929D62CE37C7C505B6B16D93F1DC
SHA-256:	95C9619234E4C0FEB72CD913280552B2DFA9CE6B1B8422FB31696917B880F4ED
SHA-512:	8C31B996DA89C2F5396A9D8EABDDEBF239771B51D5B17E350B9BE9B9EA8EA6C2FF99FF0499F5A5C098AA59BA5CF8740983D27B8F4AE8413C14674736702FD6EA
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_44, Description: Yara detected HtmlPhish_44, Source: C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e\SARS OUTSTANDING LETTER OF DEMAND.html, Author: Joe Security
Reputation:	low
Preview:	<script language=javascript>document.write(unescape('%3Cscript%20language%3Djavascript%3Edocument.write%28unescape%28%27%250A%253Chtml%2520xmlns%253D%2522http%253A//www.w3.org/1999/xhtml%2522%253E%250A%253Chead%253E%250A%253Cscript%2520type%253D%2522text/javascript%2522%253Efunction%2520showDiv%2528%2529%2520%257B%2520%2520%2520document.getElementById%2528%2527welcomeDiv%2527%2529.style.display%2520%253D%2520%2522block%2522%253B%2520%2520%2520document.getElementById%2528

C:\Users\user\AppData\Local\Temp\oluilyf2.xu4\SARS OUTSTANDING LETTER OF DEMAND.html

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	607486
Entropy (8bit):	5.2236882570919505
Encrypted:	false
SSDEEP:	6144:IgudndlMFDNrPmbRo0oGPmgE+fgx5b1ZugL6kVxV7HX756inXK4C3ambG0OUy5j9:JAWeXE+AlgmmxWina4C3DJOUmzDa7y
MD5:	6C7C272ABC28BF1E856F0B55908EFDF8
SHA1:	C59D77633692929D62CE37C7C505B6B16D93F1DC
SHA-256:	95C9619234E4C0FEB72CD913280552B2DFA9CE6B1B8422FB31696917B880F4ED
SHA-512:	8C31B996DA89C2F5396A9D8EABDDEBF239771B51D5B17E350B9BE9B9EA8EA6C2FF99FF0499F5A5C098AA59BA5CF8740983D27B8F4AE8413C14674736702FD6EA
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_44, Description: Yara detected HtmlPhish_44, Source: C:\Users\user\AppData\Local\Temp\oluilyf2.xu4\SARS OUTSTANDING LETTER OF DEMAND.html, Author: Joe Security
Reputation:	low
Preview:	<script language=javascript>document.write(unescape('%3Cscript%20language%3Djavascript%3Edocument.write%28unescape%28%27%250A%253Chtml%2520xmlns%253D%2522http%253A//www.w3.org/1999/xhtml%2522%253E%250A%253Chead%253E%250A%253Cscript%2520type%253D%2522text/javascript%2522%253Efunction%2520showDiv%2528%2529%2520%257B%2520%2520%2520document.getElementById%2528%2527welcomeDiv%2527%2529.style.display%2520%253D%2520%2522block%2522%253B%2520%2520%2520document.getElementById%2528

C:\Users\user\AppData\Local\Temp\unarchiver.log

Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	4236
Entropy (8bit):	5.232726440512009
Encrypted:	false
SSDEEP:	48:vuvFGTGbTGTGpJGYGTGpvnGbFGGnG7GVGTGOGTGTG0lywbWGTGbTGTGpJGYGTGpz:vQMFsUw4w9FwlUh/F0v
MD5:	4EE4F7492444E8A277AFD31BE256EA59
SHA1:	7DB4767426AA4F6F058339526DD8CE377CB0F586

SHA-256:	92EA0D6D6903C7F8880CDEC5A3B795400381D8F2A5DDDBE88757EAEB88B94472
SHA-512:	0F3C1FAA7124E44A1B9C415A725219398F939C13DCB6FB8AF00B45F47477CFC354F1894C9C25428587C1E18E51FA8DE8CA2AF267C73517F29636728224198ED9
Malicious:	false
Reputation:	low
Preview:	09/23/2022 8:14 AM: Unpack: C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip..09/23/2022 8:15 AM: Tmp dir: C:\Users\user\AppDat a\Local\Temp\fsnnqwuj.h1e..09/23/2022 8:15 AM: Received from standard out: ..09/23/2022 8:15 AM: Received from standard out: 7-Zip 18.05 (x86) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30..09/23/2022 8:15 AM: Received from standard out: ..09/23/2022 8:15 AM: Received from standard out: Scanning the drive for archives:..09/23/2022 8:15 AM: Received from standard out: 1 file, 218624 bytes (214 KiB)..09/23/2022 8:15 AM: Received from standard out: ..09/23/2022 8:15 AM: Received from standard out: Extracting archive: C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip..09/23/2022 8:15 AM: Received from standard out: --.. 09/23/2022 8:15 AM: Received from standard out: Path = C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip..09/23/2022 8:15 AM: Received fro m standard out: Type = zip..09/23/2022 8:15 AM: Received from stan

