ID: 756113
Sample Name: Payslip 28.11.22.html
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 16:45:13
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

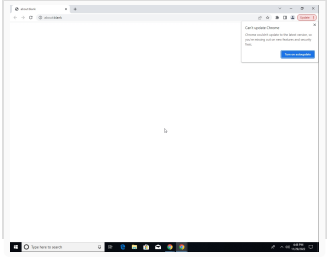
Windows Analysis Report

Payslip 28.11.22.html

Overview

General Information

Sample Name:	Payslip 28.11.22.html
Analysis ID:	756113
MD5:	b10534ae0a0f18..
SHA1:	aaf347a354f63f7..
SHA256:	808131c12aff58f..
Tags:	html
Infos:	



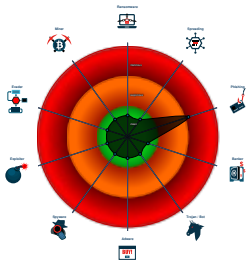
Detection

Score:	21
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on im…
- JA3 SSL client fingerprint seen in co…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4796 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6036 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=1960 --field-trial-handle=1748,i,8435815585756977 43,11274918621816804293,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 1504 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\Payslip 28.11.22.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

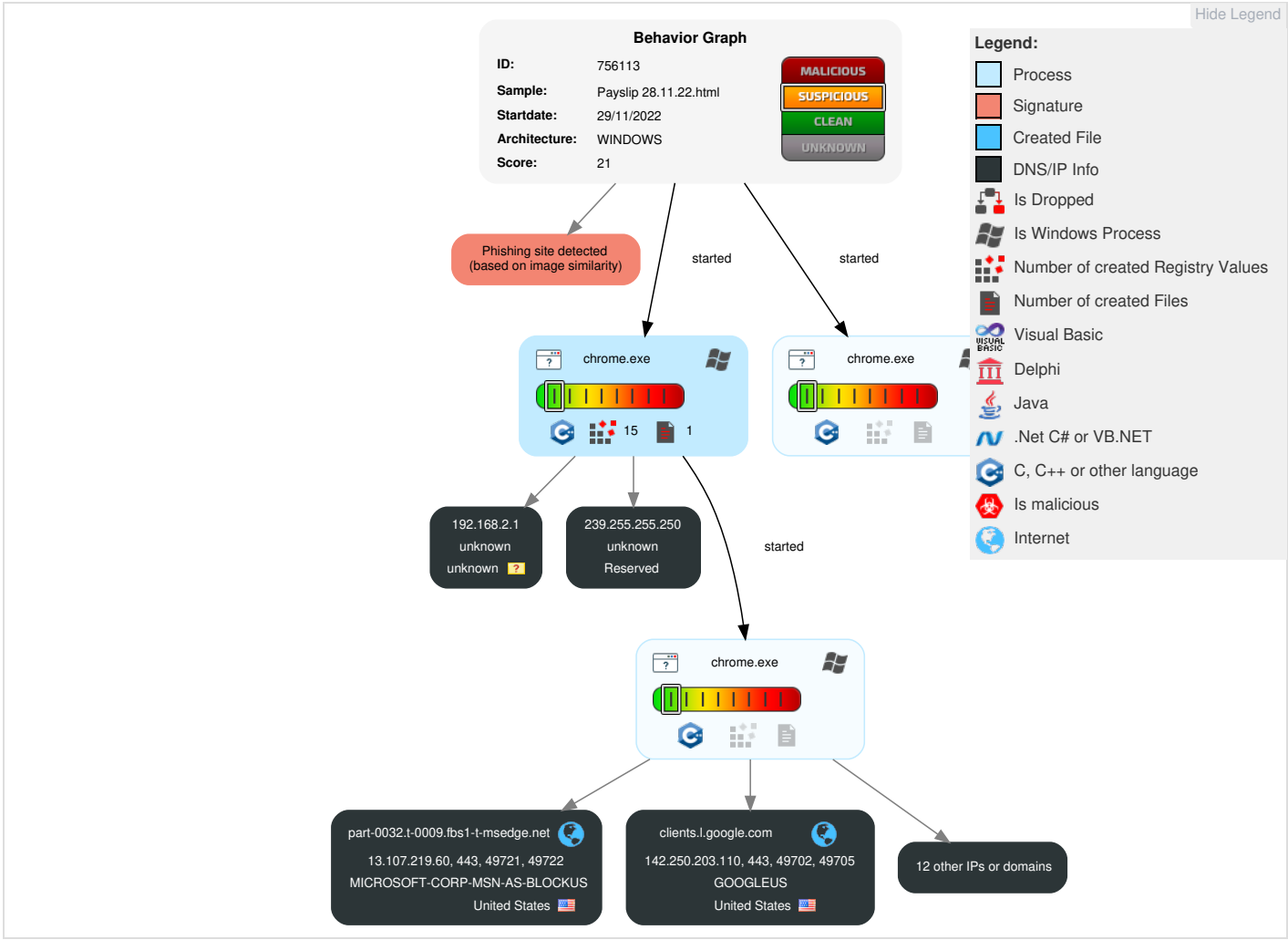
Phishing

Phishing site detected (based on image similarity)

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)	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

