ID: 468969
Cookbook: browseurl.jbs
Time: 18:01:24
Date: 20/08/2021
Version: 33.0.0 White Diamond

Table of Contents

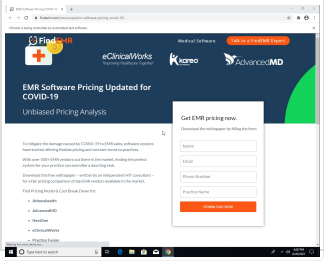
Windows Analysis Report https://nxm7qtkm.r.us-east-1....

Overview

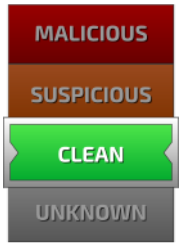
General Information

Sample URL:	https://nxm7qtkm.r.us-east-1.awstrack.me/L0/https:%2F%2Fwww.findemr.com%2Fr...e46e8282-c9b4-471e-8ced-e85be6830ecf-000000/X8kT0A8I5y43QpMcpToFLRdF4Mk=232
Analysis ID:	468969
Infos:	

Most interesting Screenshot:



Detection

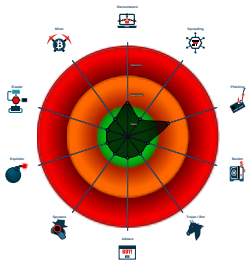


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Found iframes
- No HTML title found
- Form action URLs do not match mai...

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3108 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://nxm7qtkm.r.us-east-1.awstrack.me/L0/https:%2F%2Fwww.findemr.com%2Fresources%2Femr-software-pricing-covid-19%2F/2/0100017b644021e1-e46e8282-c9b4-471e-8ced-e85be6830ecf-000000/X8kT0A8I5y43QpMcpToFLRdF4Mk=232' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4892 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1608,9865191421646431568,12435009540188830314,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1672 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

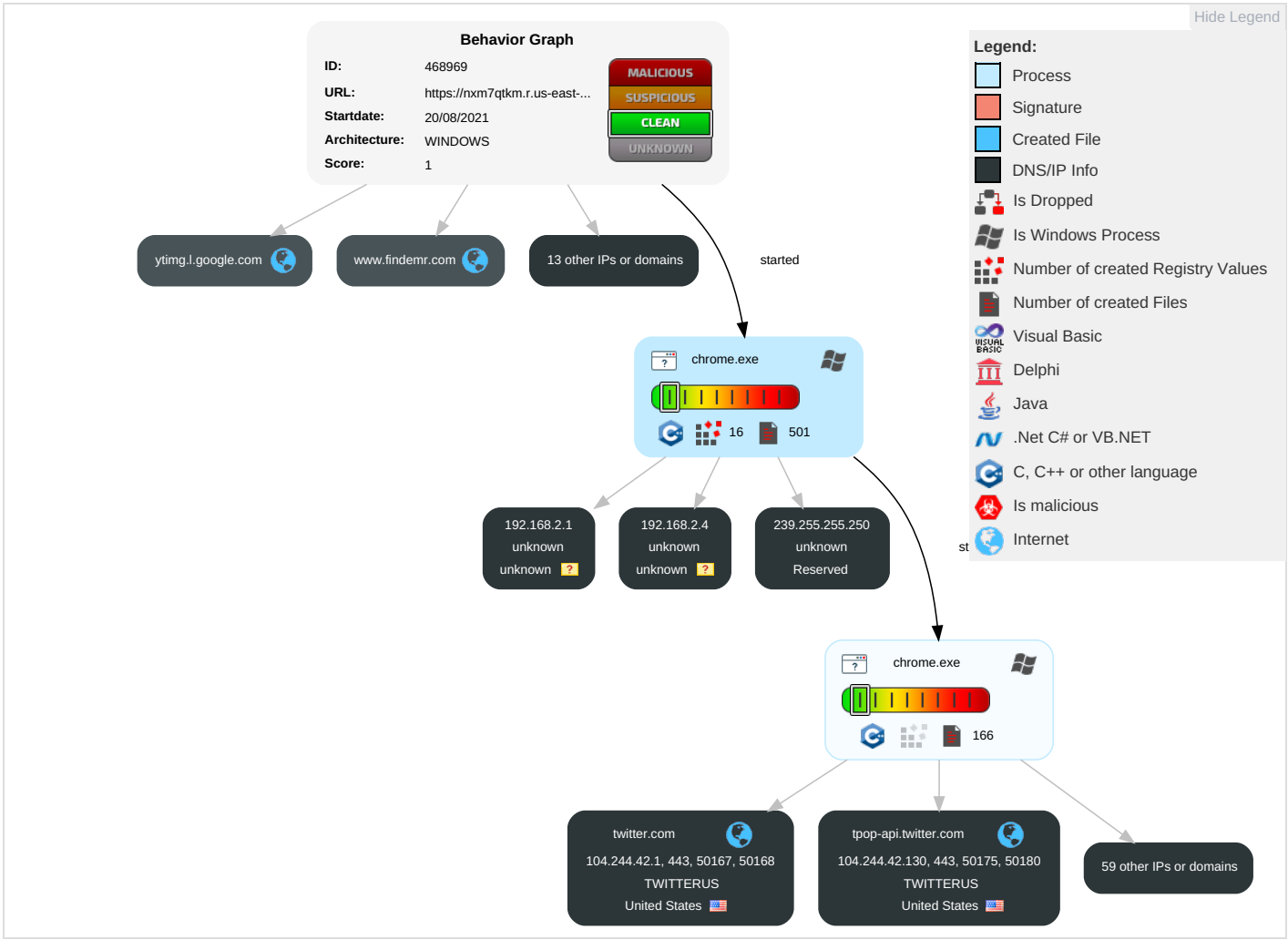
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
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	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
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	Ingress Tool Transfer 1	SIM Card Swap	

