ID: 756206
Sample Name: Remittance.html
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 20:12:04
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

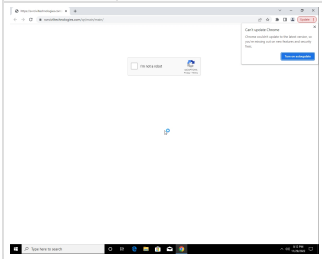
Windows Analysis Report

Remittance.html

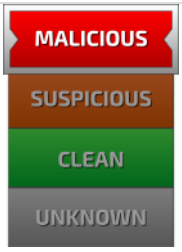
Overview

General Information

Sample Name:	Remittance.html
Analysis ID:	756206
MD5:	2e6a26923a22e7.
SHA1:	8f6857398dfe794.
SHA256:	6ff75a1daf291ab..
Infos:	



Detection



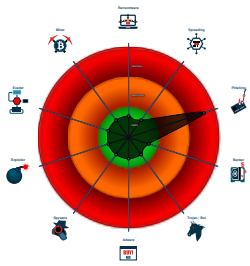
Captcha Phish, HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Yara detected Captcha Phish
- HTML document with suspicious na…
- JA3 SSL client fingerprint seen in co…
- HTML body contains low number of …
- Invalid T&C link found
- Suspicious form URL found
- IP address seen in connection with …
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 6760 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\Remittance.html MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6968 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=2056 --field-trial-handle=1812,i,8274798147493147586,16206874965015421851,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
73402.1.pages.csv	JoeSecurity_CaptchaPhish_1	Yara detected Captcha Phish	Joe Security	
39468.7.pages.csv	JoeSecurity_CaptchaPhish_1	Yara detected Captcha Phish	Joe Security	
94194.8.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Yara detected Captcha Phish