C:\Users\user\Downloads\22e8244c-6e16-464c-801c-35bec625d846.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	**7.992671078684705**
Encrypted:	**true**
SSDEEP:	768:U4HB+ZeuYtS2pfJN/DXcT/k1J1/WzzYaHxKA695tdZP+Q9bgJ:U4H2euORdX4/sJ1/8zYaHxKA67BP+RJ
MD5:	F4CDDC3CA6224D9613C1309A94F05FE4
SHA1:	6024DF7345E7A805DDF0D83A2E766B8C8F96F4C1
SHA-256:	00384D0BEC2D3E1BDE76849383B8016C4748D114EE2A2D7E66C97B4D0CF3E16D
SHA-512:	C67DABE92C8E4043E43CF16F8CC6301A8FC499653438C915984C447B1FB300A8C598B428B6F86AF19786A9CCE0171E85D5694378636B321518317AEF32F0FAC5
Malicious:	false
Reputation:	low
Preview:	PK.....Z6U./..RU...D..&...SARS OUTSTANDING LETTER OF DEMAND.html.:Y..Z..e^:.0,v....@....E.e...Mv...b.[-.]}..<.z8.9.yr'3.....O.....-t..^...b...(..R?..UDvf.....L. ?`....B.P. .#...xC.....xy.t.0X.A.....W.....^*.%N].''I...p.3.sG....7.....+....:.....J.)''3.....L.....|....\..s&...fj]1....8._..=..,o....$.7b..{.....o_.....g.sg.G.....WU.k8.s..=[lh..^.W-O.(.../..I.y.. ..x.....}.)rgH..'.r?.z.2.....N.l+.K.....9.,j...._.....z?..PO]?....sL..`R..s....k..w...0.<..O`..<.i\D...8.....7X.~.d.[...I,.3...C?hnt.....vP.o.L..af..s.'...}#.....[..n...a.G.'....Z.....D^=..@ .g...../....N....e.....'N..9..8x q.....D./.o...f...Z...g?.*|g.w..nY~../..5..X.y...|..../.....P.S..8.;..D..8....2.C;.G.S...zU_....a.4.....W..V.q.....%?..?.r....F....xr...x.../x../|.4O...?....,. .....).'.....\.....9.!_..?..=.?...^....Id....%2#.....G}.....i>k.>E.....WO.).r..|...t...z.wV4...@>N.^W...D7.2R...8]9..`..B.

C:\Users\user\Downloads\97f61521-b3dd-4003-bb1c-5ea026c9e45a.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	**7.992671078684705**
Encrypted:	**true**
SSDEEP:	768:U4HB+ZeuYtS2pfJN/DXcT/k1J1/WzzYaHxKA695tdZP+Q9bgJ:U4H2euORdX4/sJ1/8zYaHxKA67BP+RJ
MD5:	F4CDDC3CA6224D9613C1309A94F05FE4
SHA1:	6024DF7345E7A805DDF0D83A2E766B8C8F96F4C1
SHA-256:	00384D0BEC2D3E1BDE76849383B8016C4748D114EE2A2D7E66C97B4D0CF3E16D
SHA-512:	C67DABE92C8E4043E43CF16F8CC6301A8FC499653438C915984C447B1FB300A8C598B428B6F86AF19786A9CCE0171E85D5694378636B321518317AEF32F0FAC5
Malicious:	false
Reputation:	low
Preview:	PK.....Z6U./..RU...D..&...SARS OUTSTANDING LETTER OF DEMAND.html.:Y..Z..e^:.0,v....@....E.e...Mv...b.[-.]}..<.z8.9.yr'3.....O.....-t..^...b...(..R?..UDvf.....L. ?`....B.P. .#...xC.....xy.t.0X.A.....W.....^*.%N].''I...p.3.sG....7.....+....:.....J.)''3.....L.....|....\..s&...fj]1....8._..=..,o....$.7b..{.....o_.....g.sg.G.....WU.k8.s..=[lh..^.W-O.(.../..I.y.. ..x.....}.)rgH..'.r?.z.2.....N.l+.K.....9.,j...._.....z?..PO]?....sL..`R..s....k..w...0.<..O`..<.i\D...8.....7X.~.d.[...I,.3...C?hnt.....vP.o.L..af..s.'...}#.....[..n...a.G.'....Z.....D^=..@ .g...../....N....e.....'N..9..8x q.....D./.o...f...Z...g?.*|g.w..nY~../..5..X.y...|..../.....P.S..8.;..D..8....2.C;.G.S...zU_....a.4.....W..V.q.....%?..?.r....F....xr...x.../x../|.4O...?....,. .....).'.....\.....9.!_..?..=.?...^....Id....%2#.....G}.....i>k.>E.....WO.).r..|...t...z.wV4...@>N.^W...D7.2R...8]9..`..B.

C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	218624
Entropy (8bit):	**7.997633897441664**
Encrypted:	**true**
SSDEEP:	6144:Uir/w6o2bJbeM8N39ricj/EkZe1cGDRyKkcWT0n0v:5Do2NbeM8NhiM/EkmTZX0v
MD5:	768A4E2E3787C533A467D3FB433F9BEB
SHA1:	E3EB38314319F27BCA5F17DA7CEB96CA64030894
SHA-256:	3CB16DBD2D8C4D037FB5A6BA58D24CBDC6E82A23021FC0666FE0CAB25AA47E3E

