



ID: 715060
Sample Name: Milwaukeetool Payment.hTml
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 15:44:53
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Milwaukeetool Payment.hTml 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Initial Sample 3
Sigma Signatures 4
Snort Signatures 4
Joe Sandbox Signatures 4
Phishing 4
System Summary 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
World Map of Contacted IPs 7
Public IPs 7
Private 7
General Information 8
Warnings 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASNs 8
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
Network Behavior 9
Network Port Distribution 9
TCP Packets 9
UDP Packets 11
ICMP Packets 12
DNS Queries 12
DNS Answers 12
HTTP Request Dependency Graph 12
HTTPS Proxied Packets 12
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: chrome.exePID: 5772, Parent PID: 1420 14
General 14
File Activities 15
Registry Activities 15
Analysis Process: chrome.exePID: 5940, Parent PID: 5772 15
General 15
File Activities 15
Analysis Process: chrome.exePID: 4912, Parent PID: 1420 15
General 15
Registry Activities 16
Disassembly 16

Copyright Joe Security LLC 2022

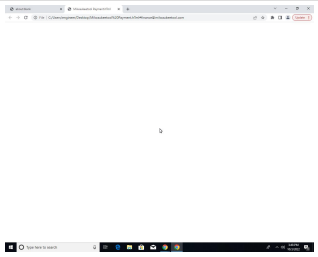
Windows Analysis Report

Milwaukeetool Payment.hTml

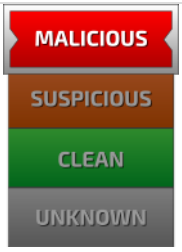
Overview

General Information

Sample Name:	Milwaukeetool Payment.hTml
Analysis ID:	715060
MD5:	148dbfa4a28fb63.
SHA1:	6f731eb3f50a128.
SHA256:	58bb9db8b22c7b..
Infos:	



Detection



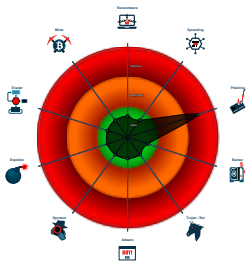
HTMLPhisher

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish44
- Yara detected obfuscated html page
- HTML document with suspicious na…
- Yara signature match
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5772 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5940 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=1956 --field-trial-handle=1700,i,2030005579113327324,13011269261470832477,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4912 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\Milwaukeetool Payment.hTml MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Milwaukeetool Payment.hTml	SUSP_obfuscated_JS_obfuscatorio	Detect JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x156:$c8: while(!![]) • 0x175:$d1: parseInt(_0x483f24(0x177))/0x1+-parseInt(_0x483f24(0x169))/0x2+parseInt(_0x483f24(0x171))/0x3+-parseInt(_0x483f24(0x175))/0x4+parseInt(_0x483f24(0x163))/0x5+-parseInt(_0x483f24(0x16f))/0x6*(• 0x195:$d1: parseInt(_0x483f24(0x169))/0x2+parseInt(_0x483f24(0x171))/0x3+-parseInt(_0x483f24(0x175))/0x4+parseInt(_0x483f24(0x163))/0x5+-parseInt(_0x483f24(0x16f))/0x6*(parseInt(_0x483f24(0x16a))/0x7)+
Milwaukeetool Payment.hTml	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
Milwaukeetool Payment.hTml	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing



Yara detected HtmlPhish44

Yara detected obfuscated html page

System Summary

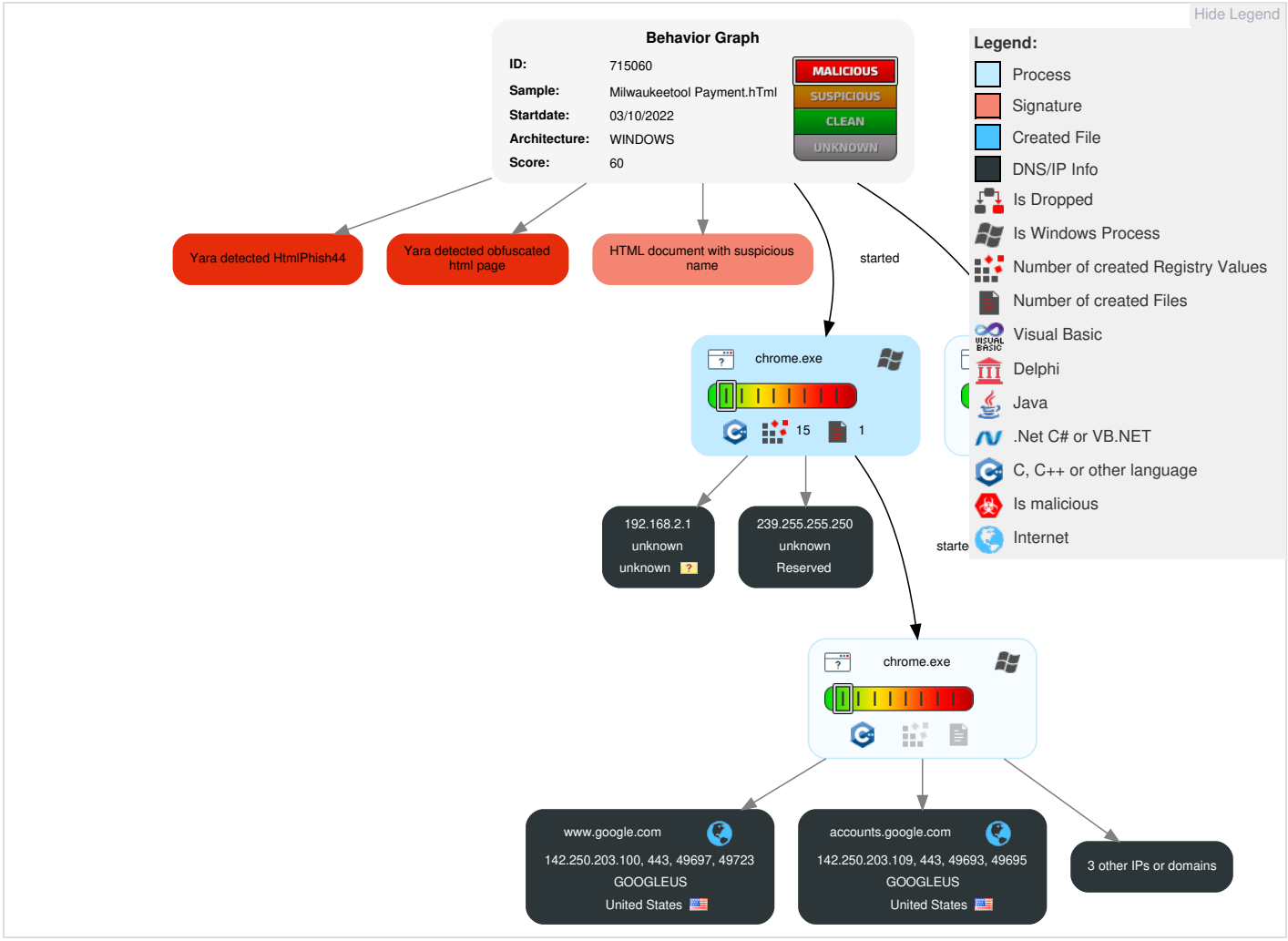


HTML document with suspicious name

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	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