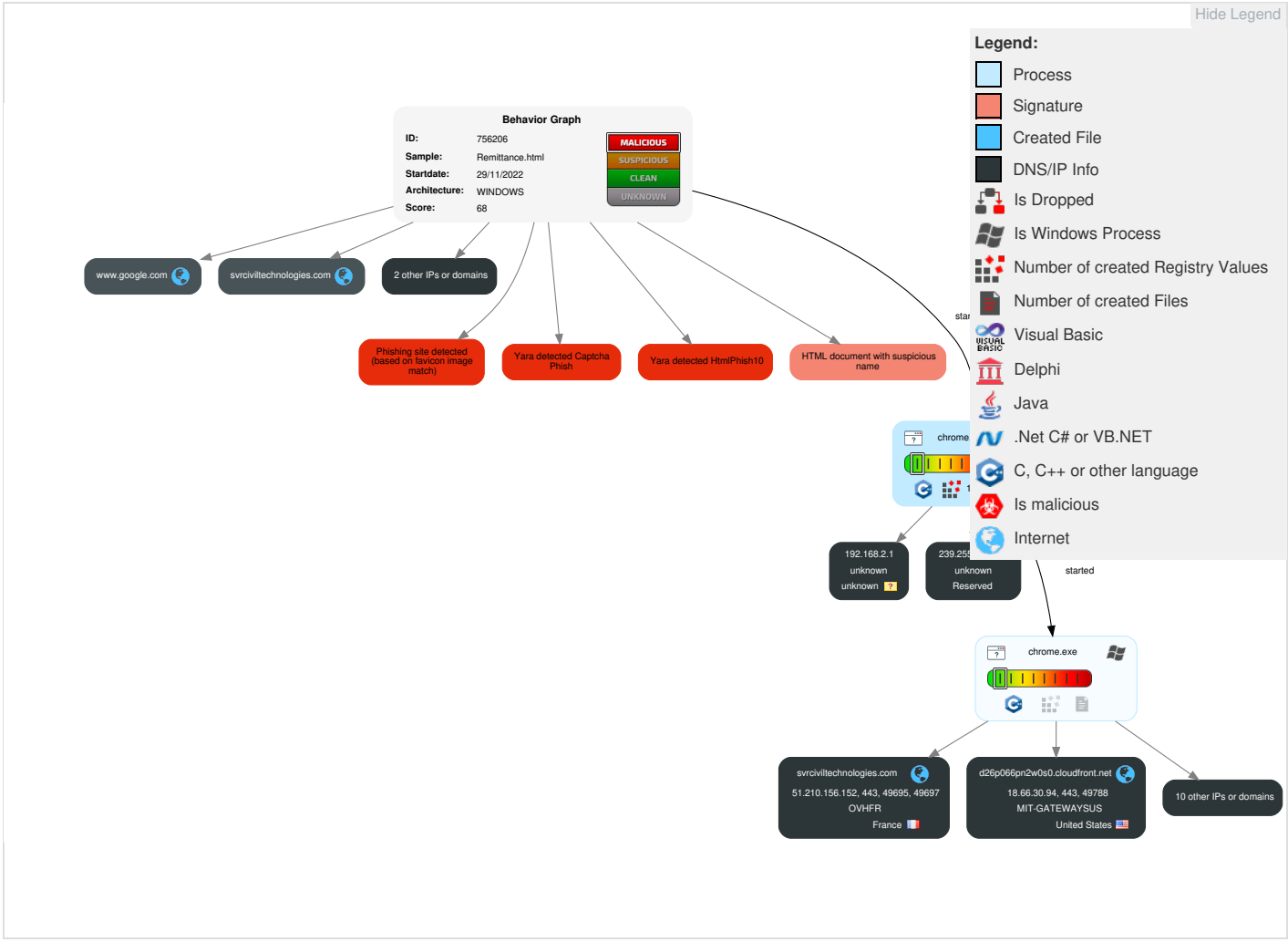
System Summary

HTML document with suspicious name

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	3 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)	1 Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 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	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