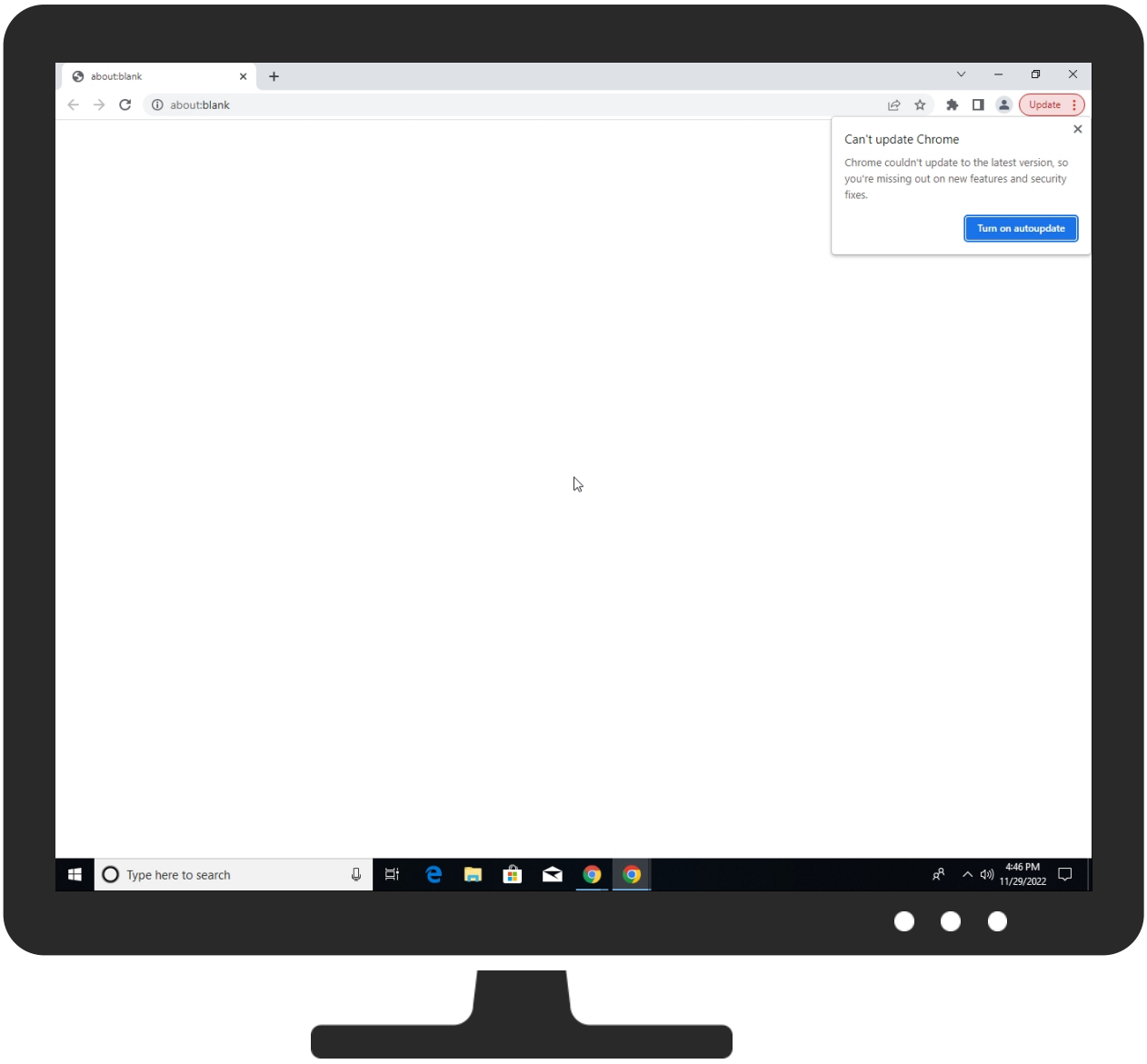
Behavior Graph



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

Source	Detection	Scanner	Label	Link
Payslip 28.11.22.html	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
socialgrow.co.in	0%	Virustotal		Browse
cs1227.wpc.alphacdn.net	0%	Virustotal		Browse
part-0032.t-0009.fbs1-t-msedge.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://socialgrow.co.in/tech/host9/admin/js/mj.php?ar=d29yZA==	0%	Avira URL Cloud	safe	
http://https://socialgrow.co.in/tech/host9/9c80cd4.php	0%	Avira URL Cloud	safe	

Domains and IPs

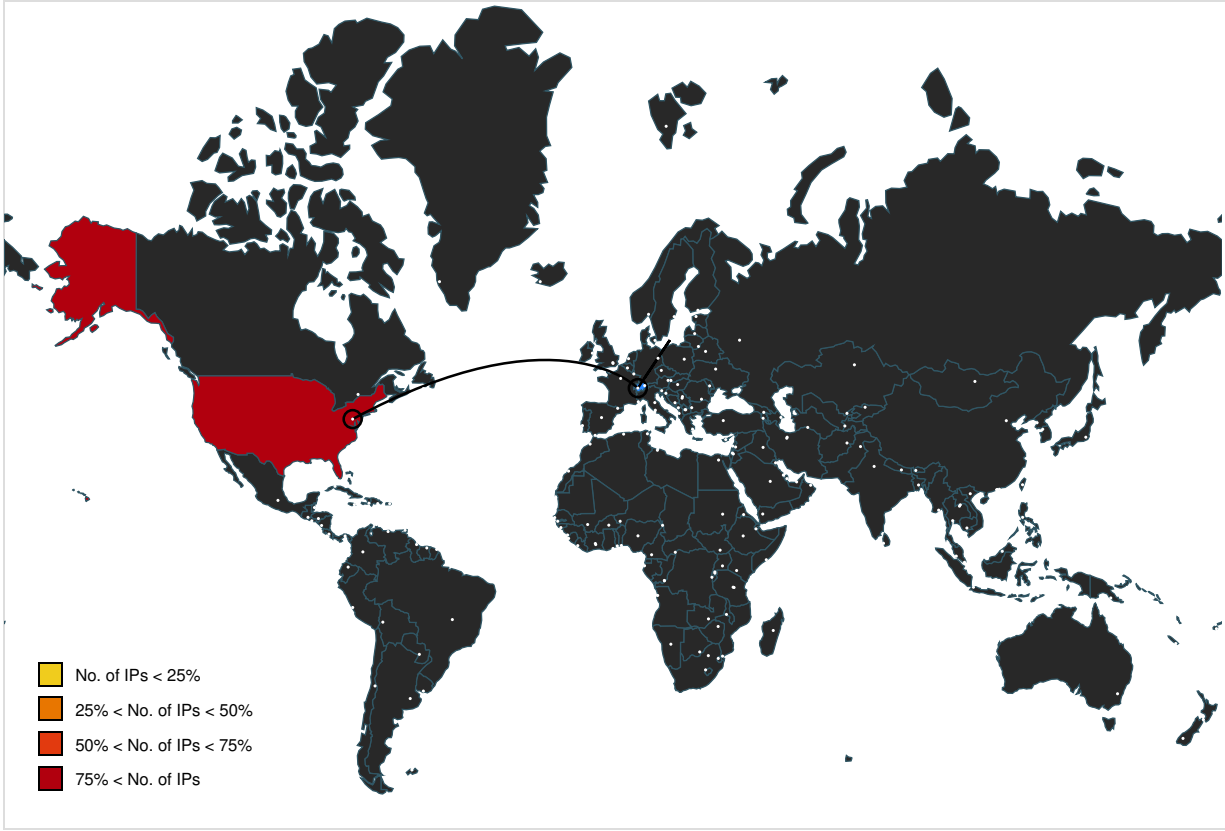
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
socialgrow.co.in	65.21.127.94	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
www.google.com	172.217.168.36	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false	• 0%, Virustotal, Browse	unknown
clients.l.google.com	142.250.203.110	true	false		high
part-0032.t-0009.fbs1-t-msedge.net	13.107.219.60	true	false	• 0%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
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://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	false		high
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.woff2?v=4.7.0	false		high
file:///C:/Users/user/Desktop/Payslip%2028.11.22.html	false		low
http://https://socialgrow.co.in/tech/host9/admin/js/mj.php?ar=d29yZA==	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://socialgrow.co.in/tech/host9/9c80cd4.php	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.21.127.94	socialgrow.co.in	United States		199592	CP-ASDE	false
13.107.219.60	part-0032.t-0009.fbs1-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	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:	756113
Start date and time:	2022-11-29 16:45:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payslip 28.11.22.html
Cookbook file name:	defaultwindowshtmlcookbook.jbs
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:	17