SHA-512:	768740724AADDD9BEF9C4EF0F0CE57CC5316BEC60AE3C956ACAE3E62BF9F99983EC0231C9F487593A8CE4B4BD10927F1F66608F3B24987895E449F8403818C0 4
Malicious:	false
Reputation:	low
Preview:	PK.....Z6U./..RU...D..&...SARS OUTSTANDING LETTER OF DEMAND.html.:Y..Z..e^:.0,v....@....E.e...Mv...b.[-.]}..<.z8.9.yr'3.....O.....-t...^...b...(..R?..UDvf.....L. ?`....B.P. .#...xC.....xy.t.0X.A.....W.....^*.%N]."I...p.3.sG....7.....+....:....J.)"3.....L.....|....\..s&...fj]1....8._..=..,o....$.7b..{.....o_.....g.sg.G.....WU.k8.s..=[lh..^.W-O.(.../..I.y.. ..x.....}.)rgH..'.r?.z.2.....N.l+.K.....9..,j...._.....z?..PO]?....sL..`R..s....k..w...0.<..O`..<.i\D...8.....7X.~.d.[...I,.3...C?hnt.....vP.o.L..af..s.'...}#.....[..n...a.G.'....Z.....D^=..@ .g...../....N....e.....'N..9..8x q.....D./.o...f...Z...g?.*|g.w..nY~../..5..X.y...|..../.....P.S..8.;..D..8....2.C;.G.S...zU_....a.4.....W..V.q.....%?..?.r....F....xr...x.../x../|.4O...?....,. .....).'.....\.....9.!_..?..=.?...^....Id....%2#.....G}.....i>k.>E.....WO.).r..|...t...z.wV4...@>N.^W...D7.2R...8]9..`..B.

C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip.crdownload

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	218624
Entropy (8bit):	**7.997633897441664**
Encrypted:	**true**
SSDEEP:	6144:Uir/w6o2bJbeM8N39ricj/EkZe1cGDRyKkcWT0n0v:5Do2NbeM8NhiM/EkmTZX0v
MD5:	768A4E2E3787C533A467D3FB433F9BEB
SHA1:	E3EB38314319F27BCA5F17DA7CEB96CA64030894
SHA-256:	3CB16DBD2D8C4D037FB5A6BA58D24CBDC6E82A23021FC0666FE0CAB25AA47E3E
SHA-512:	768740724AADDD9BEF9C4EF0F0CE57CC5316BEC60AE3C956ACAE3E62BF9F99983EC0231C9F487593A8CE4B4BD10927F1F66608F3B24987895E449F8403818C0 4
Malicious:	false
Reputation:	low
Preview:	PK.....Z6U./..RU...D..&...SARS OUTSTANDING LETTER OF DEMAND.html.:Y..Z..e^:.0,v....@....E.e...Mv...b.[-.]}..<.z8.9.yr'3.....O.....-t...^...b...(..R?..UDvf.....L. ?`....B.P. .#...xC.....xy.t.0X.A.....W.....^*.%N]."I...p.3.sG....7.....+....:....J.)"3.....L.....|....\..s&...fj]1....8._..=..,o....$.7b..{.....o_.....g.sg.G.....WU.k8.s..=[lh..^.W-O.(.../..I.y.. ..x.....}.)rgH..'.r?.z.2.....N.l+.K.....9..,j...._.....z?..PO]?....sL..`R..s....k..w...0.<..O`..<.i\D...8.....7X.~.d.[...I,.3...C?hnt.....vP.o.L..af..s.'...}#.....[..n...a.G.'....Z.....D^=..@ .g...../....N....e.....'N..9..8x q.....D./.o...f...Z...g?.*|g.w..nY~../..5..X.y...|..../.....P.S..8.;..D..8....2.C;.G.S...zU_....a.4.....W..V.q.....%?..?.r....F....xr...x.../x../|.4O...?....,. .....).'.....\.....9.!_..?..=.?...^....Id....%2#.....G}.....i>k.>E.....WO.).r..|...t...z.wV4...@>N.^W...D7.2R...8]9..`..B.

C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	218624
Entropy (8bit):	**7.997633897441664**
Encrypted:	**true**
SSDEEP:	6144:Uir/w6o2bJbeM8N39ricj/EkZe1cGDRyKkcWT0n0v:5Do2NbeM8NhiM/EkmTZX0v
MD5:	768A4E2E3787C533A467D3FB433F9BEB
SHA1:	E3EB38314319F27BCA5F17DA7CEB96CA64030894
SHA-256:	3CB16DBD2D8C4D037FB5A6BA58D24CBDC6E82A23021FC0666FE0CAB25AA47E3E
SHA-512:	768740724AADDD9BEF9C4EF0F0CE57CC5316BEC60AE3C956ACAE3E62BF9F99983EC0231C9F487593A8CE4B4BD10927F1F66608F3B24987895E449F8403818C0 4
Malicious:	false
Reputation:	low
Preview:	PK.....Z6U./..RU...D..&...SARS OUTSTANDING LETTER OF DEMAND.html.:Y..Z..e^:.0,v....@....E.e...Mv...b.[-.]}..<.z8.9.yr'3.....O.....-t...^...b...(..R?..UDvf.....L. ?`....B.P. .#...xC.....xy.t.0X.A.....W.....^*.%N]."I...p.3.sG....7.....+....:....J.)"3.....L.....|....\..s&...fj]1....8._..=..,o....$.7b..{.....o_.....g.sg.G.....WU.k8.s..=[lh..^.W-O.(.../..I.y.. ..x.....}.)rgH..'.r?.z.2.....N.l+.K.....9..,j...._.....z?..PO]?....sL..`R..s....k..w...0.<..O`..<.i\D...8.....7X.~.d.[...I,.3...C?hnt.....vP.o.L..af..s.'...}#.....[..n...a.G.'....Z.....D^=..@ .g...../....N....e.....'N..9..8x q.....D./.o...f...Z...g?.*|g.w..nY~../..5..X.y...|..../.....P.S..8.;..D..8....2.C;.G.S...zU_....a.4.....W..V.q.....%?..?.r....F....xr...x.../x../|.4O...?....,. .....).'.....\.....9.!_..?..=.?...^....Id....%2#.....G}.....i>k.>E.....WO.).r..|...t...z.wV4...@>N.^W...D7.2R...8]9..`..B.