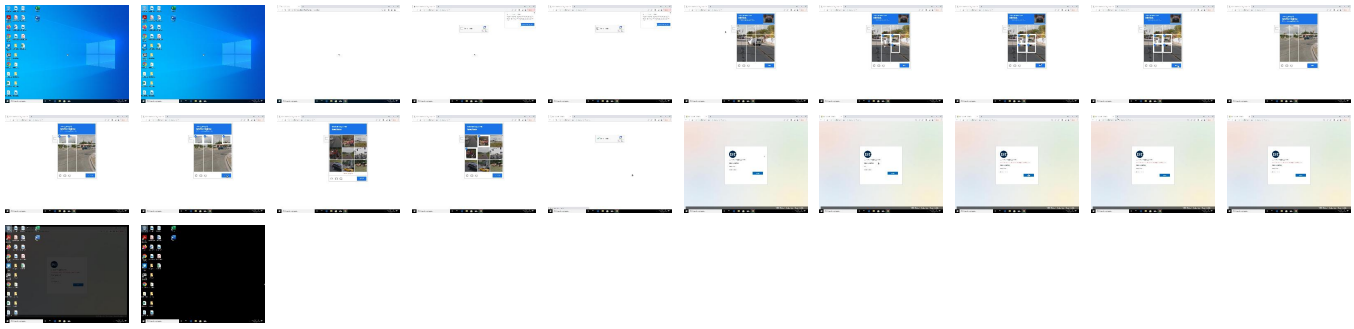
Behavior Graph

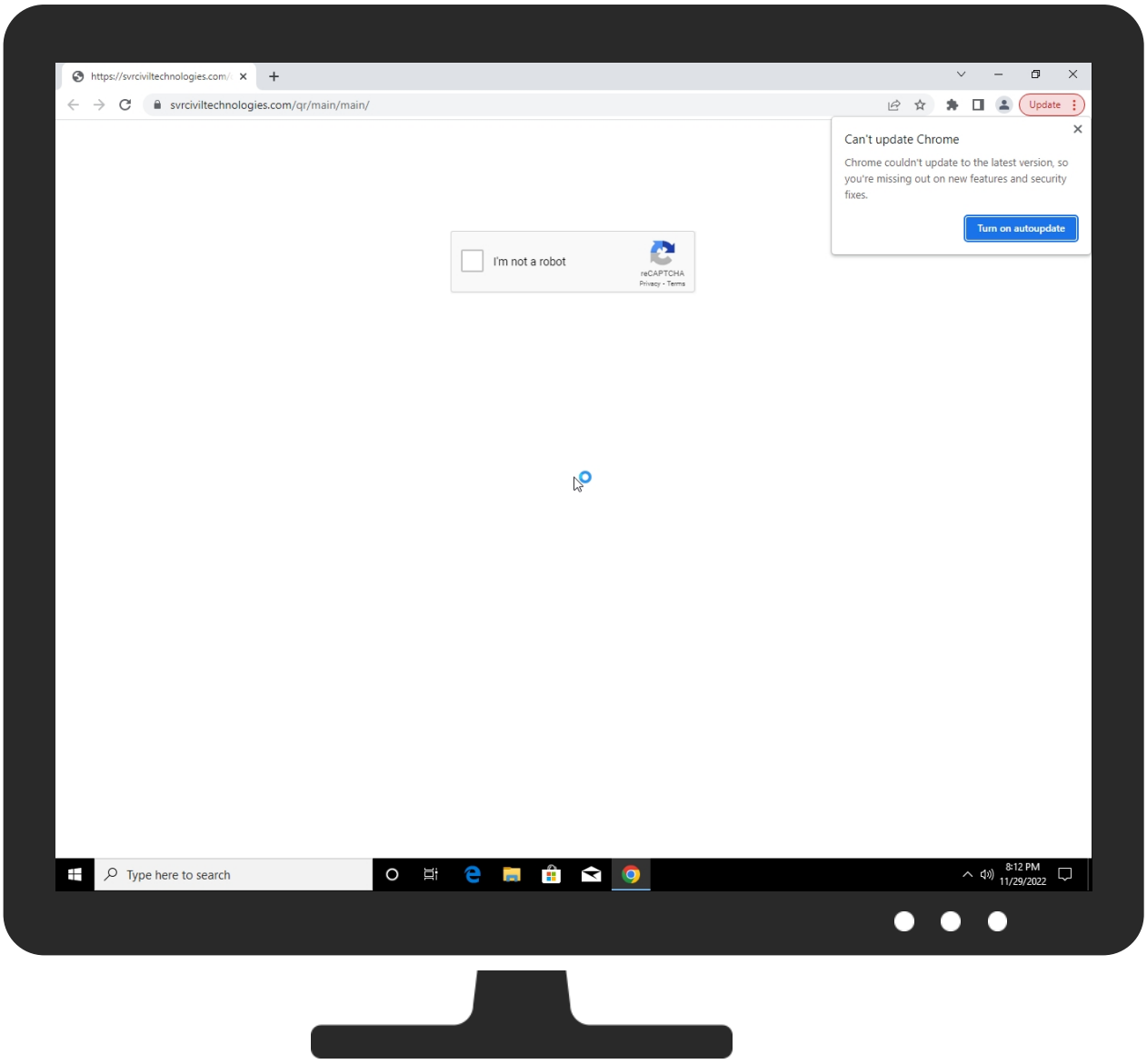


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://https://svrciviltechnologies.com/qr/main?e=?$	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/qr/main/?e=?Facilities@fsbwa.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://svrciviltechnologies.com/wp-content/uploads/2020/02/cropped-IMG-20200221-WA0039-removebg-preview-32x32.png	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/qr/main/main/css/bootstrap.min.css	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/qr/main?e=?Facilities@fsbwa.com	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/qr/main/main/action.php	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/qr/main/main/images/arrow.JPG	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/qr/main/main/images/ellipsis_white.svg	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/qr/main/main/images/bg.jpg	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/qr/main/main/css/style.css	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/qr/main/main/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://svrciviltechnologies.com/qr/main/main	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
d26p066pn2w0s0.cloudfront.net	18.66.30.94	true	false		high
accounts.google.com	142.250.186.109	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
svrciviltechnologies.com	51.210.156.152	true	false	• 0%, Virustotal, Browse	unknown
www.google.com	142.250.186.36	true	false		high
clients.l.google.com	142.250.186.110	true	false		high
clients2.google.com	unknown	unknown	false		high
logo.clearbit.com	unknown	unknown	false		high