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:	SUS
Classification:	sus21.phis.winHTML@28/0@9/11
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 • Browse: https://privacy.microsoft.com/fr/privacystatement

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 34.104.35.123, 104.16.86.20, 104.16.85.20, 104.16.87.20, 104.16.88.20, 104.16.89.20, 69.16.175.10, 69.16.175.42
- Excluded domains from analysis (whitelisted): logincdn.msauth.net, cdn.jsdelivr.net.cdn.cloudflare.net, cds.s5x3j6q5.hwcdn.net, fs.microsoft.com, aadcdnoriginwus2.azureedge.net, lgincdnvzeuno.ec.azureedge.net, clientservices.googleapis.com, aadcdn.msauth.net, firstparty-azurefd-prod.trafficmanager.net, lgincdnvzeuno.azureedge.net, edgedl.me.gvt1.com, logincdn.trafficmanager.net, update.googleapis.com, aadcdnoriginwus2.afd.azureedge.net, global-entry-afdthirdparty-fallback.trafficmanager.net
- 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

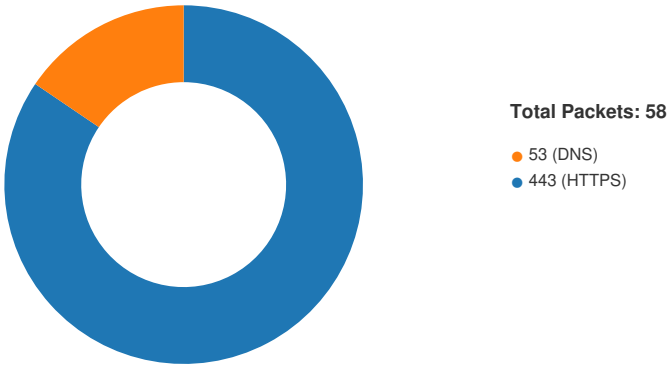
Static File Info

General

File type:	HTML document, ASCII text, with very long lines (616), with CRLF line terminators
Entropy (8bit):	5.41578686683262
TrID:	• HyperText Markup Language (12001/1) 66.65% • HyperText Markup Language (6006/1) 33.35%
File name:	Payslip 28.11.22.html
File size:	1639
MD5:	b10534ae0a0f1898d66dc74203e858a1
SHA1:	aaf347a354f63f7192bbe436401f4228251a1b82
SHA256:	808131c12aff58fce72de031c64535333f0b6a171bfcebd45732587487447cfd
SHA512:	47521d043fbe5478154e27ba4289b66c5ccbd506a75d059279f968cf418ba489f8a7001715b6f72fac9b3a2ee728e6705af9ed70c98f7662df0f7bcea82fc8a1
SSDEEP:	24:DwK1VaODNXKCQwQkpi6c9P/IwkMPtNcz4rMR5dH5kVQozr31HPSTi6fgxkW1zYMf:D7aODxtQo3MPt2ErgaeozdaN6kwzPf
TLSH:	BD315F3590339D3188A34CB8B4C5AF2E209EC109CB0658452AE88CEB67E7C460266EE9
File Content Preview:	<html>..<head>..</head>..<body>.. <label for="price_per_item" class="font-weight-bold">PriceB 5.00 % discount</label><input

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:46:11.793051004 CET	49701	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:11.793107986 CET	443	49701	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:11.793231964 CET	49701	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:11.797557116 CET	49702	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:11.797610044 CET	443	49702	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:11.797708988 CET	49702	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:11.799981117 CET	49704	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:11.800015926 CET	443	49704	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:11.800105095 CET	49704	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:11.800843954 CET	49705	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:11.800873041 CET	443	49705	142.250.203.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:46:11.800957918 CET	49705	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:11.802480936 CET	49701	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:11.802505016 CET	443	49701	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:11.803487062 CET	49702	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:11.803529024 CET	443	49702	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:11.858628988 CET	443	49701	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:11.872416019 CET	443	49702	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:11.903265953 CET	49701	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:11.915292978 CET	49702	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:12.126543999 CET	49704	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:12.126569986 CET	443	49704	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:12.126974106 CET	49705	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:12.127000093 CET	443	49705	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:12.127907991 CET	49702	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:12.127950907 CET	443	49702	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:12.128423929 CET	49701	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:12.128454924 CET	443	49701	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:12.129081011 CET	443	49702	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:12.129162073 CET	49702	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:12.131283045 CET	443	49701	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:12.131364107 CET	49701	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:12.131558895 CET	443	49702	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:12.131623030 CET	49702	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:12.213440895 CET	443	49705	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:12.235071898 CET	443	49704	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:12.303354979 CET	49704	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:12.315280914 