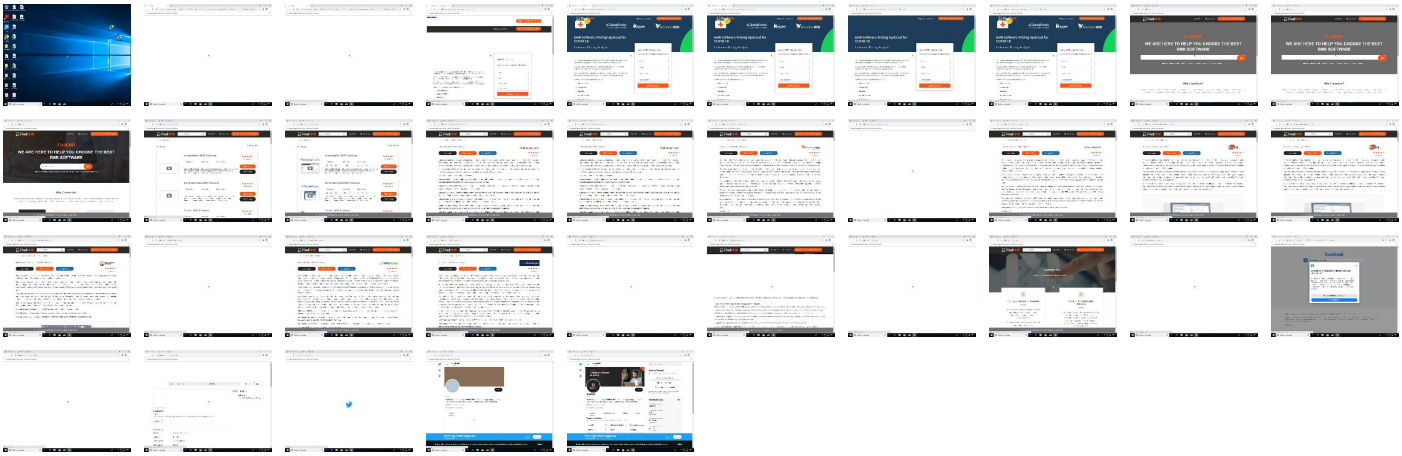
Behavior Graph

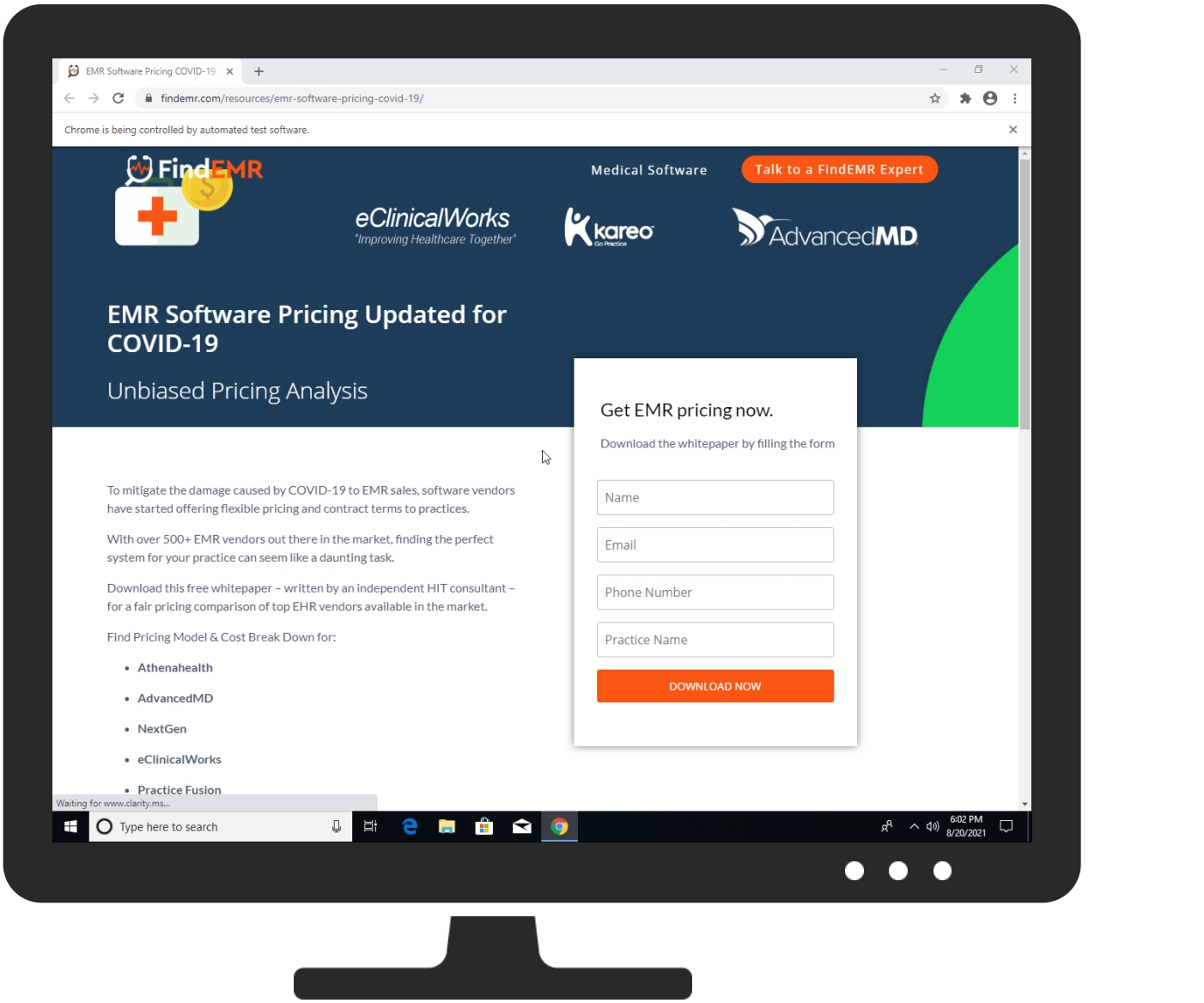


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://nxm7qtkm.r.us-east-1.awstrack.me/L0/https:%2F%2Fwww.findemr.com%2Fresources%2Femr-software-pricing-covid-19%2F/2/0100017b644021e1-e46e8282-c9b4-471e-8ced-e85be6830ecf-000000/X8kT0A8I5y43QpMcpToFLRdF4Mk=232	0%	Virustotal		Browse
http://https://nxm7qtkm.r.us-east-1.awstrack.me/L0/https:%2F%2Fwww.findemr.com%2Fresources%2Femr-software-pricing-covid-19%2F/2/0100017b644021e1-e46e8282-c9b4-471e-8ced-e85be6830ecf-000000/X8kT0A8I5y43QpMcpToFLRdF4Mk=232	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.findemr.com/resources/wp-content/plugins/wp-rocket/assets/js/lazyload/16.1/lazyload.min.	0%	Avira URL Cloud	safe	
http://https://www.findemr.com/catalog/view/javascript/review_filter.jsa	0%	Avira URL Cloud	safe	
http://https://www.findemr.com/athenahealth-ehr-software	0%	Virustotal		Browse
http://https://www.findemr.com/advancedmd-ehr-softwareAdvancedMD	0%	Avira URL Cloud	safe	
http://https://www.findemr.com/chartlogic-ehr-suiteB	0%	Avira URL Cloud	safe	
http://https://www.findemr.com/resources/emr-software-pricing-covid-19/#wpcf7-f1841-p1579-o1	0%	Avira URL Cloud	safe	
http://https://www.findemr.com/catalog/view/javascript/review_filter.jsaD	0%	Avira URL Cloud	safe	
http://https://twitter.github.io/birdwatch/join	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.184.195	true	false		high
vc-live-cf.hotjar.io	52.84.174.67	true	false		unknown
apexsol.us	217.79.240.66	true	false		unknown
tpop-api.twitter.com	104.244.42.130	true	false		high
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
t.co	104.244.42.5	true	false		high
www.findemr.com	172.67.179.161	true	false		unknown
script.hotjar.com	52.84.174.78	true	false		high
facebook.com	31.13.92.36	true	false		high
www.google.com	142.250.185.164	true	false		high
baconredirects-elb-1w79jy7i6g0wf-1154668140.us-east-1.elb.amazonaws.com	3.229.3.83	true	false		high
cs510.wpc.edgecastcdn.net	152.199.21.141	true	false		high
ytimg.l.google.com	216.58.212.174	true	false		high
static-cdn.hotjar.com	52.84.174.89	true	false		high