Contacted URLs

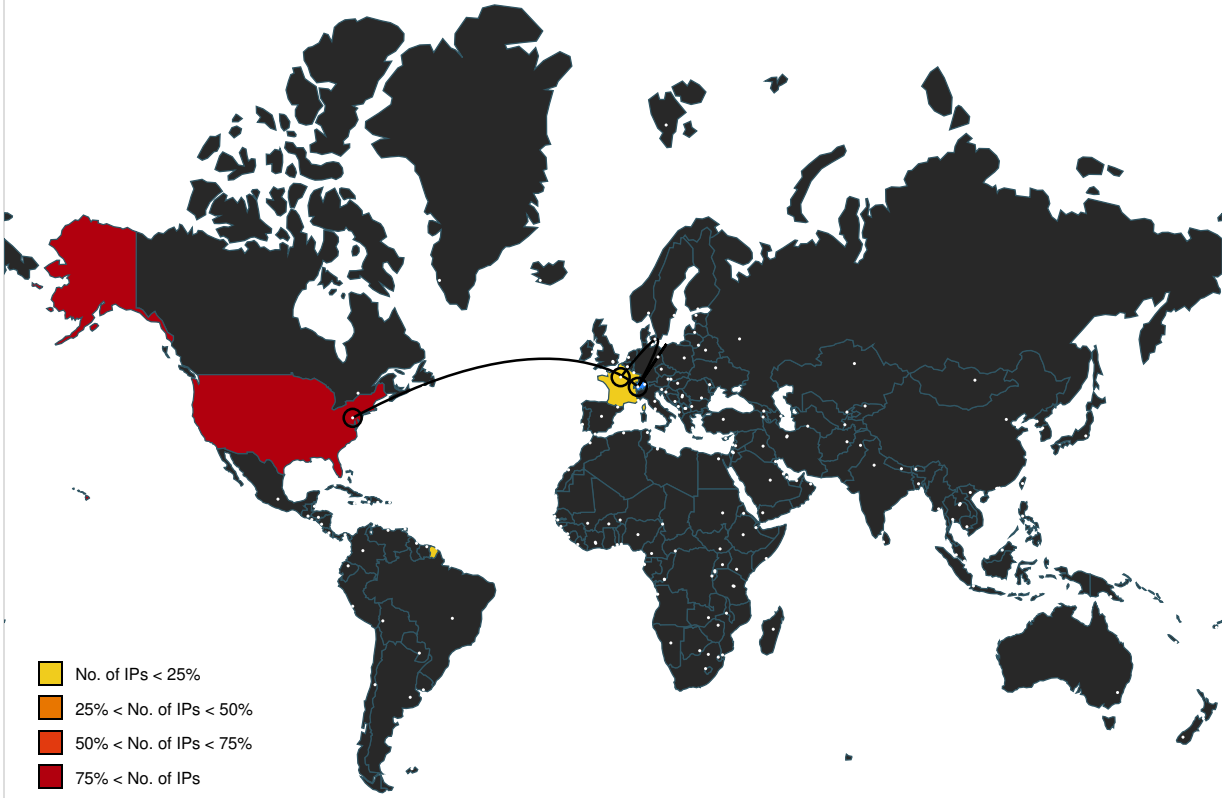
Name	Malicious	Antivirus Detection	Reputation
http://https://svrciviltechnologies.com/qr/main?e=?Facilities@fsbwa.com	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/recaptcha/api2/payload?p=06AEkXODD1_BdB7nrMCvTq-x5W-ERRA2trmCU7z6q9Ohx3TZJQz8IBQZNXRTpXomJG04OVLjYiuJG6KMWK7dDdEZVH3HfVlu5Y1MRSCWqvoYZyOTZAJPJBgVTzY1izWIeMWQ1DdNyNVyR64t3bez5sDMUahfW9fGzMqb09hVueealuKLbXoTcDUNKEKtPgqJx3qSMQ9726-FY5QGW7dHeOBTjK3VDzNLKONA&k=6LevKEMjAAAAACrP5tlDxBo0GwS2VQ_w4JoD2PKb&id=2	false		high
http://https://svrciviltechnologies.com/wp-content/uploads/2020/02/cropped-IMG-20200221-WA0039-removebg-preview-32x32.png	false	• Avira URL Cloud: safe	unknown
http://https://svrciviltechnologies.com/qr/main/main/	false		unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://svrciviltechnologies.com/qr/main/?e=?Facilities@fsbwa.com	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/recaptcha/api2/userverify?k=6LevKEMjAAAAACrP5tlDxBo0GwS2VQ_w4JoD2PKb	false		high
http://https://svrciviltechnologies.com/qr/main/main/css/bootstrap.min.css	false	• Avira URL Cloud: safe	unknown
http://https://svrciviltechnologies.com/qr/main/main/	false		unknown
http://https://svrciviltechnologies.com/qr/main/main/action.php	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=Km9gKuG06He-isPsP6saG8cn	false		high
http://https://www.google.com/recaptcha/api2/bframe?hl=en&v=Km9gKuG06He-isPsP6saG8cn&k=6LevKEMjAAAAACrP5tlDxBo0GwS2VQ_w4JoD2PKb	false		high
http://https://svrciviltechnologies.com/qr/main/main/images/arrow.JPG	false	• Avira URL Cloud: safe	unknown
http://https://svrciviltechnologies.com/qr/main/main/images/ellipsis_white.svg	false	• Avira URL Cloud: safe	unknown
http://https://svrciviltechnologies.com/qr/main/main/images/bg.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/recaptcha/api2/payload?p=06AEkXODDBsSDm1gZwjhI95pI5c4GaymKZ6r6Iw096p69astcTB3G4FXgfiittMYfFWq2EDjyd_PO35Xo8aQWy442eIPrtPQgRcERcH50_bB30vydG3nbQSKX-Ys3S96DPr2GptcX5QBPkLNhhGtPbu7tBPyA0sOZVjaV3W5rwHGPoNmQe61xiRIc3B4oq2HOuxGlnLHV9yMiv34I9yPITP684ylRSb7h2wg&k=6LevKEMjAAAAACrP5tlDxBo0GwS2VQ_w4JoD2PKb	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://svrciviltechnologies.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://svrciviltechnologies.com/qr/main/main/css/style.css	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/recaptcha/api.js	false		high
http://https://www.google.com/recaptcha/api2/replaceimage?k=6LevKEMjAAAAACrP5tlDxBo0GwS2VQ_w4JoD2PKb	false		high
http://https://svrciviltechnologies.com/qr/main/main/main.php	true		unknown
http://https://svrciviltechnologies.com/qr/main/main	false	• Avira URL Cloud: safe	unknown
http://https://logo.clearbit.com/fsbwa.com	false		high
http://https://svrciviltechnologies.com/qr/main/main/main.php	true		unknown
http://https://www.google.com/recaptcha/api2/bframe?hl=en&v=Km9gKuG06He-isPsP6saG8cn&k=6LevKEMjAAAAACrP5tlDxBo0GwS2VQ_w4JoD2PKb	false		high
http://https://www.google.com/recaptcha/api2/payload?p=06AEkXODD1_BdB7nrMCvTq-x5W-ERRA2trmCU7z6q9Ohx3TZJQz8IBQZNXRTpXomJG04OVLjYiuJG6KMWK7dDdEZVH3HfVlu5Y1MRSCWqvoYZyOTZAJPJBgVTzY1izWIeMWQ1DdNyNVyR64t3bez5sDMUahfW9fGzMqb09hVueealuKLbXoTcDUNKEKtPgqJx3qSMQ9726-FY5QGW7dHeOBTjK3VDzNLKONA&k=6LevKEMjAAAAACrP5tlDxBo0GwS2VQ_w4JoD2PKb	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js	false		high
http://https://www.google.com/recaptcha/api2/reload?k=6LevKEMjAAAAACrP5tlDxBo0GwS2VQ_w4JoD2PKb	false		high
http://https://svrciviltechnologies.com/qr/main/main/images/favicon.ico	false	• Avira URL Cloud: safe	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=104.0.5112.102&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://svrciviltechnologies.com/qr/main?e=?$	Remittance.html	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.36	www.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.109	accounts.google.com	United States		15169	GOOGLEUS	false
18.66.30.94	d26p066pn2w0s0.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.186.110	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.100	unknown	United States		15169	GOOGLEUS	false
51.210.156.152	svrciviltechnologies.com	France		16276	OVHFR	false
104.17.25.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756206
Start date and time:	2022-11-29 20:12:04 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Remittance.html
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	11
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:	mal68.phis.winHTML@25/0@16/12
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .html