CET	49705	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:12.956907988 CET	49707	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:12.956967115 CET	443	49707	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:12.957055092 CET	49707	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:12.957256079 CET	49704	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:12.957315922 CET	443	49704	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:12.958776951 CET	443	49704	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:12.958842993 CET	443	49704	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:12.958869934 CET	49704	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:12.972431898 CET	49705	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:12.972459078 CET	443	49705	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:12.972970963 CET	443	49705	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:12.972987890 CET	443	49705	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:12.973037004 CET	49705	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:12.973882914 CET	443	49705	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:12.973926067 CET	49705	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:13.000307083 CET	49704	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:13.095467091 CET	49708	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.095529079 CET	443	49708	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.095632076 CET	49708	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.096370935 CET	49707	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.096390963 CET	443	49707	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.099550009 CET	49708	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.099560976 CET	443	49708	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.186755896 CET	443	49707	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.194175005 CET	443	49708	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.315391064 CET	49708	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.386915922 CET	443	49707	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.387162924 CET	49707	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.536859989 CET	49708	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.536899090 CET	443	49708	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.537621975 CET	49702	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:13.537669897 CET	443	49702	142.250.203.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:46:13.538238049 CET	49705	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:13.538269997 CET	443	49705	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:13.538443089 CET	443	49705	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:13.538600922 CET	49707	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.538621902 CET	443	49707	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.538897038 CET	49701	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:13.538921118 CET	443	49701	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:13.539005041 CET	49704	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:13.539033890 CET	443	49704	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:13.539132118 CET	443	49701	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:13.539232969 CET	443	49704	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:13.539242029 CET	443	49708	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.539280891 CET	443	49708	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.539316893 CET	49708	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.539470911 CET	443	49702	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:13.540003061 CET	443	49707	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.540082932 CET	49707	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.594898939 CET	49702	443	192.168.2.3	142.250.203.110
Nov 29, 2022 16:46:13.594954014 CET	443	49702	142.250.203.110	192.168.2.3
Nov 29, 2022 16:46:13.595103025 CET	49708	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.595149994 CET	443	49708	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.595500946 CET	49707	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.595541954 CET	443	49707	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.595642090 CET	49701	443	192.168.2.3	172.217.168.45
Nov 29, 2022 16:46:13.595675945 CET	443	49701	172.217.168.45	192.168.2.3
Nov 29, 2022 16:46:13.595767975 CET	443	49707	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.595818996 CET	443	49708	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.596684933 CET	49708	443	192.168.2.3	65.21.127.94
Nov 29, 2022 16:46:13.596707106 CET	443	49708	65.21.127.94	192.168.2.3
Nov 29, 2022 16:46:13.600385904 CET	49704	443	192.168.2.3	172.217.168.45