star-mini.c10r.facebook.com	31.13.92.36	true	false		high
cs531.wpc.edgecastcdn.net	192.229.220.133	true	false		high
star.c10r.facebook.com	31.13.92.10	true	false		high
twitter.com	104.244.42.1	true	false		high
accounts.google.com	172.217.18.109	true	false		high
www-google-analytics.l.google.com	142.250.186.142	true	false		high
stats.l.doubleclick.net	74.125.140.157	true	false		high
plus.l.google.com	142.250.185.142	true	false		high
www-googletagmanager.l.google.com	142.250.186.168	true	false		high
vars.hotjar.com	52.84.174.120	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
in-live.live.eks.hotjar.com	52.51.140.204	true	false		high
www.google.co.uk	142.250.186.163	true	false		unknown
cs672.wac.edgecastcdn.net	192.229.233.50	true	false		high
clients.l.google.com	216.58.212.174	true	false		high
googlehosted.l.googleusercontent.com	216.58.212.161	true	false		high
abs.twimg.com	unknown	unknown	false		high
in.hotjar.com	unknown	unknown	false		high
f.clarity.ms	unknown	unknown	false		unknown
api.twitter.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
vc.hotjar.io	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
nxm7qtkm.r.us-east-1.awstrack.me	unknown	unknown	false		unknown
video.twimg.com	unknown	unknown	false		high
c.clarity.ms	unknown	unknown	false		unknown
img.youtube.com	unknown	unknown	false		high
web.facebook.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
www.clarity.ms	unknown	unknown	false		unknown
www.linkedin.com	unknown	unknown	false		high
pbs.twimg.com	unknown	unknown	false		high
static-exp1.licdn.com	unknown	unknown	false		high
static.xx.fbcdn.net	unknown	unknown	false		high
media-exp1.licdn.com	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.findemr.com/athenahealth-ehr-software	false	• 0%, Virustotal, Browse	unknown
http://https://www.findemr.com/medical-software	false		unknown
http://https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!1d3305.994611532281!2d-118.47036858544482!3d34.04400932561276!2m3!1f0!2f0!3f0!3m2!1i1024!2i768!4f13.1!3m3!1m2!1s0x80c2bbcf1c886929%3A0x8c3b11f0bc3b2f88!2s12100%20Wilshire%20Blvd%20%231630%2C%20Los%20Angeles%2C%20CA%2090024%2C%20USA!5e0!3m2!1sen!2s!4v1583746873545!5m2!1sen!2s	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.229.3.83	baconredirects-elb-1w79jy7i6g0wf-1154668140.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