C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip.crdownload

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	218624
Entropy (8bit):	**7.997633897441664**
Encrypted:	**true**
SSDEEP:	6144:Uir/w6o2bJbeM8N39ricj/EkZe1cGDRyKkcWT0n0v:5Do2NbeM8NhiM/EkmTZX0v
MD5:	768A4E2E3787C533A467D3FB433F9BEB
SHA1:	E3EB38314319F27BCA5F17DA7CEB96CA64030894
SHA-256:	3CB16DBD2D8C4D037FB5A6BA58D24CBDC6E82A23021FC0666FE0CAB25AA47E3E

SHA-512:	768740724AADDD9BEF9C4EF0F0CE57CC5316BEC60AE3C956ACAE3E62BF9F99983EC0231C9F487593A8CE4B4BD10927F1F66608F3B24987895E449F8403818C0 4
Malicious:	false
Reputation:	low
Preview:	PK.....Z6U./..RU...D..&...SARS OUTSTANDING LETTER OF DEMAND.html.:Y..Z..e^:.0,v....@....E.e...Mv...b.[-.]}..<.z8.9.yr'3.....O.....-t...^...b...(..R?..UDvf.....L. ?`....B.P. .#...xC.....xy.t.0X.A.....W.....^*.%N]."I...p.3.sG....7.....+....:....J.)"3.....L.....|....\..s&...fj]1....8._..=..,o....$.7b..{.....o_.....g.sg.G.....WU.k8.s..=[lh..^.W-O.(.../..I.y.. ..x.....}.)rgH..'.r?.z.2.....N.l+.K.....9..,j...._.....z?..PO]?....sL..`R..s....k..w...0.<..O`..<.i\D...8.....7X.~.d.[...I,.3...C?hnt.....vP.o.L..af..s.'...}#.....[..n...a.G.'....Z.....D^=..@ .g...../....N....e...../'N..9..8x q.....D./.o...f...Z...g?.*|g.w..nY~../..5..X.y...|..../.....P.S..8.;..D..8....2.C;.G.S...zU_....a.4.....W..V.q.....%?..?.r....F....xr...x.../x../|.4O...?....,. .....).'.....\.....9.!_..?..=.?...^....Id....%2#.....G}.....i>k.>E.....WO.).r..|...t...z.wV4...@>N.^W...D7.2R...8]9..`..B.

C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	218624
Entropy (8bit):	**7.997633897441664**
Encrypted:	**true**
SSDEEP:	6144:Uir/w6o2bJbeM8N39ricj/EkZe1cGDRyKkcWT0n0v:5Do2NbeM8NhiM/EkmTZX0v
MD5:	768A4E2E3787C533A467D3FB433F9BEB
SHA1:	E3EB38314319F27BCA5F17DA7CEB96CA64030894
SHA-256:	3CB16DBD2D8C4D037FB5A6BA58D24CBDC6E82A23021FC0666FE0CAB25AA47E3E
SHA-512:	768740724AADDD9BEF9C4EF0F0CE57CC5316BEC60AE3C956ACAE3E62BF9F99983EC0231C9F487593A8CE4B4BD10927F1F66608F3B24987895E449F8403818C0 4
Malicious:	false
Reputation:	low
Preview:	PK.....Z6U./..RU...D..&...SARS OUTSTANDING LETTER OF DEMAND.html.:Y..Z..e^:.0,v....@....E.e...Mv...b.[-.]}..<.z8.9.yr'3.....O.....-t...^...b...(..R?..UDvf.....L. ?`....B.P. .#...xC.....xy.t.0X.A.....W.....^*.%N]."I...p.3.sG....7.....+....:....J.)"3.....L.....|....\..s&...fj]1....8._..=..,o....$.7b..{.....o_.....g.sg.G.....WU.k8.s..=[lh..^.W-O.(.../..I.y.. ..x.....}.)rgH..'.r?.z.2.....N.l+.K.....9..,j...._.....z?..PO]?....sL..`R..s....k..w...0.<..O`..<.i\D...8.....7X.~.d.[...I,.3...C?hnt.....vP.o.L..af..s.'...}#.....[..n...a.G.'....Z.....D^=..@ .g...../....N....e...../'N..9..8x q.....D./.o...f...Z...g?.*|g.w..nY~../..5..X.y...|..../.....P.S..8.;..D..8....2.C;.G.S...zU_....a.4.....W..V.q.....%?..?.r....F....xr...x.../x../|.4O...?....,. .....).'.....\.....9.!_..?..=.?...^....Id....%2#.....G}.....i>k.>E.....WO.).r..|...t...z.wV4...@>N.^W...D7.2R...8]9..`..B.