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, SIHClient.exe, SgrmBroker.exe, usocoreworker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.185.227, 34.104.35.123, 142.250.74.195, 142.250.185.234, 142.250.185.74, 142.250.185.138, 172.217.16.202, 142.250.184.202, 142.250.186.170, 172.217.23.106, 142.250.181.234, 142.250.74.202, 142.250.186.74, 142.250.185.202, 142.250.184.234, 142.250.185.106, 172.217.18.106, 216.58.212.170, 142.250.186.106, 142.250.186.99, 142.250.186.67
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, login.live.com, slscr.update.microsoft.com, fonts.gstatic.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, www.gstatic.com
- Not all processes where analyzed, report is missing behavior 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

General

File type:	HTML document, ASCII text, with CRLF line terminators
Entropy (8bit):	5.197854157627124
TrID:	
File name:	Remittance.html
File size:	233
MD5:	2e6a26923a22e7c63a143e11227d4161
SHA1:	8f6857398dfe794b8853efc9e02d57b12a0b3da5
SHA256:	6ff75a1daf291abf72a3be2bb5034b0b0002ed90f7ea9c40ea84b66151fdae7e
SHA512:	2a5b70d18bf08f1fa879d908887be3979a10fa376ce1211355608fb53bc8a4a298ee8cf903d29f826e30f2a16a4f9ac2a28d8c2806c0b03d35addd4715c614d8
SSDEEP:	6:wAqJXlxY2FHLGVKIHpkRSmmHhX8Aha5V/YFmFb:1qZlxY2FHLGVTHJxHHhYJYsb
TLSH:	35D097D79F4280410A584B38C839720C867FAACA8488C280BE008430B304B85304A5D0
File Content Preview:	..<script type="text/JavaScript">.. var getEmail1blue93kmslxpcrypsoem375 = "Facilities@fsbwa.com";.. setTimeout(`location.href = "https://svrciviltechnologies.com/qr/main?e=?${getEmail1blue93kmslxpcrypsoem375}";`,0);..</script>