31.13.92.36	facebook.com	Ireland		32934	FACEBOOKUS	false
217.79.240.66	apexsol.us	Netherlands		29802	HVC-ASUS	false
142.250.185.142	plus.l.google.com	United States		15169	GOOGLEUS	false
142.250.184.195	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
192.229.233.50	cs672.wac.edgecastcdn.net	United States		15133	EDGECASTUS	false
104.244.42.130	tpop-api.twitter.com	United States		13414	TWITTERUS	false
74.125.140.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.18.109	accounts.google.com	United States		15169	GOOGLEUS	false
52.84.174.89	static-cdn.hotjar.com	United States		16509	AMAZON-02US	false
142.250.186.142	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
52.84.174.120	vars.hotjar.com	United States		16509	AMAZON-02US	false
216.58.212.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.13.92.10	star.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
142.250.185.164	www.google.com	United States		15169	GOOGLEUS	false
152.199.21.141	cs510.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
216.58.212.174	ytimg.l.google.com	United States		15169	GOOGLEUS	false
52.51.140.204	in-live.live.eks.hotjar.com	United States		16509	AMAZON-02US	false
104.244.42.1	twitter.com	United States		13414	TWITTERUS	false
142.250.186.163	www.google.co.uk	United States		15169	GOOGLEUS	false
192.229.220.133	cs531.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
104.244.42.5	t.co	United States		13414	TWITTERUS	false
172.67.179.161	www.findemr.com	United States		13335	CLOUDFLARENETUS	false
52.84.174.67	vc-live-cf.hotjar.io	United States		16509	AMAZON-02US	false
142.250.186.168	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	468969
Start date:	20.08.2021
Start time:	18:01:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://nxm7qtkm.r.us-east-1.awstrack.me/L0/https:%2F%2Fwww.findemr.com%2Fresources%2Femr-software-pricing-covid-19%2F/2/0100017b644021e1-e46e8282-c9b4-471e-8ced-e85be6830ecf-000000/X8kT0A8l5y43QpMcpToFLRdF4Mk=232
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@50/658@43/30