C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip.crdownload

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	218624
Entropy (8bit):	**7.997633897441664**
Encrypted:	**true**
SSDEEP:	6144:Uir/w6o2bJbeM8N39ricj/EkZe1cGDRyKkcWT0n0v:5Do2NbeM8NhiM/EkmTZX0v
MD5:	768A4E2E3787C533A467D3FB433F9BEB
SHA1:	E3EB38314319F27BCA5F17DA7CEB96CA64030894
SHA-256:	3CB16DBD2D8C4D037FB5A6BA58D24CBDC6E82A23021FC0666FE0CAB25AA47E3E
SHA-512:	768740724AADDD9BEF9C4EF0F0CE57CC5316BEC60AE3C956ACAE3E62BF9F99983EC0231C9F487593A8CE4B4BD10927F1F66608F3B24987895E449F8403818C0 4
Malicious:	false
Reputation:	low
Preview:	PK.....Z6U./..RU...D..&...SARS OUTSTANDING LETTER OF DEMAND.html.:Y..Z..e^:.0,v....@....E.e...Mv...b.[-.]}..<.z8.9.yr'3.....O.....-t...^...b...(..R?..UDvf.....L. ?`....B.P. .#...xC.....xy.t.0X.A.....W.....^*.%N]."I...p.3.sG....7.....+....:....J.)"3.....L.....|....\..s&...fj]1....8._..=..,o....$.7b..{.....o_.....g.sg.G.....WU.k8.s..=[lh..^.W-O.(.../..I.y.. ..x.....}.)rgH..'.r?.z.2.....N.l+.K.....9..,j...._.....z?..PO]?....sL..`R..s....k..w...0.<..O`..<.i\D...8.....7X.~.d.[...I,.3...C?hnt.....vP.o.L..af..s.'...}#.....[..n...a.G.'....Z.....D^=..@ .g...../....N....e...../'N..9..8x q.....D./.o...f...Z...g?.*|g.w..nY~../..5..X.y...|..../.....P.S..8.;..D..8....2.C;.G.S...zU_....a.4.....W..V.q.....%?..?.r....F....xr...x.../x../|.4O...?....,. .....).'.....\.....9.!_..?..=.?...^....Id....%2#.....G}.....i>k.>E.....WO.).r..|...t...z.wV4...@>N.^W...D7.2R...8]9..`..B.

Static File Info

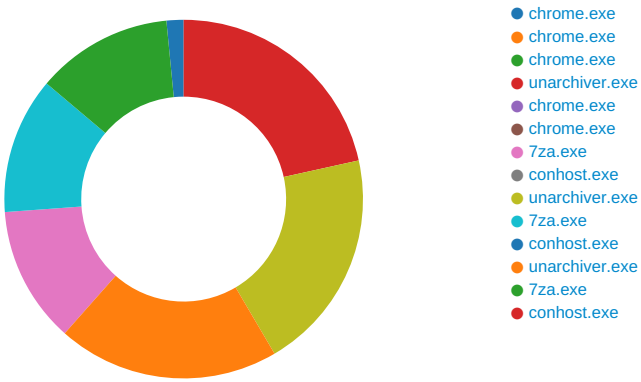
No static file info

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **5928**, Parent PID: **3128**

General

Target ID:	0
Start time:	08:14:15
Start date:	23/09/2022
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:	0x7ff614650000
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: **1572**, Parent PID: **5928**

General	
Target ID:	1
Start time:	08:14:17
Start date:	23/09/2022
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-US --service-sandbox-type=none --mojo-platform-channel-handle=1936 --field-trial-handle=1772,i,13935456055298204775,6851687727719502408,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
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: **760**, Parent PID: **3128**

General	
Target ID:	2
Start time:	08:14:18
Start date:	23/09/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://cloudfil.es/ly7mR8utBQ5
Imagebase:	0x7ff614650000
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

Analysis Process: unarchiver.exe PID: **2768**, Parent PID: **5928**

General	
Target ID:	12
Start time:	08:14:55
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip

Imagebase:	0xd60000
File size:	13312 bytes
MD5 hash:	9DE2E060A2985A232D8B96F9EC847A19
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Local\Temp\unarchiver.log	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	165A58B	CreateFileW
C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	165A999	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\unarchiver.log	0	92	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 34 20 41 4d 3a 20 55 6e 70 61 63 6b 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 6f 77 6e 6c 6f 61 64 73 5c 53 41 52 53 20 4f 55 54 53 54 41 4e 44 49 4e 47 20 4c 45 54 54 45 52 20 4f 46 20 44 45 4d 41 4e 44 2e 7a 69 70 0d 0a	09/23/2022 8:14 AM: Unpack: C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip	success or wait	1	165A8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	92	77	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 54 6d 70 20 64 69 72 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 66 73 6e 6e 71 77 75 6a 2e 68 31 65 0d 0a	09/23/2022 8:15 AM: Tmp dir: C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e	success or wait	1	165A8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	169	50	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 6f 75 74 3a 20 0d 0a	09/23/2022 8:15 AM: Received from standard out:	success or wait	16	165A8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	1336	31	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 47 65 74 20 66 69 6c 65 73 0d 0a	09/23/2022 8:15 AM: Get files	success or wait	1	165A8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	1367	37	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 4e 62 72 20 6f 66 20 66 69 6c 65 73 3a 20 31 0d 0a	09/23/2022 8:15 AM: Nbr of files: 1	success or wait	1	165A8CF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E8738	ReadFile
\pipe	unknown	1024	success or wait	2	165A8CF	ReadFile
\pipe	unknown	1024	pipe broken	1	165A8CF	ReadFile