File Icon

Icon Hash:	78d0a8cccc88c460

Network Behavior

Network Port Distribution

Total Packets: 63

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:12:33.086762905 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.086852074 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.086971045 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.092322111 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.092401028 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.149174929 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.149266005 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.149377108 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.149662971 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.149698019 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.157419920 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.157919884 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.157973051 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.159832954 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.159992933 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.217818975 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.237140894 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.237196922 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.238073111 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.238173008 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.239106894 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.239176989 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.479337931 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.479412079 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.479798079 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.480190039 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.480230093 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.481317043 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.481370926 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.481611967 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.481626987 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.481673956 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.512403011 CET	443	49694	142.250.186.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:12:33.512505054 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.512548923 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.512739897 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.512814999 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.520035982 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.530101061 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.530306101 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.530359983 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.530601025 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.530689001 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.552190065 CET	49694	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:12:33.552248001 CET	443	49694	142.250.186.110	192.168.2.3
Nov 29, 2022 20:12:33.554096937 CET	49693	443	192.168.2.3	142.250.186.109
Nov 29, 2022 20:12:33.554158926 CET	443	49693	142.250.186.109	192.168.2.3
Nov 29, 2022 20:12:33.677503109 CET	49695	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.677580118 CET	443	49695	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.677678108 CET	49695	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.678047895 CET	49695	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.678081036 CET	443	49695	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.784603119 CET	443	49695	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.785001993 CET	49695	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.785056114 CET	443	49695	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.786698103 CET	443	49695	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.786813974 CET	49695	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.790435076 CET	49695	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.790461063 CET	443	49695	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.790599108 CET	443	49695	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.790900946 CET	49695	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.790926933 CET	443	49695	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.818737030 CET	443	49695	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.818859100 CET	49695	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.819951057 CET	49695	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.819993019 CET	443	49695	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.825476885 CET	49697	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.825545073 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.825654984 CET	49697	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.825920105 CET	49697	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.825944901 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.890141964 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.890667915 CET	49697	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.890723944 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.891841888 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.893455029 CET	49697	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.893491030 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.893672943 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.894561052 CET	49697	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.894587994 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.984378099 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.984550953 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.984699965 CET	49697	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.986706972 CET	49697	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.986767054 CET	443	49697	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.986799955 CET	49697	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.986864090 CET	49697	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.989290953 CET	49698	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.989372015 CET	443	49698	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:33.989511013 CET	49698	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.989870071 CET	49698	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:33.989907026 CET	443	49698	51.210.156.152	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:12:34.053966045 CET	443	49698	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:34.058917999 CET	49698	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:34.058970928 CET	443	49698	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:34.060384035 CET	443	49698	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:34.061180115 CET	49698	443	192.168.2.3	51.210.156.152
Nov 29, 2022 20:12:34.061218977 CET	443	49698	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:34.061427116 CET	443	49698	51.210.156.152	192.168.2.3
Nov 29, 2022 20:12:34.061430931 CET	49698	443	192.168.2.3	51.210.156.152