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.findemr.com/resources/emr-software-pricing-covid-19/#jupiterx-main • Browse: https://www.findemr.com/ • Browse: https://www.findemr.com/medical-software • Browse: https://www.findemr.com/athenahealth-ehr-software • Browse: https://www.findemr.com/advancedmd-ehr-software • Browse: https://www.findemr.com/eclinicalworks-ehr-software • Browse: https://www.findemr.com/nextgen-healthcare-ehr-software • Browse: https://www.findemr.com/modernizing-medicine-healthcare-it-suite • Browse: https://www.findemr.com/wrs-health-ehr-software • Browse: https://www.findemr.com/chartlogic-ehr-suite • Browse: https://www.findemr.com/lead-generation-services • Browse: https://www.findemr.com/contact-us • Browse: https://web.facebook.com/findemr/ • Browse: https://www.linkedin.com/company/find-emr/ • Browse: https://twitter.com/find_emr
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:03:28	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\2A7611428D62805A3E4E5BC4103D82E4_93980168F338F037DAF9798B595DCB15	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.185056689581701
Encrypted:	false
SSDEEP:	6:J0MlY0CXVt5o78tjTZTQwX/YwF5Z8ukEnhNFLmZH5HH2ARiSUlIfNrJBNqGqwB1P:JY0CXX5FZT5x7m5vYerJBg8JPTGs
MD5:	B92448273EDB777B2D823EF3F26752E9
SHA1:	B73AD10A1A4DA7149A9BA9D747F63E5916AB1081
SHA-256:	42FFF6069929C4C11EA4B38D83717755C49CE8440DBB1241194E69E9D97D568B
SHA-512:	7FD14BD2447F63772D4F3C3E550369957C83444DCC7FB5001D3D7754F1608255DDDAD3E3DA8D3E0382948BAD0805EF162E8945452CA5C41304B954775BB5D5E
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....>.i...G..&....cd+...20210819003349Z0s0q0I0...+.....(..A..B..G@B.X....>.i...G..&....cd+.....y..]"g.....PX....20210819003349Z....20210826003349Z0...*.H.....N.H.....w.(>...I....?..9=..x".<.).i.c...u..]_...1..i...&...>b..7.....Md,..Q.....%S.k..9.X#....~..>2.M...Cg....>H.+...l$;[./.`..^.3.....E'..Z.ATM...'..}..&....].;.....B...|..../.... .rr..D?{.H...\..2zwq.....<f4.8.g.8..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2A7611428D62805A3E4E5BC4103D82E4_93980168F338F037DAF9798B595DCB15	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.8722222696956345
Encrypted:	false
SSDEEP:	12:3sneDmxMiv8sF1JbqDkwJr0iwUauIoZ1PsaneDmxMiv8sF1JbqDkwJr0iwUaui:osmxxvnFqYwJlTJsmxxvnFqYwJl8
MD5:	0D750CE12A336F4A640CC9BBA0BD310C
SHA1:	7E648A860F4984C806EFFE351236FE6566FDB094
SHA-256:	FD2848E89C1BF1C760B3D41861DBBD09A0E49BB4464EE9053909C3EA7FA022F8
SHA-512:	1DBB01D695688FB1C75C2D47F4A30B342A318CFC737D9FB56930598744887C813A4C488B754727F1585ED911706692309504 0D924C7594DD4FC5E0E5D7BBBEE8
Malicious:	false
Reputation:	low
Preview:	p..... .....Y(...(..... .....a.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.c.X.e.R.E.A.X.S.J.n.9.o.i.S.9.o.%.2.B.L.U.F.g.%.3.D...".6.1.1.e.7.b.f.f.-.1.d.7."...p..... .....Y(...(.....}.....}..... .....a.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.c.X.e.R.E.A.X.S.J.n.9.o.i.S.9.o.%.2.B.L.U.F.g.%.3.D...".6.1.1.e.7.b.f.f.-.1.d.7."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\1e34dd71-871b-45d3-b45c-66a01bccbdf0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	367902
Entropy (8bit):	6.015153020537832
Encrypted:	false
SSDEEP:	6144:w/RgS2KiFH+075AU8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBq:XS2KiFHt5AJxzurRDn9nfNxF4ijZVtiW
MD5:	DAF415CD485299B6D235FEE594FA8216
SHA1:	5244BE221FC6E494002D300373BD62561FD5575F
SHA-256:	58F0A44FE6FB3CF0FC971AF7BC21E029491986FC88374F1C86BFEDA8A158648E
SHA-512:	48B388C0B37DB4B9B250CD255513D1B50847ACD4563058871DE94FECCB790405058FC574F989AAFC58303BE3EC95CD9CBB7718F3683FA200A1FD902ABB33EAB
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\1e34dd71-871b-45d3-b45c-66a01bccbdf0.tmp	
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.629507737057872e+12,"network":1.629475338e+12,"ticks":5013792474.0,"uncertainty":4366198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjBylY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327398133362

C:\Users\user\AppData\Local\Google\Chrome\User Data\2af0d989-8146-4ded-9f0e-fd68bab86a8f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.737676601237838
Encrypted:	false
SSDEEP:	384:jLUrn9uMdhm3yNnr0vTJ3EDFgH5cGYHrC9Hfx0x958rGHm2B+JX3PgOxxvNu1POw:oK11OJ0EQe3TRdwv3S1Kn9b1C
MD5:	B68063C12A906833324F86E9A4C3A689
SHA1:	EF2AE8E3408383E7ADAA2D599F4A2AC7EC04660D
SHA-256:	D7601E368EAEE39A0CB38898598E9AFD0F28DF68BA61BDEB7BD826A77E746FA0
SHA-512:	043630DF60576DF61DD4EAB7C5F3E5C52816038262EA5AAB18DCDB1E481BEBF309C71608B9DE10B02A48E8600FB1BC10B46A7935CC70C22DE33F39DD90132DF
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...1C8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\3d52483d-fa7e-49de-ab5a-36681612f58a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7379470665030747
Encrypted:	false
SSDEEP:	384:dLUrn9uMxqhdV6Q3yNnr0vTJ3EDFgH5cGYHrC9Hfx0x958rGHm2iA+JX3PgOxxvp:l6K11OJgEQe3TRdwv3S1Kn9b1L
MD5:	B5CAD21AE99559A5FC06785D85ED9753
SHA1:	31FB1880E88B92EB0B41B03772CFB2873A1D8AAE
SHA-256:	7AC4B6FCD44F50B642D797D48147D94362087FEAB2799D85FA9FF2D160C20B1E
SHA-512:	18B2947168FCBC4F940805A292152C035AC0C8F0D8F5AC0941904BCDC4CB083BF2141A722147891703F762B9A302AD06775BD825E6CB7DB5AC713173CB77A905
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...1C8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\49db7853-c077-4ca0-bf84-e9b7e1baaf29.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371466
Entropy (8bit):	6.027485527146988
Encrypted:	false
SSDEEP:	6144:v/RgS2KiFH+075AU8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBq:GS2KiFHt5AJxzurRDn9nfNxF4ijZVtiW
MD5:	3D6CF22C5C38A813C23C5F601119DFFC
SHA1:	77EDEF9926538F652AA6C41E19C63F851AB3B0A4
SHA-256:	A6D1650D84C453151D1A6D3BB1AB26764E144292A01FAB80864DE1EC36015113
SHA-512:	370C872C7690B982D8C29A80302CCFA53B8A47DA2014CAC97318F920ED86EE33789FFE188FB0D7CC84AA66DDA24135AB0F93428600C29AE8F2A94B5FEAD42F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\49db7853-c077-4ca0-bf84-e9b7e1baaf29.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.629507737057872e+12,"network":1.629475338e+12,"ticks":5013792474.0,"uncertainty":4366198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1Qfj oKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP0 5zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075760451"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\55ac8194-166e-45e7-8d8a-ddb682df9839.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7383567978478327
Encrypted:	false
SSDEEP:	384:tLUrn9uMxqhdV6Q3yNnr0vTJ3EDFgH5cGYHrC9Hfx0x958rGHm2B+JX3PgOxxvN+:V6K11OJ0EQe3TRdwv3S1Kn9b1C
MD5:	A3160D7F715A2574E215EBFC450AA226
SHA1:	2B50C237C1C062E746246AB28465B5B3AF6B4775
SHA-256:	2E4CE80F9680F10F1D01ADED9389F5CCA16B14722996E35E897EACB1353D29D9
SHA-512:	20EE13EFDA5C2D6CD09D70541B8A4084FB6C3135C323DDB3DFB9D252E84B46CD44F9E1FB943D8600E5EB45258034084B3867FE45CF8187A43554C16B0C9BC1C
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...1C8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\5ab119f2-fad1-477c-921b-23f3f3bfe4a1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	367901
Entropy (8bit):	6.015153670294746
Encrypted:	false
SSDEEP:	6144:a/RgS2KiFH+075AU8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBq:1S2KiFHt5AJxzurRDn9nfNxF4ijZVtiW
MD5:	D7297D24230447691E75B84D58768472
SHA1:	4E8D942D13F14DFA86609A768C0EA2110D6B118B
SHA-256:	6BBD3606AF3FDAEB19A004B58C9312D2CE2B7BBFCC76EBD5C0DA33BB287D31B9
SHA-512:	73E7A498E91209B3DA18BE7D732A64E0E404BA1F2519971E7FB655351625969D6B751A50ADC3629557EA6E30A08DEB2B54B8967795D19E71DE033E14B5D34738
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.629507737057872e+12,"network":1.629475338e+12,"ticks":5013792474.0,"uncertainty":4366198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1Qfj oKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP0 5zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"1327398133362

C:\Users\user\AppData\Local\Google\Chrome\User Data\7834b270-442c-442c-9e97-7808bc032ebe.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371466
Entropy (8bit):	6.027485960276287
Encrypted:	false
SSDEEP:	6144:A/RgS2KiFH+075AU8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBq:nS2KiFHt5AJxzurRDn9nfNxF4ijZVtiW
MD5:	8AE894D717D9463D271E98E35D5F9882
SHA1:	D966F6E9FB917292DEBDEFB9DC6AE35221B9EA3F
SHA-256:	6E1FA504D59CEBF4EF1BE079AA1ED20EEE260F1B87E2D56716BFC7E63E4AD010
SHA-512:	CCC4474EC4BD280ABE8C830F730C2F1CBB290385C1E6F533995EE516532BBF56B2EE1BF3E09593293D94511F26A7E257974751D9A3C5198DD318561C12D2336E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\7834b270-442c-442c-9e97-7808bc032ebe.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.629507737057872e+12,"network":1.629475338e+12,"ticks":5013792474.0,"uncertainty":4366198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075760451"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\95cf619b-35dd-48f5-b19a-e0f3f7de0be7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	367904
Entropy (8bit):	6.0151528975347155
Encrypted:	false
SSDEEP:	6144:0/RgS2KiFH+075AU8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBq:7S2KiFHt5AJxzurRDn9nfNxF4ijZVtiW
MD5:	C3C998F5EAE2FEE765E3059FEDB6CE90
SHA1:	C2588E61D0005657931055CE022826C8E56C1394
SHA-256:	971B7080E2270993EBB328A18F9D05D830977DAE72DB8A4C8A66096AF41DAD5C
SHA-512:	0E91A90532CBA5D6A47248A48641A15A434566BE66481FBAC8B02D9DE893FDCADA34B115A71B7C6021D44E4780B02EF6F0BBB61E65BC12DB95F1A88230C06E49
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.629507737057872e+12,"network":1.629475338e+12,"ticks":5013792474.0,"uncertainty":4366198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075760451"},"policy":{"last_statistics_update":"1327398133362