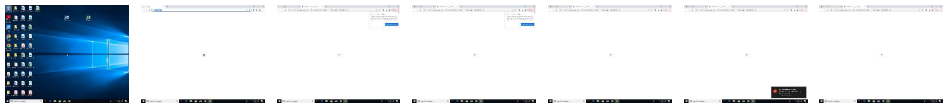
Behavior Graph

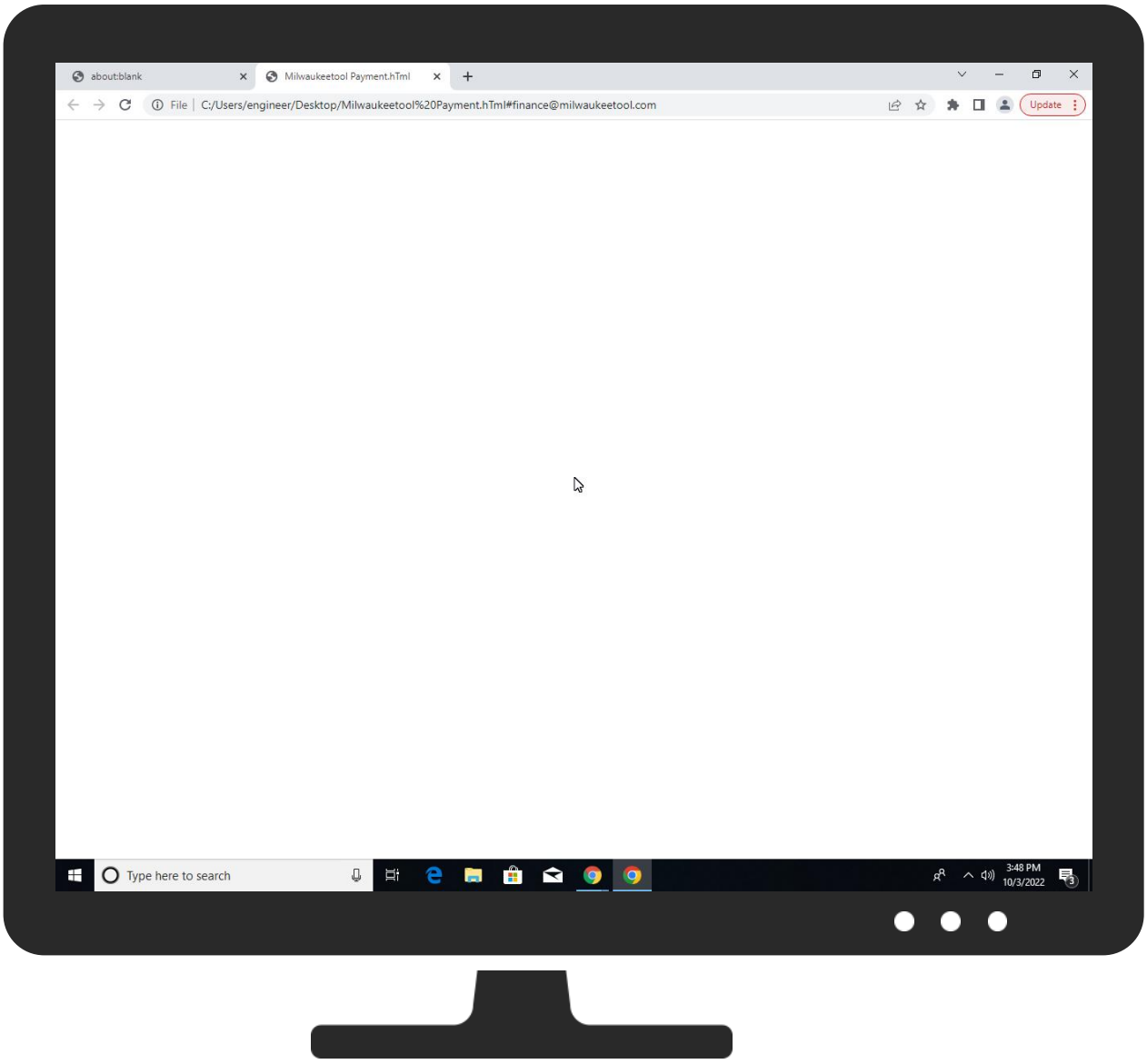


Screenshots

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

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2022

Domains and IPs

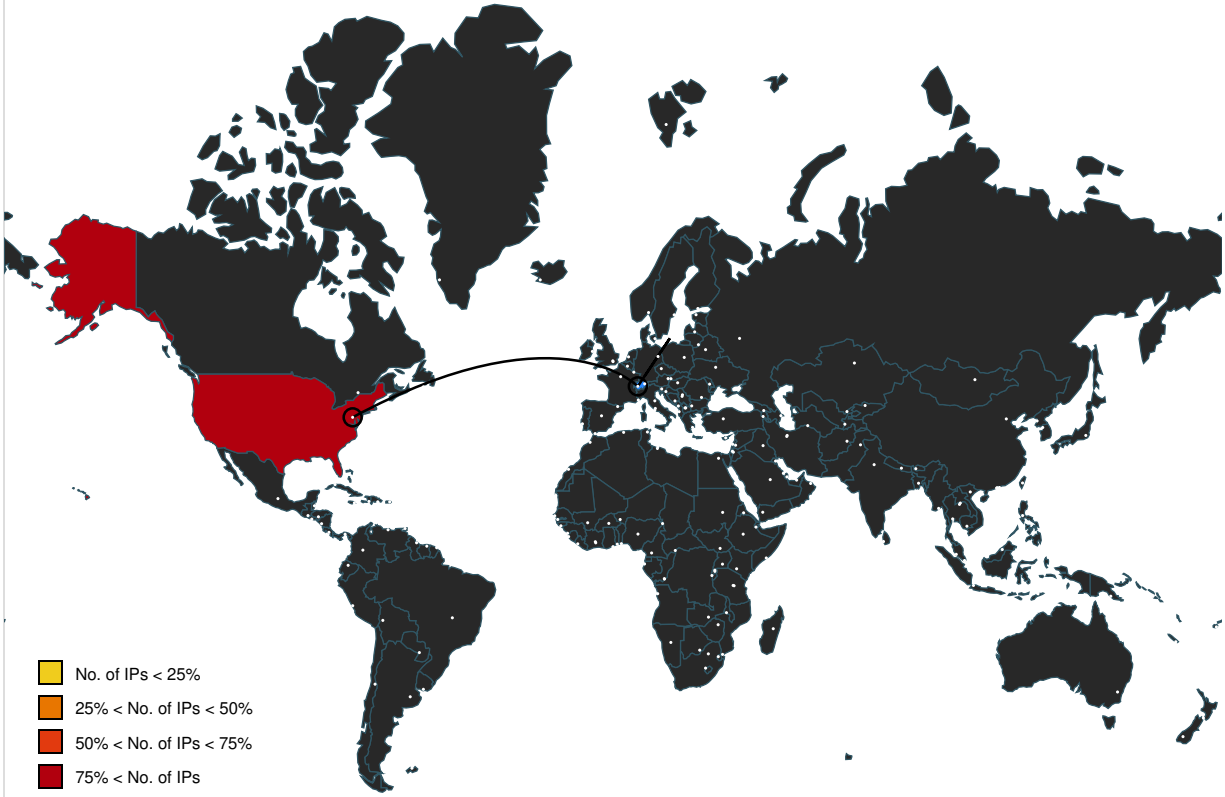
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	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://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

Copyright Joe Security LLC 2022

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715060
Start date and time:	2022-10-03 15:44:53 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Milwaukeetool Payment.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:	14
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:	mal60.phis.winHTML@28/0@7/6
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): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123
- Excluded domains from analysis (whitelisted): fs.microsoft.com, edgedl.me.gvt1.com, unitedstand.z13.web.core.windows.net, update.googleapis.com, clientservices.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