Analysis Process: chrome.exe PID: **3560**, Parent PID: **5928**

General

Target ID:	13
Start time:	08:14:57
Start date:	23/09/2022
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=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=3636 --field-trial-handle=1772,i,13935456055298204775,6851687727719502408,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: **6268**, Parent PID: **5928**

General

Target ID:	14
Start time:	08:14:58
Start date:	23/09/2022
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=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=6236 --field-trial-handle=1772,i,13935456055298204775,6851687727719502408,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: 7za.exe PID: **5912**, Parent PID: **2768**

General

Target ID:	15
Start time:	08:15:03
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip
Imagebase:	0x830000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e\SARS OUTSTANDING LETTER OF DEMAND.html	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	8363B0	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e\SARS OUTSTANDING LETTER OF DEMAND.html	0	32768	3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 6a 61 76 61 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 75 6e 65 73 63 61 70 65 28 27 25 33 43 73 63 72 69 70 74 25 32 30 6c 61 6e 67 75 61 67 65 25 33 44 6a 61 76 61 73 63 72 69 70 74 25 33 45 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 25 32 38 75 6e 65 73 63 61 70 65 25 32 38 25 32 37 25 32 35 30 41	<script language=javascr<wbr>ipt>document.write(unescape('%3Cscr<wbr>ipt%20language%3Djavascr<wbr>ipt%3Edocument.write%28unescape%28%27%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A	success or wait	1	836987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e\SARS OUTSTANDING LETTER OF DEMAND.html	32768	32768	51 79 30 79 77 6a 56 4c 47 53 55 69 68 77 36 55 41 4c 51 41 55 41 46 41 42 51 41 55 41 46 41	Qy0ywjVLGSUihw6UALQAUAFABQAUAFA	success or wait	17	836987	WriteFile
C:\Users\user\AppData\Local\Temp\fsnnqwuj.h1e\SARS OUTSTANDING LETTER OF DEMAND.html	589824	17662	38 39 41 46 79 48 56 63 34 2b 61 67 44 52 74 74 53 7a 6a 35 71 41 4e 69 30 76 63 34 2b 61 67 44 5a 74 62 6e 49 48 4e 41 47 70 42 4c 6e 46 41 46 31 48 34 6f 41 48 62 6a 72 51 42 54 6e 6b 77 44 51 42 6d 58 55 2b 4d 38 30 41 59 31 35 64 34 7a 7a 51 42 69 33 56 39 6a 50 4e 41 47 62 50 71 4f 50 34 71 41 4d 2b 58 55 2f 39 71 67 43 70 4c 71 76 2b 31 51 42 44 2f 61 33 50 33 71 41 4a 6f 39 56 36 66 4e 51 42 65 74 39 54 7a 6a 35 71 41 4e 65 30 76 38 34 2b 61 67 44 6f 62 43 36 33 41 63 30 41 62 74 72 4e 6e 48 4e 41 47 72 41 2b 52 51 42 65 69 4e 41 45 31 41 44 36 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41	89AFyHVc4+agDRttSzj5qANi0vc4+agDZtbnIHNAGpBLnFAF1H4oAHbjrQBTnkwDQBmXU+M80AY15d4zzQBi3V9jPNAGbPqOP4qAM+XU/9qgCpLqv+1QBD/a3P3qAJo9V6fNQBet9Tzj5qANe0v84+agDobC63Ac0AbtrNnHNAGrA+RQBeiNAE1AD6ACgAoAKACgAoAKACgAoAKACgAoAKACgAoAKACgAoA	success or wait	1	836987	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip	unknown	1024	success or wait	1	83686E	ReadFile
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip	unknown	131072	success or wait	1	83686E	ReadFile
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip	unknown	4	success or wait	1	83686E	ReadFile
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND.zip	unknown	4	success or wait	1	83686E	ReadFile

Analysis Process: conhost.exe PID: **7004**, Parent PID: **5912**

General

Target ID:	16
Start time:	08:15:04
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: unarchiver.exe PID: **1768**, Parent PID: **5928**

General

Target ID:	17
Start time:	08:15:33
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip
Imagebase:	0x620000
File size:	13312 bytes
MD5 hash:	9DE2E060A2985A232D8B96F9EC847A19
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Local\Temp\oluilyf2.xu4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	C2A999	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\unarchiver.log	1404	96	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 55 6e 70 61 63 6b 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 6f 77 6e 6c 6f 61 64 73 5c 53 41 52 53 20 4f 55 54 53 54 41 4e 44 49 4e 47 20 4c 45 54 54 45 52 20 4f 46 20 44 45 4d 41 4e 44 20 28 31 29 2e 7a 69 70 0d 0a	09/23/2022 8:15 AM: Unpack: C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip	success or wait	1	C2A8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	1500	77	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 54 6d 70 20 64 69 72 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6f 6c 75 69 6c 79 66 32 2e 78 75 34 0d 0a	09/23/2022 8:15 AM: Tmp dir: C:\Users\user\AppData\Local\Temp\oluilyf2.xu4	success or wait	1	C2A8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	1577	50	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 6f 75 74 3a 20 0d 0a	09/23/2022 8:15 AM: Received from standard out:	success or wait	16	C2A8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	2752	31	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 47 65 74 20 66 69 6c 65 73 0d 0a	09/23/2022 8:15 AM: Get files	success or wait	1	C2A8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	2783	37	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 4e 62 72 20 6f 66 20 66 69 6c 65 73 3a 20 31 0d 0a	09/23/2022 8:15 AM: Nbr of files: 1	success or wait	1	C2A8CF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E8738	ReadFile
\pipe	unknown	1024	success or wait	2	C2A8CF	ReadFile
\pipe	unknown	1024	pipe broken	1	C2A8CF	ReadFile