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:12:32.976474047 CET	51023	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:12:32.977266073 CET	54763	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:12:32.999924898 CET	53	54763	1.1.1.1	192.168.2.3
Nov 29, 2022 20:12:33.000973940 CET	53	51023	1.1.1.1	192.168.2.3
Nov 29, 2022 20:12:33.308947086 CET	62638	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:12:33.645998001 CET	53	62638	1.1.1.1	192.168.2.3
Nov 29, 2022 20:12:34.381998062 CET	63322	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:12:34.382460117 CET	58985	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:12:34.400212049 CET	53	63322	1.1.1.1	192.168.2.3
Nov 29, 2022 20:12:34.400271893 CET	53	58985	1.1.1.1	192.168.2.3
Nov 29, 2022 20:12:36.845753908 CET	50766	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:12:36.863856077 CET	53	50766	1.1.1.1	192.168.2.3
Nov 29, 2022 20:12:42.473360062 CET	50247	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:12:42.491353035 CET	53	50247	1.1.1.1	192.168.2.3
Nov 29, 2022 20:13:05.908955097 CET	52038	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:13:05.909578085 CET	64945	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:13:05.910286903 CET	60102	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:13:05.927324057 CET	53	52038	1.1.1.1	192.168.2.3
Nov 29, 2022 20:13:05.927372932 CET	53	64945	1.1.1.1	192.168.2.3
Nov 29, 2022 20:13:05.929004908 CET	53	60102	1.1.1.1	192.168.2.3
Nov 29, 2022 20:13:08.067141056 CET	63871	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:13:08.076219082 CET	51506	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:13:08.095467091 CET	53	51506	1.1.1.1	192.168.2.3
Nov 29, 2022 20:13:08.114634991 CET	53	63871	1.1.1.1	192.168.2.3
Nov 29, 2022 20:13:36.902061939 CET	56179	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:13:36.921783924 CET	53	56179	1.1.1.1	192.168.2.3
Nov 29, 2022 20:13:36.925021887 CET	64272	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:13:36.942826986 CET	53	64272	1.1.1.1	192.168.2.3
Nov 29, 2022 20:13:43.427619934 CET	59693	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:13:43.427620888 CET	56670	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:13:43.445946932 CET	53	59693	1.1.1.1	192.168.2.3
Nov 29, 2022 20:13:43.473213911 CET	53	56670	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 20:12:32.976474047 CET	192.168.2.3	1.1.1.1	0x8e3f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:32.977266073 CET	192.168.2.3	1.1.1.1	0x5d4c	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:33.308947086 CET	192.168.2.3	1.1.1.1	0x78d5	Standard query (0)	svrcivilte chnologies.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:34.381998062 CET	192.168.2.3	1.1.1.1	0x6fad	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:34.382460117 CET	192.168.2.3	1.1.1.1	0xd723	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:36.845753908 CET	192.168.2.3	1.1.1.1	0xad83	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 20:12:42.473360062 CET	192.168.2.3	1.1.1.1	0x972a	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:05.908955097 CET	192.168.2.3	1.1.1.1	0xa468	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:05.909578085 CET	192.168.2.3	1.1.1.1	0xae3a	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:05.910286903 CET	192.168.2.3	1.1.1.1	0xb736	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:08.067141056 CET	192.168.2.3	1.1.1.1	0xa503	Standard query (0)	svrcivilte chnologies.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:08.076219082 CET	192.168.2.3	1.1.1.1	0x2915	Standard query (0)	logo.clearbit.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:36.902061939 CET	192.168.2.3	1.1.1.1	0x509d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:36.925021887 CET	192.168.2.3	1.1.1.1	0xf0c2	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:43.427619934 CET	192.168.2.3	1.1.1.1	0xa852	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:43.427620888 CET	192.168.2.3	1.1.1.1	0x1408	Standard query (0)	svrcivilte chnologies.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
Nov 29, 2022 20:12:32.999924898 CET	1.1.1.1	192.168.2.3	0x5d4c	No error (0)	accounts.google.com		142.250.186.109	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:33.000973940 CET	1.1.1.1	192.168.2.3	0x8e3f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:12:33.000973940 CET	1.1.1.1	192.168.2.3	0x8e3f	No error (0)	clients.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:33.645998001 CET	1.1.1.1	192.168.2.3	0x78d5	No error (0)	svrcivilte chnologies.com		51.210.156.152	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:34.400212049 CET	1.1.1.1	192.168.2.3	0x6fad	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:34.400212049 CET	1.1.1.1	192.168.2.3	0x6fad	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:34.400271893 CET	1.1.1.1	192.168.2.3	0xd723	No error (0)	www.google.com		142.250.186.36	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:36.863856077 CET	1.1.1.1	192.168.2.3	0xad83	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:12:42.491353035 CET	1.1.1.1	192.168.2.3	0x972a	No error (0)	www.google.com		142.250.186.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:05.927324057 CET	1.1.1.1	192.168.2.3	0xa468	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:05.927324057 CET	1.1.1.1	192.168.2.3	0xa468	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:05.927372932 CET	1.1.1.1	192.168.2.3	0xae3a	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:05.927372932 CET	1.1.1.1	192.168.2.3	0xae3a	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:05.929004908 CET	1.1.1.1	192.168.2.3	0xb736	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:13:05.929004908 CET	1.1.1.1	192.168.2.3	0xb736	No error (0)	d26p066pn2w0s0.cloudfront.net		18.66.30.94	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:05.929004908 CET	1.1.1.1	192.168.2.3	0xb736	No error (0)	d26p066pn2w0s0.cloudfront.net		18.66.30.77	A (IP address)	IN (0x0001)	false