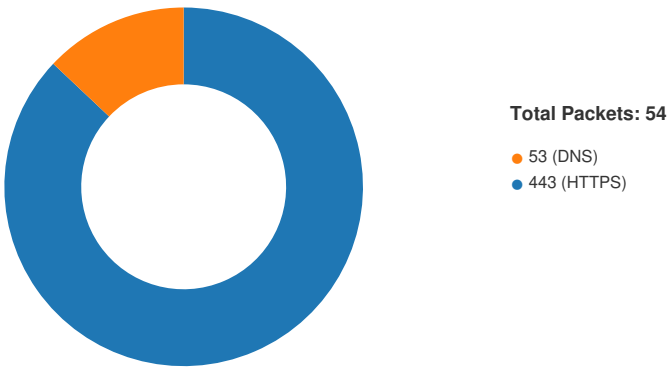
Static File Info

General

File type:	HTML document, ASCII text, with very long lines (4733), with CRLF line terminators
Entropy (8bit):	4.846047582522636
TrID:	• HyperText Markup Language (28028/1) 100.00%
File name:	Milwaukeetool Payment.hTml
File size:	4936
MD5:	148dbfa4a28fb631b5b4180c98daf28d
SHA1:	6f731eb3f50a128dab017b2fe83cbb03219a91d4
SHA256:	58bb9db8b22c7b91c7c494b9a2d65a40a82cf9a7fc6ab1168e2ef6f105f7b7fb
SHA512:	109cb1ce2e43b86e40e1f3daa22eb239c01054feae95a642c7f7b73d87d7d2283cbe688e04099f3a108820fb1fdf0ea68c0e8bc620f84056b555281b18eda66f
SSDEEP:	96:/wNPvtA8MwTlN6f9jjOpJSfyQlfzUUm8qYPYzD0gcYnThF70gR6UX:/wNXtnTlN6fljOpjhqYPYkgcYnThZRX
TLSH:	55A1BCC47FA8E11B079E4E5BFA16A9CFE17A59A7A88822038214F94C29F4509C5ED835
File Content Preview:	<script language=javascript>function _0x3f84(_0x396e53,_0x4f6a6b){var _0x18e8bd=_0x3b38();return _0x3f84=function(_0x5defaf,_0x1c9ef8){_0x5defaf=_0x5defaf-0x160;var _0x381c3f=_0x18e8bd[_0x5defaf];return _0x381c3f;},_0x3f84(_0x396e53,_0x4f6a6b);}var _0x1fa

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:45:54.993968964 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:54.994052887 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:54.994146109 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:54.999108076 CEST	49693	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:54.999145031 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:54.999217033 CEST	49693	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.002243042 CEST	49695	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.002289057 CEST	443	49695	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.002397060 CEST	49695	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.003237009 CEST	49696	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.003283978 CEST	443	49696	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.003349066 CEST	49696	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.003926992 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.003959894 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.004903078 CEST	49693	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.004925966 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.005387068 CEST	49695	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.005435944 CEST	443	49695	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.006100893 CEST	49696	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.006129980 CEST	443	49696	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.090156078 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.098866940 CEST	49693	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.098906994 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.102360964 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.102442980 CEST	49693	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.120332003 CEST	443	49695	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.124463081 CEST	49695	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.124499083 CEST	443	49695	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.128324986 CEST	443	49695	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.128452063 CEST	49695	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.133354902 CEST	443	49696	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.135584116 CEST	49696	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.135623932 CEST	443	49696	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.136214972 CEST	443	49696	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.136305094 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.136351109 CEST	49696	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.137074947 CEST	443	49696	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.137168884 CEST	49696	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.189086914 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.189155102 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.191040993 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.191081047 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.191139936 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.193635941 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.193742037 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.193773031 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.402908087 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.403394938 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.540846109 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.540879965 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.541136026 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.541398048 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.541454077 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.541665077 CEST	49693	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.541701078 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.541829109 CEST	49695	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.541867018 CEST	443	49695	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.541939020 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.542071104 CEST	443	49695	142.250.203.109	192.168.2.6

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:45:55.542335987 CEST	49696	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.542381048 CEST	443	49696	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.542609930 CEST	443	49696	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.543224096 CEST	49693	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.543258905 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.576632023 CEST	49697	443	192.168.2.6	142.250.203.100
Oct 3, 2022 15:45:55.576709032 CEST	443	49697	142.250.203.100	192.168.2.6
Oct 3, 2022 15:45:55.576983929 CEST	49697	443	192.168.2.6	142.250.203.100
Oct 3, 2022 15:45:55.580363989 CEST	49697	443	192.168.2.6	142.250.203.100
Oct 3, 2022 15:45:55.580425978 CEST	443	49697	142.250.203.100	192.168.2.6
Oct 3, 2022 15:45:55.598562956 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.598644972 CEST	49693	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.598670006 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.598809958 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.598865986 CEST	49693	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.606863976 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.613852978 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.614083052 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.614334106 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.643161058 CEST	49693	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.643193007 CEST	443	49693	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.643973112 CEST	49691	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.644002914 CEST	443	49691	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.645345926 CEST	443	49697	142.250.203.100	192.168.2.6
Oct 3, 2022 15:45:55.651815891 CEST	49695	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.651851892 CEST	443	49695	142.250.203.109	192.168.2.6
Oct 3, 2022 15:45:55.651891947 CEST	49696	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.651904106 CEST	443	49696	142.250.203.110	192.168.2.6
Oct 3, 2022 15:45:55.660098076 CEST	49697	443	192.168.2.6	142.250.203.100
Oct 3, 2022 15:45:55.660151958 CEST	443	49697	142.250.203.100	192.168.2.6
Oct 3, 2022 15:45:55.663235903 CEST	443	49697	142.250.203.100	192.168.2.6
Oct 3, 2022 15:45:55.663568974 CEST	49697	443	192.168.2.6	142.250.203.100
Oct 3, 2022 15:45:55.751873970 CEST	49695	443	192.168.2.6	142.250.203.109
Oct 3, 2022 15:45:55.751935005 CEST	49696	443	192.168.2.6	142.250.203.110
Oct 3, 2022 15:45:55.855897903 CEST	49697	443	192.168.2.6	142.250.203.100
Oct 3, 2022 15:45:55.855950117 CEST	443	49697	142.250.203.100	192.168.2.6
Oct 3, 2022 15:45:55.856198072 CEST	443	49697	142.250.203.100	192.168.2.6
Oct 3, 2022 15:45:55.904952049 CEST	49697	443	192.168.2.6	142.250.203.100
Oct 3, 2022 15:45:55.905005932 CEST	443	49697	142.250.203.100	192.168.2.6
Oct 3, 2022 15:45:56.005920887 CEST	49697	443	192.168.2.6	142.250.203.100
Oct 3, 2022 15:46:05.634701967 CEST	443	49697	142.250.203.100	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:45:51.985202074 CEST	57686	53	192.168.2.6	8.8.8.8
Oct 3, 2022 15:45:51.985297918 CEST	64382	53	192.168.2.6	8.8.8.8
Oct 3, 2022 15:45:52.010827065 CEST	53	64382	8.8.8.8	192.168.2.6
Oct 3, 2022 15:45:52.012006044 CEST	53	57686	8.8.8.8	192.168.2.6
Oct 3, 2022 15:45:54.848217964 CEST	64382	53	192.168.2.6	8.8.8.8
Oct 3, 2022 15:45:54.865638018 CEST	53	64382	8.8.8.8	192.168.2.6
Oct 3, 2022 15:45:55.461338043 CEST	53107	53	192.168.2.6	8.8.8.8
Oct 3, 2022 15:45:55.487329006 CEST	53	53107	8.8.8.8	192.168.2.6
Oct 3, 2022 15:45:55.542046070 CEST	64601	53	192.168.2.6	8.8.8.8
Oct 3, 2022 15:45:55.561158895 CEST	53	64601	8.8.8.8	192.168.2.6
Oct 3, 2022 15:45:55.585792065 CEST	53	59575	8.8.8.8	192.168.2.6
Oct 3, 2022 15:47:55.458117962 CEST	59881	53	192.168.2.6	8.8.8.8
Oct 3, 2022 15:47:55.477812052 CEST	53	59881	8.8.8.8	192.168.2.6
Oct 3, 2022 15:47:55.483985901 CEST	58917	53	192.168.2.6	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:47:55.509500980 CEST	53	58917	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Oct 3, 2022 15:45:54.865792036 CEST	192.168.2.6	8.8.8.8	d009	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 15:45:51.985202074 CEST	192.168.2.6	8.8.8.8	0xf0c8	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:45:51.985297918 CEST	192.168.2.6	8.8.8.8	0x8eec	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:45:54.848217964 CEST	192.168.2.6	8.8.8.8	0x8eec	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:45:55.461338043 CEST	192.168.2.6	8.8.8.8	0xab04	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:45:55.542046070 CEST	192.168.2.6	8.8.8.8	0x27d2	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:47:55.458117962 CEST	192.168.2.6	8.8.8.8	0x965a	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:47:55.483985901 CEST	192.168.2.6	8.8.8.8	0x1472	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
Oct 3, 2022 15:45:52.010827065 CEST	8.8.8.8	192.168.2.6	0x8eec	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:45:52.012006044 CEST	8.8.8.8	192.168.2.6	0xf0c8	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Oct 3, 2022 15:45:52.012006044 CEST	8.8.8.8	192.168.2.6	0xf0c8	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:45:54.865638018 CEST	8.8.8.8	192.168.2.6	0x8eec	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:45:55.487329006 CEST	8.8.8.8	192.168.2.6	0xab04	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:45:55.561158895 CEST	8.8.8.8	192.168.2.6	0x27d2	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:47:55.477812052 CEST	8.8.8.8	192.168.2.6	0x965a	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:47:55.509500980 CEST	8.8.8.8	192.168.2.6	0x1472	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49691	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-10-03 13:45:55 UTC	0	OUT	GET /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 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda X-Goog-Update-Updater: chromecrx-104.0.5112.81 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-10-03 13:45:55 UTC	3	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-fMO50DUDGZRLMsou00AjEw' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 03 Oct 2022 13:45:55 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5754 X-Daystart: 24355 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-10-03 13:45:55 UTC	3	IN	Data Raw: 32 63 39 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 37 35 34 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 32 34 33 35 35 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 2c9<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5754" elapsed_seconds="24355"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-10-03 13:45:55 UTC	4	IN	Data Raw: 6d 78 76 59 6e 4d 76 4e 7a 49 30 51 55 46 58 4e 56 39 7a 54 32 52 76 64 55 77 79 4d 45 52 45 53 45 5a 47 56 6d 4a 6e 51 51 2f 31 2e 30 2e 30 2e 36 5f 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 Data Ascii: mxvYnMvNzI0QUFXNV9zT2RvdUwyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" si
2022-10-03 13:45:55 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

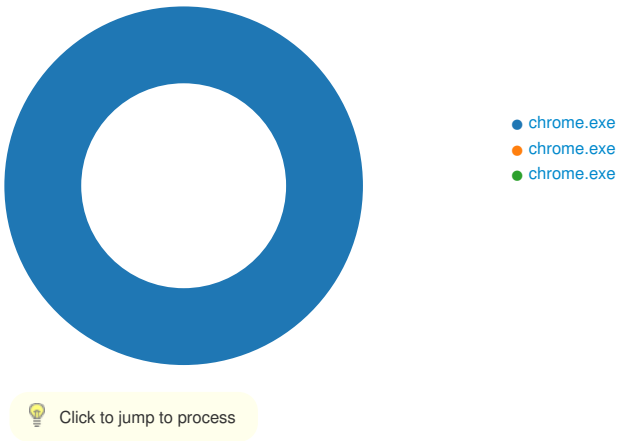
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49693	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-10-03 13:45:55 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: __Secure-ENID=6.SE=Md0Ynyf9ahpkx1CxTGF0vY434NJ6ymH-gDl2Tl5Ly-NQYGPjnNfggtiFRMAwx4JRDOC_gavEPcD5cTBJzUgtbJobmBEuJ8xi2UuotxvOZgApoqSIg1b0RP47U08XG8Bz_SExSzKy0ETSsajbToDlYyFsxfl93p7AyRAd-OeIBA0; CONSENT=PENDING+070

Timestamp	kBytes transferred	Direction	Data
2022-10-03 13:45:55 UTC	1	OUT	Data Raw: 20 Data Ascii:
2022-10-03 13:45:55 UTC	1	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 03 Oct 2022 13:45:55 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-platform=*, ch-ua-platform-version=* Content-Security-Policy: script-src 'report-sample' 'nonce-TstWCeDkfcAsAGTij6MZkw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'unsafe-inline' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport/allowlist Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-10-03 13:45:55 UTC	3	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-10-03 13:45:55 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5772, Parent PID: 1420

General

Target ID:	0
Start time:	15:45:48

Start date:	03/10/2022
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:	0x7ff6f9750000
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: **5940**, Parent PID: **5772**

General

Target ID:	1
Start time:	15:45:49
Start date:	03/10/2022
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=1956 --field-trial-handle=1700,i,2030005579113327324,13011269261470832477,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6f9750000
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: **4912**, Parent PID: **1420**

General

Target ID:	2
Start time:	15:45:50
Start date:	03/10/2022

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\Milwaukeetool Payment.hTml
Imagebase:	0x7ff6f9750000
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