Analysis Process: 7za.exe PID: **4852**, Parent PID: **1768**

General

Target ID:	18
Start time:	08:15:34
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\oluilyf2.xu4" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip
Imagebase:	0x830000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\oluilyf2.xu4\SARS OUTSTANDING LETTER OF DEMAND.html	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	8363B0	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\oluilyf2.xu4\SARS OUTSTANDING LETTER OF DEMAND.html	0	32768	3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 6a 61 76 61 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 75 6e 65 73 63 61 70 65 28 27 25 33 43 73 63 72 69 70 74 25 32 30 6c 61 6e 67 75 61 67 65 25 33 44 6a 61 76 61 73 63 72 69 70 74 25 33 45 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 25 32 38 75 6e 65 73 63 61 70 65 25 32 38 25 32 37 25 32 35 30 41	<script language=javascr<wbr>ipt>document.write(unescape('%3Cscr<wbr>ipt%20language%3Djavascr<wbr>ipt%3Edocument.write%28unescape%28%27%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A	success or wait	1	836987	WriteFile
C:\Users\user\AppData\Local\Temp\oluilyf2.xu4\SARS OUTSTANDING LETTER OF DEMAND.html	32768	32768	51 79 30 79 77 6a 56 4c 47 53 55 69 68 77 36 55 41 4c 51 41 55 41 46 41 42 51 41 55 41 46 41	Qy0ywjVLGSUihw6UALQAUAFABQAUAFA	success or wait	17	836987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\oluilyf2.xu4\SARS OUTSTANDING LETTER OF DEMAND.html	589824	17662	38 39 41 46 79 48 56 63 34 2b 61 67 44 52 74 74 53 7a 6a 35 71 41 4e 69 30 76 63 34 2b 61 67 44 5a 74 62 6e 49 48 4e 41 47 70 42 4c 6e 46 41 46 31 48 34 6f 41 48 62 6a 72 51 42 54 6e 6b 77 44 51 42 6d 58 55 2b 4d 38 30 41 59 31 35 64 34 7a 7a 51 42 69 33 56 39 6a 50 4e 41 47 62 50 71 4f 50 34 71 41 4d 2b 58 55 2f 39 71 67 43 70 4c 71 76 2b 31 51 42 44 2f 61 33 50 33 71 41 4a 6f 39 56 36 66 4e 51 42 65 74 39 54 7a 6a 35 71 41 4e 65 30 76 38 34 2b 61 67 44 6f 62 43 36 33 41 63 30 41 62 74 72 4e 6e 48 4e 41 47 72 41 2b 52 51 42 65 69 4e 41 45 31 41 44 36 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41	89AFyHVc4+agDRttSzj5qANi0vc4+agDZtbnIHNAGpBLnFAF1H4oAHbjrQBTnkwDQBmXU+M80AY15d4zzQBi3V9jPNAGbPqOP4qAM+XU/9qgCpLqv+1QBD/a3P3qAJo9V6fNQBet9Tzj5qANe0v84+agDobC63Ac0AbtrNnHNAGrA+RQBeiNAE1AD6ACgAoAKACgAoAKACgAoAKACgAoAKACgAoAKACgAoAKACgAoAKACgAoA	success or wait	1	836987	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip	unknown	1024	success or wait	1	83686E	ReadFile
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip	unknown	131072	success or wait	1	83686E	ReadFile
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip	unknown	4	success or wait	1	83686E	ReadFile
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (1).zip	unknown	4	success or wait	1	83686E	ReadFile

Analysis Process: conhost.exe PID: **6420**, Parent PID: **4852**

General

Target ID:	19
Start time:	08:15:36
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: unarchiver.exe PID: **4788**, Parent PID: **5928**