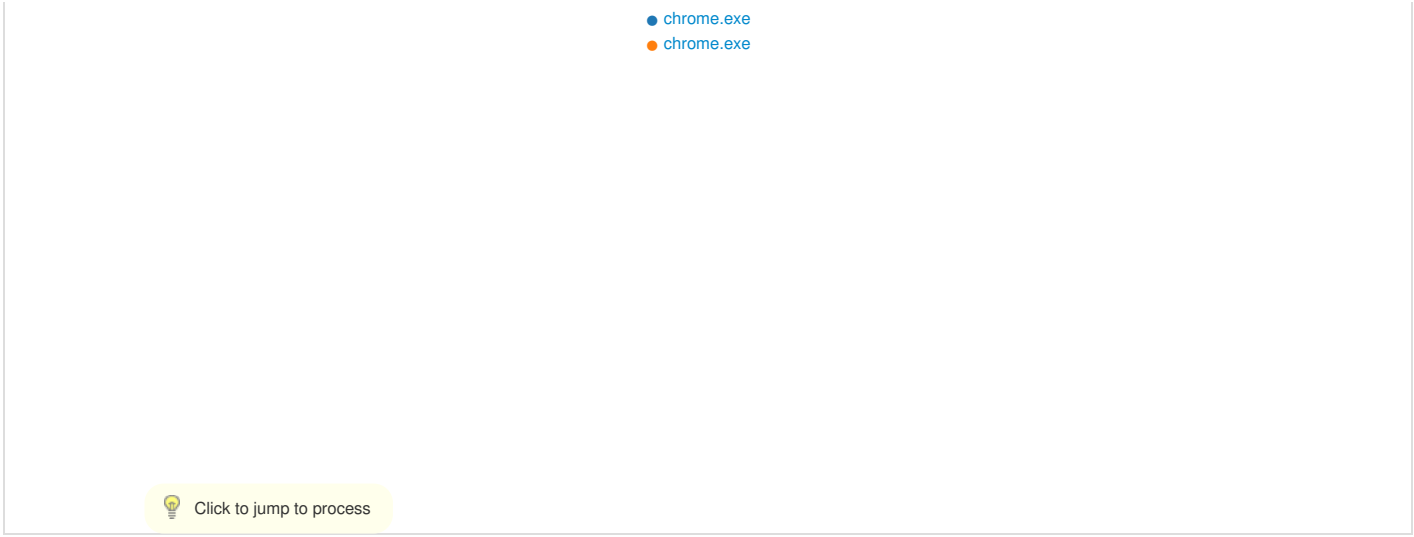
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 20:13:05.929004908 CET	1.1.1.1	192.168.2.3	0xb736	No error (0)	d26p066pn2w0s0.cloudfront.net		18.66.30.32	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:05.929004908 CET	1.1.1.1	192.168.2.3	0xb736	No error (0)	d26p066pn2w0s0.cloudfront.net		18.66.30.111	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:08.095467091 CET	1.1.1.1	192.168.2.3	0x2915	No error (0)	logo.clearbit.com	d26p066pn2w0s0.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:13:08.095467091 CET	1.1.1.1	192.168.2.3	0x2915	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.189.78	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:08.095467091 CET	1.1.1.1	192.168.2.3	0x2915	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.189.9	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:08.095467091 CET	1.1.1.1	192.168.2.3	0x2915	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.189.75	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:08.095467091 CET	1.1.1.1	192.168.2.3	0x2915	No error (0)	d26p066pn2w0s0.cloudfront.net		13.224.189.91	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:08.114634991 CET	1.1.1.1	192.168.2.3	0xa503	No error (0)	svrcivilte chnologies .com		51.210.156.152	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:36.921783924 CET	1.1.1.1	192.168.2.3	0x509d	No error (0)	www.google .com		142.250.185.196	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:36.942826986 CET	1.1.1.1	192.168.2.3	0xf0c2	No error (0)	www.google .com		142.250.186.100	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:43.445946932 CET	1.1.1.1	192.168.2.3	0xa852	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:43.445946932 CET	1.1.1.1	192.168.2.3	0xa852	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:13:43.473213911 CET	1.1.1.1	192.168.2.3	0x1408	No error (0)	svrcivilte chnologies .com		51.210.156.152	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- svrciviltechnologies.com
- https:
  - stackpath.bootstrapcdn.com
  - www.google.com
  - cdnjs.cloudflare.com
  - maxcdn.bootstrapcdn.com
  - logo.clearbit.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6760**, Parent PID: **3800**

General

Target ID:	0
Start time:	20:12:30
Start date:	29/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\Remittance.html
Imagebase:	0x7ff6566b0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

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

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

Analysis Process: chrome.exe PID: **6968**, Parent PID: **6760**

General

Target ID:	2
Start time:	20:12:31
Start date:	29/11/2022
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=2056 --field-trial-handle=1812,i,8274798147493147586,16206874965015421851,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6566b0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Disassembly

No disassembly