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:46:10.590328932 CET	57840	53	192.168.2.3	8.8.8.8
Nov 29, 2022 16:46:10.592724085 CET	52387	53	192.168.2.3	8.8.8.8
Nov 29, 2022 16:46:10.609754086 CET	53	57840	8.8.8.8	192.168.2.3
Nov 29, 2022 16:46:10.620765924 CET	53	52387	8.8.8.8	192.168.2.3
Nov 29, 2022 16:46:12.063255072 CET	60625	53	192.168.2.3	8.8.8.8
Nov 29, 2022 16:46:12.117599010 CET	53	60625	8.8.8.8	192.168.2.3
Nov 29, 2022 16:46:13.598861933 CET	53975	53	192.168.2.3	8.8.8.8
Nov 29, 2022 16:46:13.627137899 CET	53	53975	8.8.8.8	192.168.2.3
Nov 29, 2022 16:46:13.939086914 CET	60582	53	192.168.2.3	8.8.8.8
Nov 29, 2022 16:46:13.958861113 CET	53	60582	8.8.8.8	192.168.2.3
Nov 29, 2022 16:46:13.989461899 CET	57134	53	192.168.2.3	8.8.8.8
Nov 29, 2022 16:46:14.003297091 CET	62050	53	192.168.2.3	8.8.8.8
Nov 29, 2022 16:46:15.197282076 CET	57704	53	192.168.2.3	8.8.8.8
Nov 29, 2022 16:46:15.219022989 CET	53	57704	8.8.8.8	192.168.2.3
Nov 29, 2022 16:48:13.587235928 CET	53049	53	192.168.2.3	8.8.8.8
Nov 29, 2022 16:48:13.606765032 CET	53	53049	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:46:10.590328932 CET	192.168.2.3	8.8.8.8	0x73d	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:10.592724085 CET	192.168.2.3	8.8.8.8	0xc9c5	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:12.063255072 CET	192.168.2.3	8.8.8.8	0xb93d	Standard query (0)	socialgrow.co.in	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:46:13.598861933 CET	192.168.2.3	8.8.8.8	0x49ec	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:13.939086914 CET	192.168.2.3	8.8.8.8	0x8257	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:13.989461899 CET	192.168.2.3	8.8.8.8	0xd98d	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:14.003297091 CET	192.168.2.3	8.8.8.8	0x40ae	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:15.197282076 CET	192.168.2.3	8.8.8.8	0xb07d	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:48:13.587235928 CET	192.168.2.3	8.8.8.8	0x1ee2	Standard query (0)	www.google.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 16:46:10.609754086 CET	8.8.8.8	192.168.2.3	0x73d	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:46:10.609754086 CET	8.8.8.8	192.168.2.3	0x73d	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:10.620765924 CET	8.8.8.8	192.168.2.3	0xc9c5	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:12.117599010 CET	8.8.8.8	192.168.2.3	0xb93d	No error (0)	socialgrow.co.in		65.21.127.94	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:13.627137899 CET	8.8.8.8	192.168.2.3	0x49ec	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:13.958861113 CET	8.8.8.8	192.168.2.3	0x8257	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:13.958861113 CET	8.8.8.8	192.168.2.3	0x8257	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:14.009639025 CET	8.8.8.8	192.168.2.3	0xd98d	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:46:14.021028042 CET	8.8.8.8	192.168.2.3	0x40ae	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:46:14.286166906 CET	8.8.8.8	192.168.2.3	0x9a2f	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:15.219022989 CET	8.8.8.8	192.168.2.3	0xb07d	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:15.219022989 CET	8.8.8.8	192.168.2.3	0xb07d	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:15.250801086 CET	8.8.8.8	192.168.2.3	0x9ca0	No error (0)	dual.part-0032.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:46:15.250801086 CET	8.8.8.8	192.168.2.3	0x9ca0	No error (0)	dual.part-0032.t-0009.fbs1-t-msedge.net	part-0032.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:46:15.250801086 CET	8.8.8.8	192.168.2.3	0x9ca0	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.219.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:15.250801086 CET	8.8.8.8	192.168.2.3	0x9ca0	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.227.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:16.768930912 CET	8.8.8.8	192.168.2.3	0x1fcb	No error (0)	dual.part-0032.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false