General

Target ID:	20
Start time:	08:15:51
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\unarchiver.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip
Imagebase:	0xbb0000
File size:	13312 bytes
MD5 hash:	9DE2E060A2985A232D8B96F9EC847A19
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Local\Temp\evppz250.yan	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	15CA999	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\unarchiver.log	2820	96	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 55 6e 70 61 63 6b 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 6f 77 6e 6c 6f 61 64 73 5c 53 41 52 53 20 4f 55 54 53 54 41 4e 44 49 4e 47 20 4c 45 54 54 45 52 20 4f 46 20 44 45 4d 41 4e 44 20 28 32 29 2e 7a 69 70 0d 0a	09/23/2022 8:15 AM: Unpack: C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip	success or wait	1	15CA8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	2916	77	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 54 6d 70 20 64 69 72 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 65 76 70 70 7a 32 35 30 2e 79 61 6e 0d 0a	09/23/2022 8:15 AM: Tmp dir: C:\Users\user\AppData\Local\Temp\evppz250.yan	success or wait	1	15CA8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	2993	50	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 35 20 41 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 6f 75 74 3a 20 0d 0a	09/23/2022 8:15 AM: Received from standard out:	success or wait	16	15CA8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	4168	31	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 36 20 41 4d 3a 20 47 65 74 20 66 69 6c 65 73 0d 0a	09/23/2022 8:16 AM: Get files	success or wait	1	15CA8CF	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	4199	37	30 39 2f 32 33 2f 32 30 32 32 20 38 3a 31 36 20 41 4d 3a 20 4e 62 72 20 6f 66 20 66 69 6c 65 73 3a 20 31 0d 0a	09/23/2022 8:16 AM: Nbr of files: 1	success or wait	1	15CA8CF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E8738	ReadFile
\pipe	unknown	1024	success or wait	2	15CA8CF	ReadFile
\pipe	unknown	1024	pipe broken	1	15CA8CF	ReadFile

Analysis Process: 7za.exe PID: 7164, Parent PID: 4788

General

Target ID:	23
Start time:	08:15:53
Start date:	23/09/2022
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\evppz250.yan" "C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip
Imagebase:	0x830000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\evppz250.yan\SARS OUTSTANDING LETTER OF DEMAND.html	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	8363B0	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\evppz250.yan\SARS OUTSTANDING LETTER OF DEMAND.html	0	32768	3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 6a 61 76 61 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 75 6e 65 73 63 61 70 65 28 27 25 33 43 73 63 72 69 70 74 25 32 30 6c 61 6e 67 75 61 67 65 25 33 44 6a 61 76 61 73 63 72 69 70 74 25 33 45 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 25 32 38 75 6e 65 73 63 61 70 65 25 32 38 25 32 37 25 32 35 30 41	<script language=javascr<wbr>ipt>document.write(unescape('%3Cscr<wbr>ipt%20language%3Djavascr<wbr>ipt%3Edocument.write%28unescape%28%27%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A%250A	success or wait	1	836987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\evppz250.yan\SARS OUTSTANDING LETTER OF DEMAND.html	32768	32768	51 79 30 79 77 6a 56 4c 47 53 55 69 68 77 36 55 41 4c 51 41 55 41 46 41 42 51 41 55 41 46 41	Qy0ywjVLGSUihw6UALQ AUAFABQAUAF ABQAUAFABQAUAFAB QAUAFABQAUAFAB QAUAFABQAUAFABQA UAFABQAUAFABQA UAFABQAUAFABQAUA FABQAUAFABQAUA FABQAUAFABQAUAFA BQAUAFABQAUAFA BQAUAFABQAUAFABQ AUAFABQAUAFABQ AUAFABQAUAFABQAU AFABQAUAFABQAU AFABQAUAFABQAUAF ABQAUAFABQAUAF ABQAUAFABQAUAFA	success or wait	17	836987	WriteFile
C:\Users\user\AppData\Local\Temp\evppz250.yan\SARS OUTSTANDING LETTER OF DEMAND.html	589824	17662	38 39 41 46 79 48 56 63 34 2b 61 67 44 52 74 74 53 7a 6a 35 71 41 4e 69 30 76 63 34 2b 61 67 44 5a 74 62 6e 49 48 4e 41 47 70 42 4c 6e 46 41 46 31 48 34 6f 41 48 62 6a 72 51 42 54 6e 6b 77 44 51 42 6d 58 55 2b 4d 38 30 41 59 31 35 64 34 7a 7a 51 42 69 33 56 39 6a 50 4e 41 47 62 50 71 4f 50 34 71 41 4d 2b 58 55 2f 39 71 67 43 70 4c 71 76 2b 31 51 42 44 2f 61 33 50 33 71 41 4a 6f 39 56 36 66 4e 51 42 65 74 39 54 7a 6a 35 71 41 4e 65 30 76 38 34 2b 61 67 44 6f 62 43 36 33 41 63 30 41 62 74 72 4e 6e 48 4e 41 47 72 41 2b 52 51 42 65 69 4e 41 45 31 41 44 36 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41 4b 41 43 67 41 6f 41	89AFyHVc4+agDRttSzj5 qANi0vc4+a gDZtbnIHNAGpBLnFAF1 H4oAHbjrQBT nkwDQBmXU+M80AY15 d4zzQBi3V9jPN AGbPqOP4qAM+XU/9qg CpLqv+1QBD/a 3P3qAJo9V6fNQBet9Tzj 5qANe0v84+ agDobC63Ac0AbtrNnHN AGrA+RQBeiN AE1AD6ACgAoAKACgA oAKACgAoAKACg AoAKACgAoAKACgAoA KACgAoAKACgAo AKACgAoAKACgAoA	success or wait	1	836987	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip	unknown	1024	success or wait	1	83686E	ReadFile
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip	unknown	131072	success or wait	1	83686E	ReadFile
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip	unknown	4	success or wait	1	83686E	ReadFile
C:\Users\user\Downloads\SARS OUTSTANDING LETTER OF DEMAND (2).zip	unknown	4	success or wait	1	83686E	ReadFile

Analysis Process: conhost.exe PID: **5772**, Parent PID: **7164**

General

Target ID:	24
Start time:	08:15:55
Start date:	23/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly