ID: 756210
Sample Name: Markelcorp Pay-Application Completed November 29, 2022_4870771223077411004 6.html
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 20:23:50
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

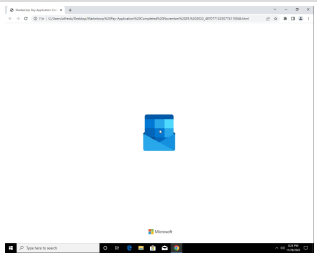
Windows Analysis Report

Markelcorp Pay-Application Completed November 29, 2022_48707712230774110046.html

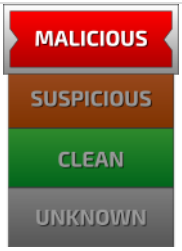
Overview

General Information

Sample Name:	Markelcorp Pay-Application Completed November 29, 2022_4870771223077411 0046.html
Analysis ID:	756210
MD5:	d21ad4851c9616..
SHA1:	bee29bccd77e68..
SHA256:	989f90793f02c5b..
Infos:	



Detection



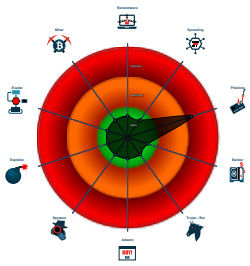
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish45
- JA3 SSL client fingerprint seen in co…
- Yara signature match
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 6832 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\Markelcorp Pay-Application Completed November 29, 2022_48707712230774110046.html MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 7036 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=2036 --field-trial-handle=1748,i,3206524124022006366,8441393421957404145,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
Markelcorp Pay-Application Completed November 29, 2022_4870771223077411004 6.html	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x5d0e:$c8: while(!![]) • 0x5d2c:$d1: parseInt(_0x111cb9(0x7c))/0x1*(parseInt(_0x111cb9(0x75))/0x2)+-parseInt(_0x111cb9(0x80))/0x3*(-parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(• 0x5d4b:$d1: parseInt(_0x111cb9(0x75))/0x2)+-parseInt(_0x111cb9(0x80))/0x3*(-parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+- • 0x5d6b:$d1: parseInt(_0x111cb9(0x80))/0x3*(-parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+-parseInt(_0x111cb9(0x6f))/0x8*(• 0x5d8b:$d1: parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+-parseInt(_0x111cb9(0x6f))/0x8*(parseInt(_0x111cb9(0x81))/0x9)+ • 0x5dab:$d1: parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+-parseInt(_0x111cb9(0x6f))/0x8*(parseInt(_0x111cb9(0x81))/0x9)+parseInt(_0x111cb9(0x8d))/0xa+

HTML

Source	Rule	Description	Author	Strings
49412.0.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x7807:$c8: while(!![]) • 0x7825:$d1: parseInt(_0x111cb9(0x7c))/0x1*(parseInt(_0x111cb9(0x75))/0x2)+-parseInt(_0x111cb9(0x80))/0x3*(-parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(• 0x7844:$d1: parseInt(_0x111cb9(0x75))/0x2)+-parseInt(_0x111cb9(0x80))/0x3*(-parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+- • 0x7864:$d1: parseInt(_0x111cb9(0x80))/0x3*(-parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+-parseInt(_0x111cb9(0x6f))/0x8*(• 0x7884:$d1: parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+-parseInt(_0x111cb9(0x6f))/0x8*(parseInt(_0x111cb9(0x81))/0x9)+ • 0x78a4:$d1: parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+-parseInt(_0x111cb9(0x6f))/0x8*(parseInt(_0x111cb9(0x81))/0x9)+parseInt(_0x111cb9(0x8d))/0xa+
49412.0.pages.csv	JoeSecurity_HtmlPhish_45	Yara detected HtmlPhish_45	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

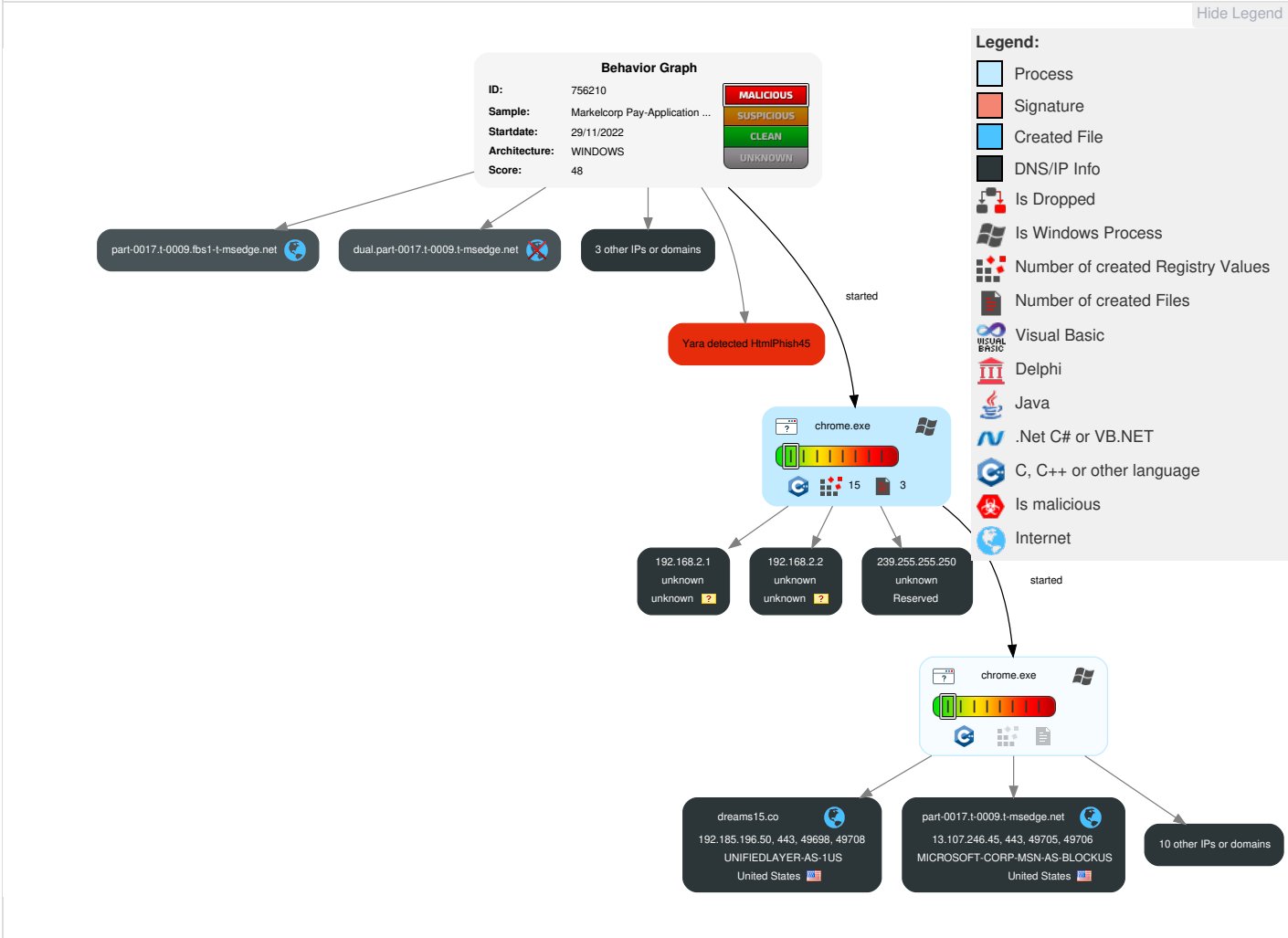
Phishing

Yara detected HtmlPhish45

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

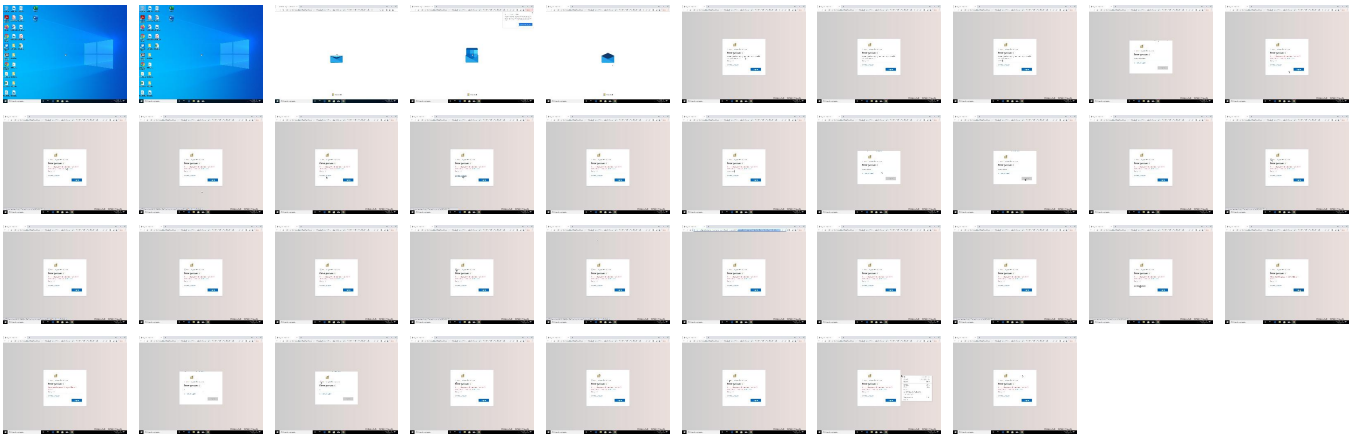
Behavior Graph

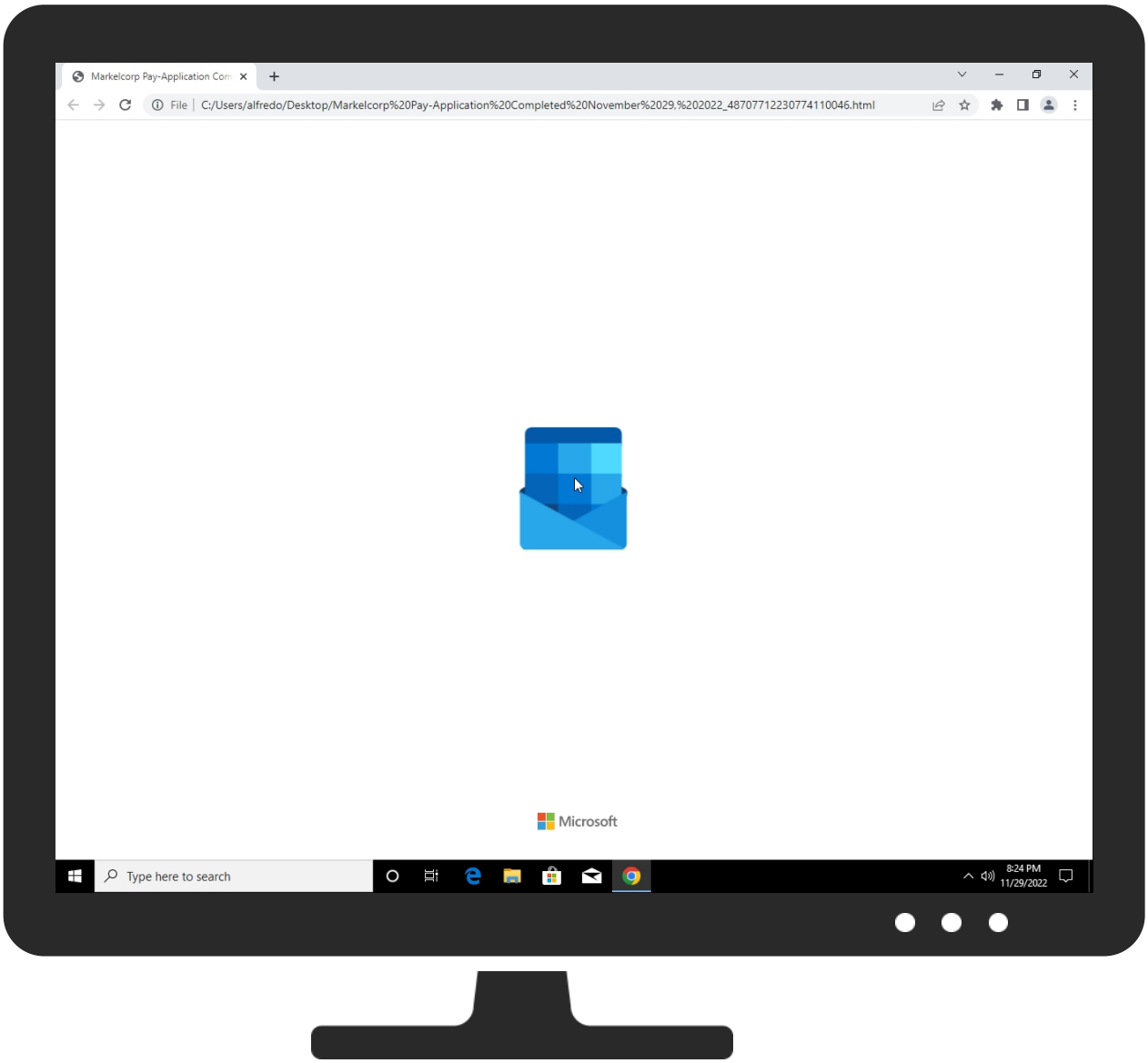


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
part-0017.t-0009.t-msedge.net	0%	Virustotal		Browse
part-0017.t-0009.fbs1-t-msedge.net	0%	Virustotal		Browse
cs1025.wpc.upsiloncdn.net	0%	Virustotal		Browse
aadcdn.msauthimages.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msauthimages.net/dbd5a2dd-ttl-x9zsondwno6uogaxggczkbj5okcite29gtm-6do/logintenantbranding/0/bannerlogo?ts=636450702596912772	0%	Avira URL Cloud	safe	
http://https://dreams15.co/csc/host9/0f70e1a.php	0%	Avira URL Cloud	safe	

Domains and IPs

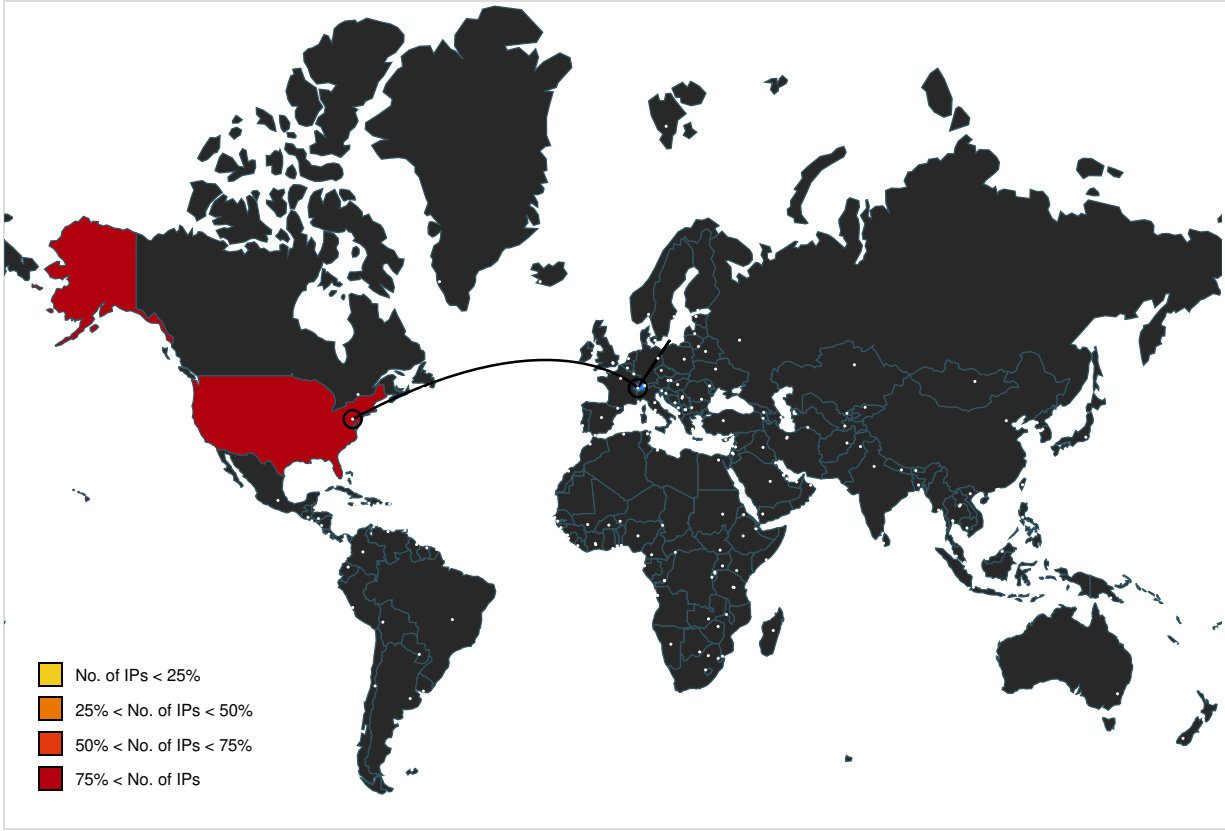
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
part-0017.t-0009.t-msedge.net	13.107.246.45	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	142.250.186.45	true	false		high
cdnjs.cloudflare.com	104.17.24.14	true	false		high
part-0017.t-0009.fbs1-t-msedge.net	13.107.219.45	true	false	• 0%, Virustotal, Browse	unknown
www.google.com	142.250.181.228	true	false		high
clients.l.google.com	142.250.186.110	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false	• 0%, Virustotal, Browse	unknown
dreams15.co	192.185.196.50	true	false		unknown
aadcdn.msauthimages.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/Markelcorp%20Pay-Application%20Completed%20November%2029,%202022_48707712230774110046.html	false		low
http://https://dreams15.co/csc/host9/0f70e1a.php	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	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=104.0.5112.102&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://aadcdn.msauthimages.net/dbd5a2dd-ttl-x9zsondwno6uogaxggczkbj5okcite29gtm-6do/logintenantbranding/0/bannerlogo?ts=636450702596912772	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.45	accounts.google.com	United States		15169	GOOGLEUS	false
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
13.107.246.45	part-0017.t-0009.t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.181.228	www.google.com	United States		15169	GOOGLEUS	false
192.185.196.50	dreams15.co	United States		46606	UNIFIEDLAYER-AS-1US	false
142.250.186.110	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.2
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756210
Start date and time:	2022-11-29 20:23:50 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Markelcorp Pay-Application Completed November 29, 2022_4870771223077411004 6.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:	mal48.phis.winHTML@23/0@12/11
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

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): 69.16.175.42, 69.16.175.10, 142.250.185.67, 34.104.35.123, 142.250.185.227
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, cds.s5x3j6q5.hwcdn.net, fs.microsoft.com, slscr.update.microsoft.com, aadcdnoriginwus2.azureedge.net, ctldl.windowsupdate.com, clientservices.googleapis.com, aadcdn.msauth.net, firstparty-azurefd-prod.trafficmanager.net, edgedl.me.gvt1.com, login.live.com, aadcdn.azureedge.net, aadcdn.ec.azureedge.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

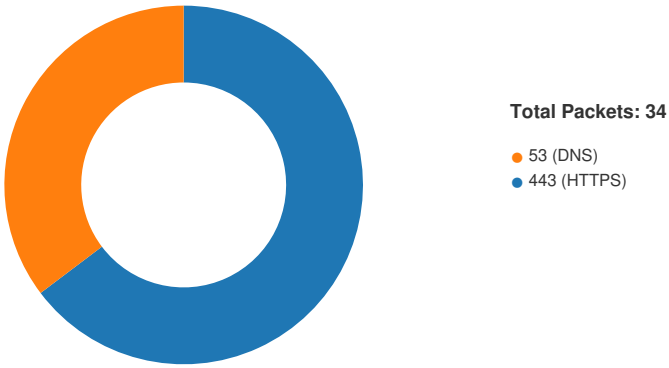
File type:	HTML document, ASCII text, with very long lines (27424), with no line terminators
Entropy (8bit):	5.901905953457114
TrID:	
File name:	Markelcorp Pay-Application Completed November 29, 2022_4870771223077411004 6.html
File size:	27424
MD5:	d21ad4851c96168de4456dea77044b9c
SHA1:	bee29bccd77e6848093f899a493f1330442899da
SHA256:	989f90793f02c5b623cf3830d184dba364fef0d2c2726d4636fb3b4877cafa39
SHA512:	3a6bf8462a335e0a83ed20aa7840f4c4b891afd95299b08f55b8e878927ad2dce5fb94a6dff0904e0fbcbf70a05ee87c338ffc43e4e062577753617ce5a6a882
SSDEEP:	768:72zsDrtJtatBLtrevto8W+3YNYziUr9Dng6PsyTljhdqk/rmWLT/AhlDfy:724DrtJtatxtrevto8W+7iUJg6PsUrw6
TLSH:	87C23D130A077A775F113B7B0B5B3E0F2405BD9D2AE16984D7168E64E11EB0B09EA23D
File Content Preview:	<head> </head><body> <input class="UOvCe9ucmB4k" type="hidden" id="b64u" value="aHR0cHM6Ly9kcmVhbXMxNS5jby9jc2MvaG9zdDkvMGY3MGUxYS5waHA="></input><div style="display:none;" id="e5zezr5TRTXB" name="V2Y8WIS38Z3i" class="5tAa

File Icon

Icon Hash:	78d0a8cccc88c460

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:24:19.603596926 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:19.603663921 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:19.603761911 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:19.606369972 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:19.606403112 CET	443	49693	142.250.186.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:24:19.618220091 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:19.618302107 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:19.618407965 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:19.618762016 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:19.618792057 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:19.714555025 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:19.715059042 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:19.715111971 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:19.716875076 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:19.716993093 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:19.721939087 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:19.744334936 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:19.744398117 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:19.745439053 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:19.745567083 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:19.746886969 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:19.746975899 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:20.022597075 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:20.022658110 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:20.022981882 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:20.024271011 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:20.024315119 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:20.025073051 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:20.025147915 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:20.025357008 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:20.025378942 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:20.025429010 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:20.053329945 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:20.053431988 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:20.053474903 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:20.053576946 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:20.053663969 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:20.057389021 CET	49693	443	192.168.2.3	142.250.186.110
Nov 29, 2022 20:24:20.057430983 CET	443	49693	142.250.186.110	192.168.2.3
Nov 29, 2022 20:24:20.065962076 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:20.066020966 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:20.080029011 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:20.080111027 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:20.080159903 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:20.080389023 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:20.080462933 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:20.082889080 CET	49696	443	192.168.2.3	142.250.186.45
Nov 29, 2022 20:24:20.082932949 CET	443	49696	142.250.186.45	192.168.2.3
Nov 29, 2022 20:24:20.506098032 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:20.506182909 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:20.506308079 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:20.506639004 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:20.506669044 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:20.778419018 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:20.788678885 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:20.788736105 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:20.790395975 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:20.790596962 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:20.792845011 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:20.792865992 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:20.793039083 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:20.793091059 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:20.793104887 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:20.833014011 CET	49698	443	192.168.2.3	192.185.196.50

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:24:20.833054066 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:20.873086929 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.432343006 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.432408094 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.432425022 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.432492971 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.432519913 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.432521105 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.432570934 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.432627916 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.473212004 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.555254936 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.555283070 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.555424929 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.555480003 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.555529118 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.555538893 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.555540085 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.555547953 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.555573940 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.555591106 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.555634022 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.555679083 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.555704117 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.555785894 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.555807114 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.595247984 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.679264069 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.679289103 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.679389000 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.679449081 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.679471970 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.679867029 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.679972887 CET	49698	443	192.168.2.3	192.185.196.50
Nov 29, 2022 20:24:22.679990053 CET	443	49698	192.185.196.50	192.168.2.3
Nov 29, 2022 20:24:22.680197954 CET	443	49698	192.185.196.50	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:24:19.556044102 CET	65186	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:24:19.557481050 CET	50041	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:24:19.558235884 CET	63765	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:24:19.575220108 CET	53	50041	1.1.1.1	192.168.2.3
Nov 29, 2022 20:24:19.578953028 CET	53	63765	1.1.1.1	192.168.2.3
Nov 29, 2022 20:24:20.271323919 CET	49454	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:24:20.501948118 CET	53	49454	1.1.1.1	192.168.2.3
Nov 29, 2022 20:24:23.285932064 CET	64579	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:24:23.304537058 CET	53	64579	1.1.1.1	192.168.2.3
Nov 29, 2022 20:24:23.311235905 CET	52348	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:24:23.330245972 CET	53	52348	1.1.1.1	192.168.2.3
Nov 29, 2022 20:24:23.522164106 CET	52907	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:24:23.539839029 CET	53	52907	1.1.1.1	192.168.2.3
Nov 29, 2022 20:24:24.897500038 CET	56244	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:24:27.267615080 CET	58946	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:25:23.342816114 CET	55220	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:25:23.360928059 CET	53	55220	1.1.1.1	192.168.2.3
Nov 29, 2022 20:25:23.367889881 CET	57975	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:25:23.386446953 CET	53	57975	1.1.1.1	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:25:29.444670916 CET	49767	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:25:29.674268007 CET	53	49767	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 20:24:19.556044102 CET	192.168.2.3	1.1.1.1	0x5469	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:19.557481050 CET	192.168.2.3	1.1.1.1	0xc108	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:19.558235884 CET	192.168.2.3	1.1.1.1	0x8e35	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:20.271323919 CET	192.168.2.3	1.1.1.1	0x51c8	Standard query (0)	dreams15.co	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:23.285932064 CET	192.168.2.3	1.1.1.1	0x4b23	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:23.311235905 CET	192.168.2.3	1.1.1.1	0xaa0d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:23.522164106 CET	192.168.2.3	1.1.1.1	0xb7d1	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:24.897500038 CET	192.168.2.3	1.1.1.1	0x63d	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:27.267615080 CET	192.168.2.3	1.1.1.1	0x9293	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:25:23.342816114 CET	192.168.2.3	1.1.1.1	0x6b47	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:25:23.367889881 CET	192.168.2.3	1.1.1.1	0xa4db	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:25:29.444670916 CET	192.168.2.3	1.1.1.1	0xda0b	Standard query (0)	dreams15.co	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 20:24:19.575120926 CET	1.1.1.1	192.168.2.3	0x5469	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:24:19.575220108 CET	1.1.1.1	192.168.2.3	0xc108	No error (0)	accounts.google.com		142.250.186.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:19.578953028 CET	1.1.1.1	192.168.2.3	0x8e35	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:24:19.578953028 CET	1.1.1.1	192.168.2.3	0x8e35	No error (0)	clients.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:20.501948118 CET	1.1.1.1	192.168.2.3	0x51c8	No error (0)	dreams15.co		192.185.196.50	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:23.304537058 CET	1.1.1.1	192.168.2.3	0x4b23	No error (0)	www.google.com		142.250.181.228	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:23.330245972 CET	1.1.1.1	192.168.2.3	0xaa0d	No error (0)	www.google.com		142.250.181.228	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:23.539839029 CET	1.1.1.1	192.168.2.3	0xb7d1	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:23.539839029 CET	1.1.1.1	192.168.2.3	0xb7d1	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:23.601629972 CET	1.1.1.1	192.168.2.3	0xc441	No error (0)	dual.part-0017.t-0009.t-msedge.net	part-0017.t-0009.t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:24:23.601629972 CET	1.1.1.1	192.168.2.3	0xc441	No error (0)	part-0017.t-0009.t-msedge.net		13.107.246.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:23.601629972 CET	1.1.1.1	192.168.2.3	0xc441	No error (0)	part-0017.t-0009.t-msedge.net		13.107.213.45	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 20:24:24.917996883 CET	1.1.1.1	192.168.2.3	0x63d	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:24:24.917996883 CET	1.1.1.1	192.168.2.3	0x63d	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:27.290196896 CET	1.1.1.1	192.168.2.3	0x9293	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:24:27.290196896 CET	1.1.1.1	192.168.2.3	0x9293	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:27.380778074 CET	1.1.1.1	192.168.2.3	0xb0cc	No error (0)	dual.part-0017.t-0009.t-msedge.net	global-entry-afdthirdparty-fallback.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:24:27.380778074 CET	1.1.1.1	192.168.2.3	0xb0cc	No error (0)	dual.part-0017.t-0009.fbs1-t-msedge.net	part-0017.t-0009.fbs1-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:24:27.380778074 CET	1.1.1.1	192.168.2.3	0xb0cc	No error (0)	part-0017.t-0009.fbs1-t-msedge.net		13.107.219.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:24:27.380778074 CET	1.1.1.1	192.168.2.3	0xb0cc	No error (0)	part-0017.t-0009.fbs1-t-msedge.net		13.107.227.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:25:23.360928059 CET	1.1.1.1	192.168.2.3	0x6b47	No error (0)	www.google.com		142.250.185.100	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:25:23.386446953 CET	1.1.1.1	192.168.2.3	0xa4db	No error (0)	www.google.com		142.250.181.228	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:25:29.674268007 CET	1.1.1.1	192.168.2.3	0xda0b	No error (0)	dreams15.co		192.185.196.50	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- dreams15.co
- cdnjs.cloudflare.com
- aadcdn.msauth.net
- aadcdn.msauthimages.net

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **6832**, Parent PID: **3800**

General

Target ID:	0
Start time:	20:24:15
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\Markelcorp Pay-Application Completed November 29, 2022_48707712230774110046.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: **7036**, Parent PID: **6832**

General	
Target ID:	2
Start time:	20:24:17
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=2036 --field-trial-handle=1748,i,3206524124022006366,8441393421957404145,131072 --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