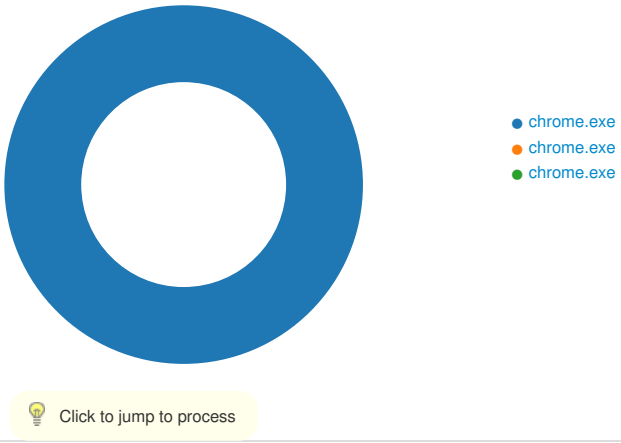
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:46:16.768930912 CET	8.8.8.8	192.168.2.3	0x1fcb	No error (0)	dual.part-0032.t-0009.fbs1-t-msedge.net	part-0032.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:46:16.768930912 CET	8.8.8.8	192.168.2.3	0x1fcb	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.219.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:46:16.768930912 CET	8.8.8.8	192.168.2.3	0x1fcb	No error (0)	part-0032.t-0009.fbs1-t-msedge.net		13.107.227.60	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:48:13.606765032 CET	8.8.8.8	192.168.2.3	0x1ee2	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- socialgrow.co.in
- maxcdn.bootstrapcdn.com
- logincdn.msauth.net
- https:
- cdnjs.cloudflare.com
- aadcdn.msauth.net

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **4796**, Parent PID: **2224**

General

Target ID:	0
Start time:	16:46:06
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 "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:	high

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: **6036**, Parent PID: **4796**

General

Target ID:	1
Start time:	16:46:07
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=1960 --field-trial-handle=1748,i,843581558575697743,11274918621816804293,131072 --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:	high

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: **1504**, Parent PID: **2224**

General	
Target ID:	2
Start time:	16:46:08
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" "C:\Users\user\Desktop\Payslip 28.11.22.html
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:	high

Registry Activities

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

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

Disassembly

No disassembly