ID: 756249
Sample Name: Markelcorp Pay Application November 29, 2022_1172551224782016142 3.html
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 21:48:50
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

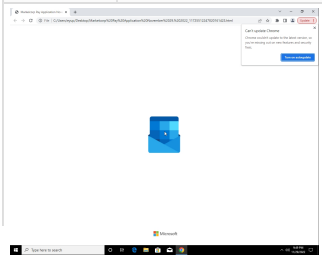
Windows Analysis Report

Markelcorp Pay Application November 29, 2022_1172551224782016 1423.html

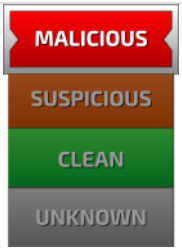
Overview

General Information

Sample Name:	Markelcorp Pay Application November 29, 2022_1172551224782016 1423.html
Analysis ID:	756249
MD5:	397547503a0f97..
SHA1:	3953830b316290.
SHA256:	57cbed8d8d5433..
Infos:	



Detection



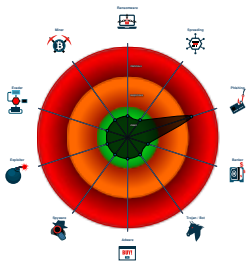
HTMLPhisher

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: 6868 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\Markelcorp Pay Application November 29, 2022_1172551224782016 1423.html MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 2864 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=1800,i,13735318130024018 01,16495176252513405895,131072 --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 November 29, 2022_11725 51224782016142 3.html	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x5d06:$c8: while(!![]) • 0x5d24:$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*(• 0x5d43:$d1: parseInt(_0x111cb9(0x75))/0x2)+-parseInt(_0x111cb9(0x80))/0x3*(-parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+- • 0x5d63:$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*(• 0x5d83:$d1: parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+-parseInt(_0x111cb9(0x6f))/0x8*(parseInt(_0x111cb9(0x81))/0x9)+ • 0x5da3:$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
22653.0.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x77e8:$c8: while(!![]) • 0x7806:$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*(• 0x7825:$d1: parseInt(_0x111cb9(0x75))/0x2)+-parseInt(_0x111cb9(0x80))/0x3*(-parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+- • 0x7845:$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*(• 0x7865:$d1: parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+-parseInt(_0x111cb9(0x6f))/0x8*(parseInt(_0x111cb9(0x81))/0x9)+ • 0x7885:$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+
22653.0.pages.csv	JoeSecurity_HtmlPhish_45	Yara detected HtmlPhish_45	Joe Security	
22275.2.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x77ea:$c8: while(!![]) • 0x7808:$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*(• 0x7827:$d1: parseInt(_0x111cb9(0x75))/0x2)+-parseInt(_0x111cb9(0x80))/0x3*(-parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+- • 0x7847:$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*(• 0x7867:$d1: parseInt(_0x111cb9(0x7b))/0x4)+-parseInt(_0x111cb9(0x6e))/0x5+-parseInt(_0x111cb9(0x83))/0x6*(parseInt(_0x111cb9(0x86))/0x7)+-parseInt(_0x111cb9(0x6f))/0x8*(parseInt(_0x111cb9(0x81))/0x9)+ • 0x7887:$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+
22275.2.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

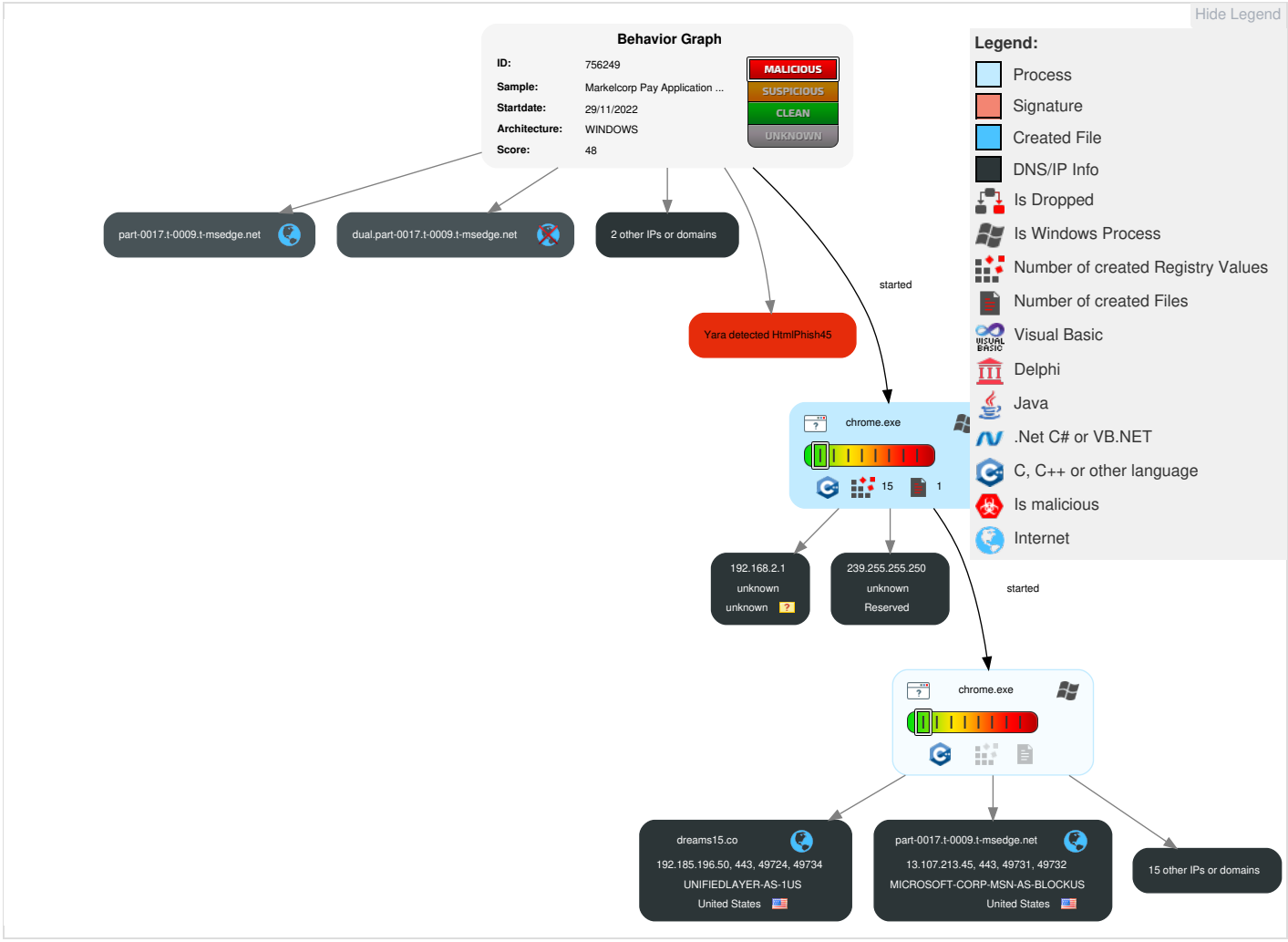
Phishing

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

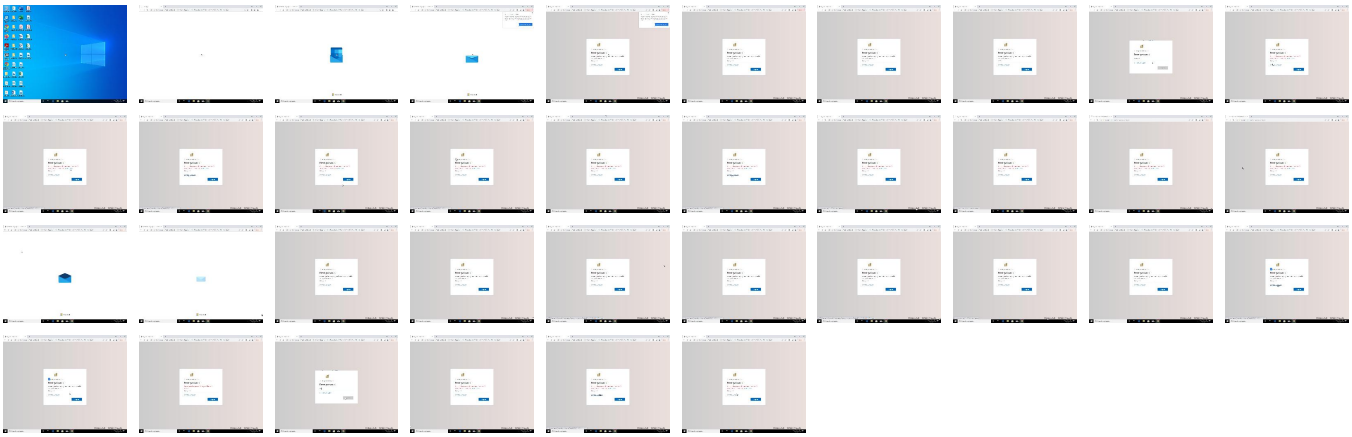
Behavior Graph

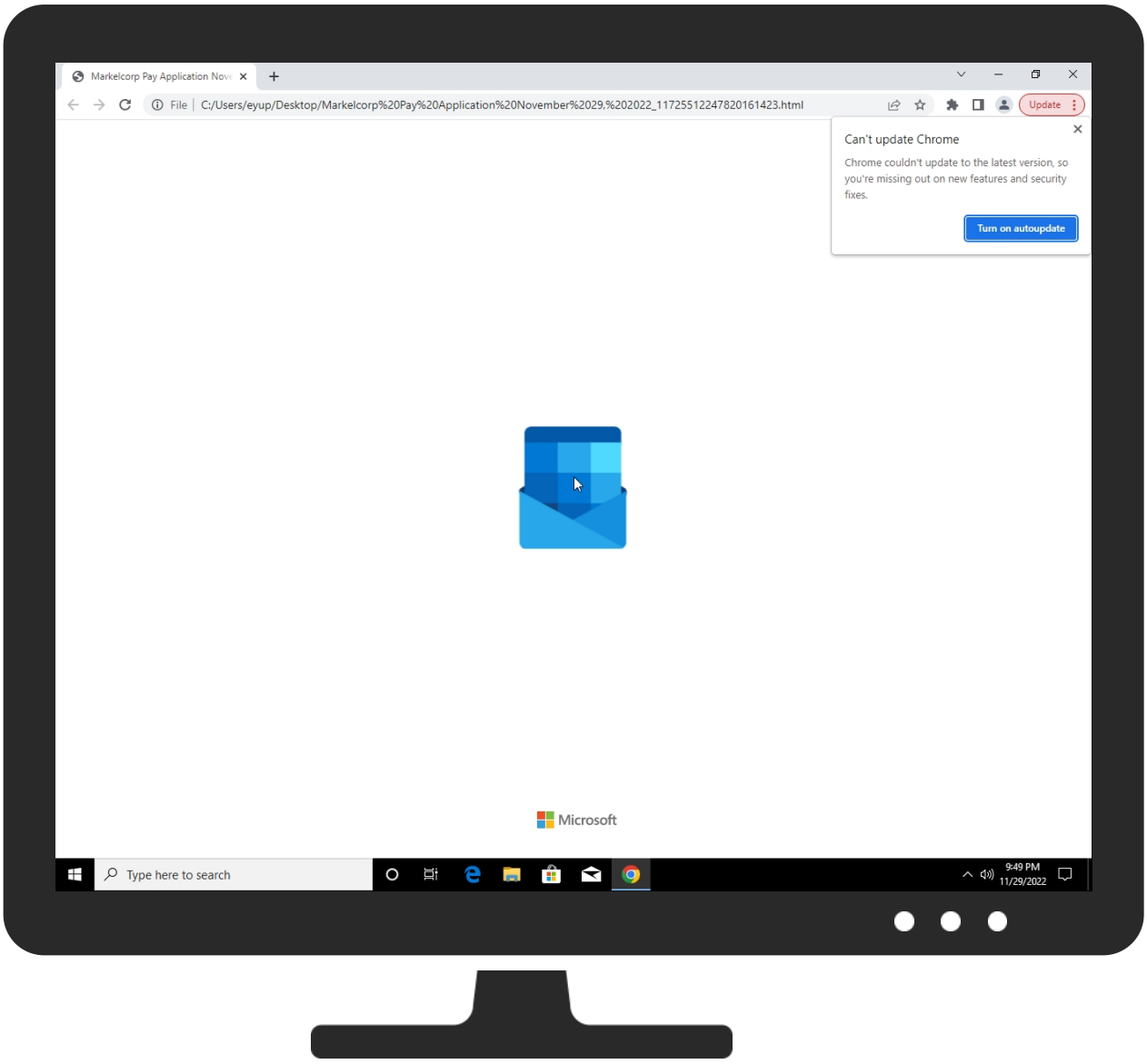


Screenshots

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
cs1025.wpc.upsiloncdn.net	0%	Virustotal		Browse
dreams15.co	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

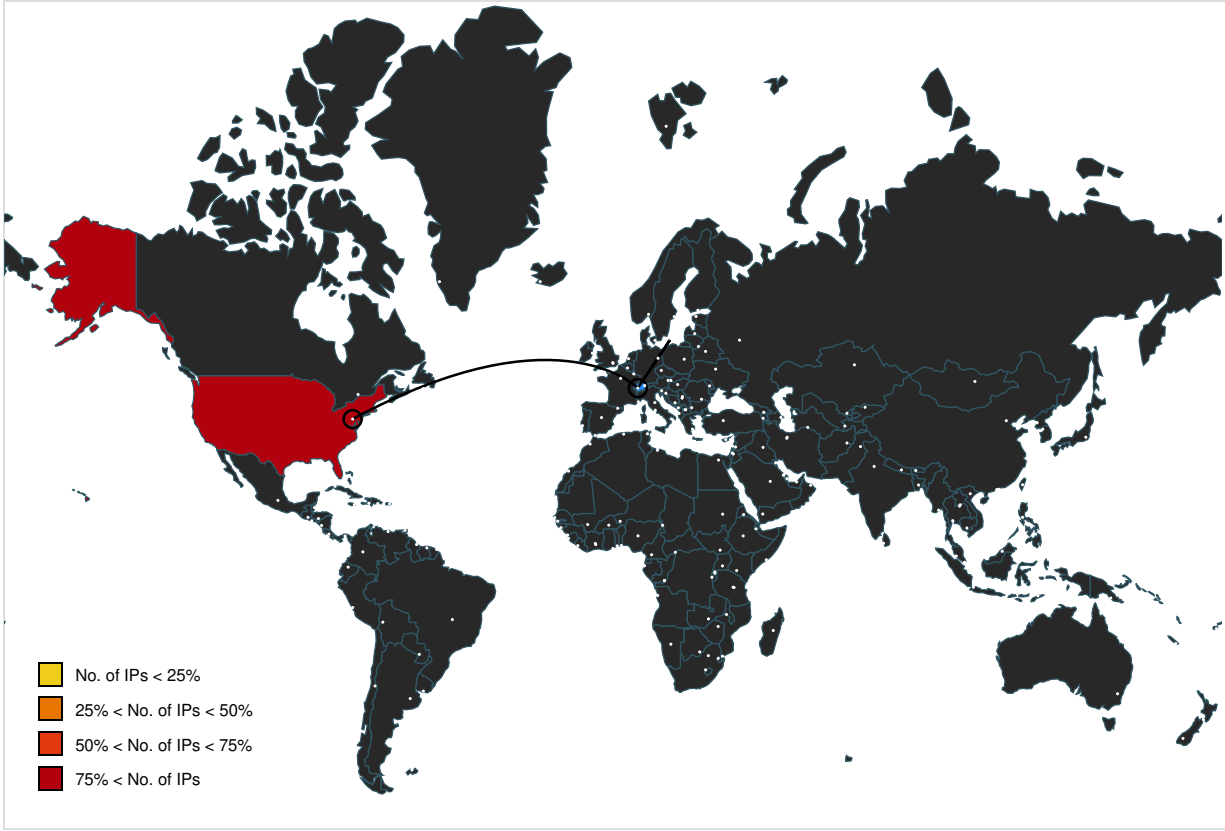
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
part-0017.t-0009.t-msedge.net	13.107.213.45	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	142.250.186.109	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
www.google.com	172.217.16.132	true	false		high
clients.l.google.com	142.250.185.206	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	• 0%, Virustotal, Browse	unknown
aadcdn.msauthimages.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
c.s-microsoft.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
assets.onestore.ms	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/Markelcorp%20Pay%20Application%20November%2029,%202022_1172551224782016142 3.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
file:///C:/Users/user/Desktop/Markelcorp%20Pay%20Application%20November%2029,%202022_1172551224782016142 3.html#	false		low
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
142.250.186.68	unknown	United States		15169	GOOGLEUS	false
142.250.185.206	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.36	unknown	United States		15169	GOOGLEUS	false
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
13.107.213.45	part-0017.t-0009.t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.186.109	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.185.196.50	dreams15.co	United States		46606	UNIFIEDLAYER-AS-1US	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:	756249
Start date and time:	2022-11-29 21:48:50 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Markelcorp Pay Application November 29, 2022_1172551224782016142 3.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:	5

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.winHTML@26/0@15/11
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): WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 69.16.175.42, 69.16.175.10, 216.58.212.131, 34.104.35.123, 88.221.169.152, 23.3.109.244, 152.199.19.160, 184.24.10.194, 95.101.54.137, 95.101.54.139, 95.101.54.216, 95.101.54.121, 172.217.16.131
- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, assets.onestore.ms.edgekey.net, slscr.update.microsoft.com, e13678.dscb.akamaiedge.net, clientservices.googleapis.com, a1449.dscg2.akamai.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, a1945.g2.akamai.net, www.microsoft.com-c-3.edgekey.net, mscomajax.vo.msecnd.net, login.live.com, aadcdn.azureedge.net, aadcdn.ec.azureedge.net, update.googleapis.com, statics-marketingsites-eus-ms-com.akamaized.net, img-prod-cms-rt-microsoft-com.akamaized.net, e10583.dspg.akamaiedge.net, client.wns.windows.com, aadcdnoriginwus2.azureedge.net, cs22.wpc.v0cdn.net, aadcdn.msauth.net, assets.onestore.ms.akadns.net, firstparty-azurefd-prod.trafficmanager.net, c-s.cms.ms.akadns.net, edgedl.me.gvt1.com, privacy.microsoft.com, aadcdnoriginwus2.afd.azureedge.net, c.s-microsoft.com-c.edgekey.net, e13678.dscg.akamaiedge.net, privacy.microsoft.com.edgekey.net, www.microsoft.com, e13678.dspb.akamaiedge.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

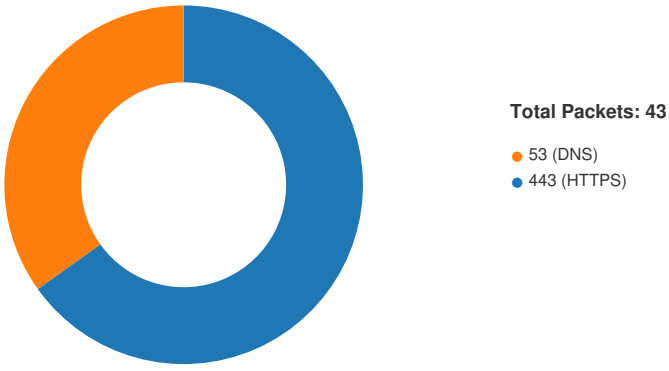
File type:	HTML document, ASCII text, with very long lines (27416), with no line terminators
Entropy (8bit):	5.901857288894095
TrID:	
File name:	Markelcorp Pay Application November 29, 2022_11725512247820161423.html
File size:	27416
MD5:	397547503a0f979f55d246022dd70ddf
SHA1:	3953830b316290a8f8a4f4f8e8040a9d0231038b
SHA256:	57cbed8d8d5433b7e12c7838a6a458adaf27bea086602bf666ecf4276df62fd5
SHA512:	3eada352c4b80b96222e2430e354201f2d813372c437418632927013a444fc6d9ef8ce67ce3b7d3025f8ccd4fa888f3d26b615dc9abc885ab2459dd927e55ab5
SSDEEP:	768:7nzsDrtJtatBLtrevto8W+3YNYziUr9Dng6PsyTljhdqk/rmWLT/AhlDfy:7n4DrtJtatxtrevto8W+7iUJg6PsUrw6
TLSH:	C2C23D130A077A775F113B7B0B5B3E0F2405BD9D2AE16984D7168E64E11EB0B09EA23D
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 21:49:25.169923067 CET	49720	443	192.168.2.2	142.250.185.206
Nov 29, 2022 21:49:25.169967890 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.170053005 CET	49720	443	192.168.2.2	142.250.185.206
Nov 29, 2022 21:49:25.170311928 CET	49720	443	192.168.2.2	142.250.185.206

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:49:25.170341969 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.171641111 CET	49721	443	192.168.2.2	142.250.186.109
Nov 29, 2022 21:49:25.171701908 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.171828032 CET	49721	443	192.168.2.2	142.250.186.109
Nov 29, 2022 21:49:25.172151089 CET	49721	443	192.168.2.2	142.250.186.109
Nov 29, 2022 21:49:25.172179937 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.230479002 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.234889984 CET	49721	443	192.168.2.2	142.250.186.109
Nov 29, 2022 21:49:25.234934092 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.236869097 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.236974001 CET	49721	443	192.168.2.2	142.250.186.109
Nov 29, 2022 21:49:25.264257908 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.264630079 CET	49720	443	192.168.2.2	142.250.185.206
Nov 29, 2022 21:49:25.264659882 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.265274048 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.265377045 CET	49720	443	192.168.2.2	142.250.185.206
Nov 29, 2022 21:49:25.266294956 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.266380072 CET	49720	443	192.168.2.2	142.250.185.206
Nov 29, 2022 21:49:25.609740019 CET	49721	443	192.168.2.2	142.250.186.109
Nov 29, 2022 21:49:25.609904051 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.609936953 CET	49721	443	192.168.2.2	142.250.186.109
Nov 29, 2022 21:49:25.609950066 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.610193968 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.616101027 CET	49720	443	192.168.2.2	142.250.185.206
Nov 29, 2022 21:49:25.616147995 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.616252899 CET	49720	443	192.168.2.2	142.250.185.206
Nov 29, 2022 21:49:25.616266966 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.616398096 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.645034075 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.645133972 CET	49720	443	192.168.2.2	142.250.185.206
Nov 29, 2022 21:49:25.645164967 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.645329952 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.645414114 CET	49720	443	192.168.2.2	142.250.185.206
Nov 29, 2022 21:49:25.647753000 CET	49720	443	192.168.2.2	142.250.185.206
Nov 29, 2022 21:49:25.647782087 CET	443	49720	142.250.185.206	192.168.2.2
Nov 29, 2022 21:49:25.661397934 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.661525011 CET	49721	443	192.168.2.2	142.250.186.109
Nov 29, 2022 21:49:25.661566019 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.661901951 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:25.662024021 CET	49721	443	192.168.2.2	142.250.186.109
Nov 29, 2022 21:49:25.663353920 CET	49721	443	192.168.2.2	142.250.186.109
Nov 29, 2022 21:49:25.663387060 CET	443	49721	142.250.186.109	192.168.2.2
Nov 29, 2022 21:49:26.055250883 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:26.055305958 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:26.055425882 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:26.056669950 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:26.056695938 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:26.344027996 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:26.367523909 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:26.367566109 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:26.371709108 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:26.371860981 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:26.374160051 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:26.374183893 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:26.374389887 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:26.374411106 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:26.374438047 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:26.492465019 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:26.492506027 CET	443	49724	192.185.196.50	192.168.2.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:49:26.690649033 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:27.820089102 CET	49729	443	192.168.2.2	142.250.186.36
Nov 29, 2022 21:49:27.820167065 CET	443	49729	142.250.186.36	192.168.2.2
Nov 29, 2022 21:49:27.820301056 CET	49729	443	192.168.2.2	142.250.186.36
Nov 29, 2022 21:49:27.820621014 CET	49729	443	192.168.2.2	142.250.186.36
Nov 29, 2022 21:49:27.820648909 CET	443	49729	142.250.186.36	192.168.2.2
Nov 29, 2022 21:49:27.882930040 CET	443	49729	142.250.186.36	192.168.2.2
Nov 29, 2022 21:49:27.883419037 CET	49729	443	192.168.2.2	142.250.186.36
Nov 29, 2022 21:49:27.883466959 CET	443	49729	142.250.186.36	192.168.2.2
Nov 29, 2022 21:49:27.884829998 CET	443	49729	142.250.186.36	192.168.2.2
Nov 29, 2022 21:49:27.884938002 CET	49729	443	192.168.2.2	142.250.186.36
Nov 29, 2022 21:49:27.898240089 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:27.898283005 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:27.898294926 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:27.898370981 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:27.898518085 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:27.898565054 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:27.936952114 CET	49729	443	192.168.2.2	142.250.186.36
Nov 29, 2022 21:49:27.937006950 CET	443	49729	142.250.186.36	192.168.2.2
Nov 29, 2022 21:49:27.937390089 CET	443	49729	142.250.186.36	192.168.2.2
Nov 29, 2022 21:49:27.991183996 CET	49729	443	192.168.2.2	142.250.186.36
Nov 29, 2022 21:49:27.991214037 CET	443	49729	142.250.186.36	192.168.2.2
Nov 29, 2022 21:49:27.991281033 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:28.030251980 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:28.030282974 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:28.030421019 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:28.030462980 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:28.030524969 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:28.030549049 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:28.030570984 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:28.030581951 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:28.030642986 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:28.030642986 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:28.030654907 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:28.030723095 CET	49724	443	192.168.2.2	192.185.196.50
Nov 29, 2022 21:49:28.030745029 CET	443	49724	192.185.196.50	192.168.2.2
Nov 29, 2022 21:49:28.030920029 CET	443	49724	192.185.196.50	192.168.2.2

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:49:25.122175932 CET	63816	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:49:25.137428999 CET	59174	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:49:25.138392925 CET	56924	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:49:25.155177116 CET	53	59174	1.1.1.1	192.168.2.2
Nov 29, 2022 21:49:25.155576944 CET	53	56924	1.1.1.1	192.168.2.2
Nov 29, 2022 21:49:25.820012093 CET	59098	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:49:26.053008080 CET	53	59098	1.1.1.1	192.168.2.2
Nov 29, 2022 21:49:27.760616064 CET	51479	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:49:27.779509068 CET	53	51479	1.1.1.1	192.168.2.2
Nov 29, 2022 21:49:27.791209936 CET	55033	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:49:27.809509993 CET	53	55033	1.1.1.1	192.168.2.2
Nov 29, 2022 21:49:28.536875010 CET	49913	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:49:28.555459023 CET	53	49913	1.1.1.1	192.168.2.2
Nov 29, 2022 21:49:29.472599030 CET	63604	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:49:32.623863935 CET	54770	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:50:15.816103935 CET	53580	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:50:15.816636086 CET	61575	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:50:15.816977978 CET	64419	53	192.168.2.2	1.1.1.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:50:27.823905945 CET	49737	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:50:27.842633963 CET	53	49737	1.1.1.1	192.168.2.2
Nov 29, 2022 21:50:27.870192051 CET	64597	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:50:27.888355017 CET	53	64597	1.1.1.1	192.168.2.2
Nov 29, 2022 21:50:46.049969912 CET	55156	53	192.168.2.2	1.1.1.1
Nov 29, 2022 21:50:46.282641888 CET	53	55156	1.1.1.1	192.168.2.2

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 21:49:25.122175932 CET	192.168.2.2	1.1.1.1	0xc9f4	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:25.137428999 CET	192.168.2.2	1.1.1.1	0xb156	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:25.138392925 CET	192.168.2.2	1.1.1.1	0x2714	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:25.820012093 CET	192.168.2.2	1.1.1.1	0x1f	Standard query (0)	dreams15.co	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:27.760616064 CET	192.168.2.2	1.1.1.1	0x50ab	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:27.791209936 CET	192.168.2.2	1.1.1.1	0xd888	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:28.536875010 CET	192.168.2.2	1.1.1.1	0x80c8	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:29.472599030 CET	192.168.2.2	1.1.1.1	0xb9f3	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:32.623863935 CET	192.168.2.2	1.1.1.1	0x12d	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:50:15.816103935 CET	192.168.2.2	1.1.1.1	0x624b	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:50:15.816636086 CET	192.168.2.2	1.1.1.1	0x548b	Standard query (0)	c.s-microsoft.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:50:15.816977978 CET	192.168.2.2	1.1.1.1	0x4e8f	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:50:27.823905945 CET	192.168.2.2	1.1.1.1	0x6b6c	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:50:27.870192051 CET	192.168.2.2	1.1.1.1	0x8055	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:50:46.049969912 CET	192.168.2.2	1.1.1.1	0x192d	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 21:49:25.141035080 CET	1.1.1.1	192.168.2.2	0xc9f4	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:49:25.155177116 CET	1.1.1.1	192.168.2.2	0xb156	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:49:25.155177116 CET	1.1.1.1	192.168.2.2	0xb156	No error (0)	clients.l.google.com		142.250.185.206	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:25.155576944 CET	1.1.1.1	192.168.2.2	0x2714	No error (0)	accounts.google.com		142.250.186.109	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:26.053008080 CET	1.1.1.1	192.168.2.2	0x1f	No error (0)	dreams15.co		192.185.196.50	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:27.779509068 CET	1.1.1.1	192.168.2.2	0x50ab	No error (0)	www.google.com		172.217.16.132	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:27.809509993 CET	1.1.1.1	192.168.2.2	0xd888	No error (0)	www.google.com		142.250.186.36	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:28.555459023 CET	1.1.1.1	192.168.2.2	0x80c8	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false

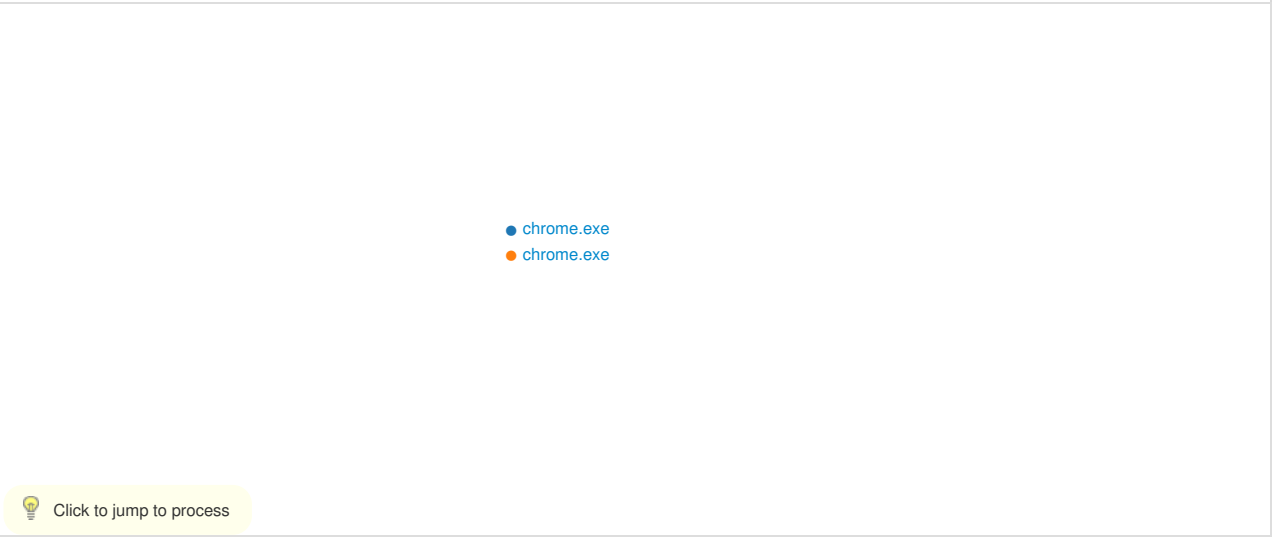
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 21:49:28.555459023 CET	1.1.1.1	192.168.2.2	0x80c8	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:28.560442924 CET	1.1.1.1	192.168.2.2	0x9a60	No 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 21:49:28.560442924 CET	1.1.1.1	192.168.2.2	0x9a60	No error (0)	part-0017.t-0009.t-msedge.net		13.107.213.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:28.560442924 CET	1.1.1.1	192.168.2.2	0x9a60	No error (0)	part-0017.t-0009.t-msedge.net		13.107.246.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:29.490746975 CET	1.1.1.1	192.168.2.2	0xb9f3	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:49:29.490746975 CET	1.1.1.1	192.168.2.2	0xb9f3	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:32.642046928 CET	1.1.1.1	192.168.2.2	0x12d	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:49:32.642046928 CET	1.1.1.1	192.168.2.2	0x12d	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:32.964016914 CET	1.1.1.1	192.168.2.2	0x786a	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 21:49:32.964016914 CET	1.1.1.1	192.168.2.2	0x786a	No error (0)	part-0017.t-0009.t-msedge.net		13.107.246.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:49:32.964016914 CET	1.1.1.1	192.168.2.2	0x786a	No error (0)	part-0017.t-0009.t-msedge.net		13.107.213.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:50:15.833900928 CET	1.1.1.1	192.168.2.2	0x624b	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:50:15.837498903 CET	1.1.1.1	192.168.2.2	0x548b	No error (0)	c.s-microsoft.com	c-s.cms.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:50:15.838330984 CET	1.1.1.1	192.168.2.2	0x4e8f	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:50:27.842633963 CET	1.1.1.1	192.168.2.2	0x6b6c	No error (0)	www.google.com		142.250.185.132	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:50:27.888355017 CET	1.1.1.1	192.168.2.2	0x8055	No error (0)	www.google.com		142.250.186.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:50:46.282641888 CET	1.1.1.1	192.168.2.2	0x192d	No error (0)	dreams15.co		192.185.196.50	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6868**, Parent PID: **3580**

General

Target ID:	0
Start time:	21:49:20
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 November 29, 2022_1172551224782016142 3.html
Imagebase:	0x7ff600460000
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: **2864**, Parent PID: **6868**

General

Target ID:	1
Start time:	21:49:22
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=1800,i,13735318130024018 01,16495176252513405895,131072 --disable-features =OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff600460000
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