C:\Users\user\AppData\Local\Google\Chrome\User Data\96ce7f91-4d11-4c2f-b45d-e79f658fac7f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	367902
Entropy (8bit):	6.015153090971686
Encrypted:	false
SSDEEP:	6144:3/RgS2KiFH+075AU8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBq:OS2KiFHt5AJxzurRDn9nfNxF4ijZVtiW
MD5:	48C352B78FDF511D13407C75214A4568
SHA1:	278A5AEBADB26094BA4CA4E6DFE64D728E7ACAE5
SHA-256:	560C93DECF9C6AE7656B7FD792A3CC3BE05C195A70A55ED8CC5CC555A5BA6943
SHA-512:	F41D180E42C3EE60B048B52279DFF40612B85021C6E7D83FD31A7F29F1E3982C2AEF7CF82E25DF367DCF0CB1870041976449337C729CBC87EE92D16C9F1408FE
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.629507737057872e+12,"network":1.629475338e+12,"ticks":5013792474.0,"uncertainty":4366198.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075760451"},"policy":{"last_statistics_update":"1327398133362

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0e1302ad-e3ed-4d76-b555-79b6ec4b2f4a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.535310796246744
Encrypted:	false
SSDEEP:	384:AZetMLlv8XZ1kXqKf/pUZNCgVLH2HfDNrUKHGV6nTV6gQ54y:cLlmZ1kXqKf/pUZNCgVLH2HfJrUaGV6W
MD5:	C874DE2DBEECC113D3E1CC80B019429E
SHA1:	CBF8DFB548047E487E279B120160A4997E30C05D
SHA-256:	28F458C1C38823688A525C27C4214AF4A862F257D47007BD2ACD704E6A476953
SHA-512:	D4835B69B317C71A6476CF67EEBBCA83E3EF4FA59252986E139D7E1610979491C0B4A7548961F841DFF25C94D2D70DE4DC213BA6A9C35B3EC41E55A5CCA704A1
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13273981333732093","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1a8ed70c-c7c7-432e-8478-d1ba0040f7e0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1374
Entropy (8bit):	5.5959699110307515
Encrypted:	false
SSDEEP:	24:YxyKeUKJS9RAeU9Y6H0UhHKrfwUiyG1KUB6NaUeCpp7wUNRUeIQ:YzeUKJeieU9Y6UUhZUi9KUB6wUeCpxwo
MD5:	3A7D1C34562D1CB947CFA8E30CB4031C
SHA1:	C0A1516A412023874A04D4185C4474C9B790B10C
SHA-256:	EE03F77015EE0196F00CDDAE59DF182EABBB7F1E511A0DA2CA15C3D04FFD4C01
SHA-512:	FB178364BDF8E0F8457025C37122DBCD0A0801808FD47C7FD298E737CB2F00BA853B7EA40F5812D2C69FCC7B908B7AB4676E5EC09BB10FAA96C1852EFDCFB0DE
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1640394188.982516,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507788.982521},{"expiry":1661043792.529627,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507792.529633},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1640394141.210235,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507741.210241},{"expiry":1661043788.28102,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629507788.281025},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\31ca4259-bc42-4aee-bdf4-cd9d9fcb08fa.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	6036
Entropy (8bit):	5.1791376724126845
Encrypted:	false
SSDEEP:	96:nccr8oP9WcL4m9MSKItlkPRJCKL8lki11Z67bOTQVuwn:nccrt985SXVR4KAkiJ6v
MD5:	7C977E84CDBDCBDD25F38A3B86E26B04
SHA1:	0B0BCF84BCABD870EB617062D9F23A2D43EF0B3B
SHA-256:	8D0D1880435D5538D189BFE07725BCB5822B850469AF2B5B318234F5BA94FBE4
SHA-512:	62646F3CCDA416EE3C7284E18A952A08AD300CE335B9D296766E5A4FA3F63ABE2DFF39A79CBEF193F928CE145AE11DFAB5D02B5594D8C8F717D53F28EBF832A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\31ca4259-bc42-4aee-bdf4-cd9d9fcb08fa.tmp

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13273981334122226","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4053a2c0-9492-42b4-9325-1521efb10a2e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.53546451867572
Encrypted:	false
SSDEEP:	384:AZetMLlv8XZ1kXqKf/pUZNCgVLH2HfDNrUKHGu6nTV6gf54+:cLlmZ1kXqKf/pUZNCgVLH2HfJrUaGu6/
MD5:	BF2CBDC380635E9545923CADB7208C01
SHA1:	DF8D7651F8F13EE877A2220D9D7D6E73809713EA
SHA-256:	2DF5CA3E368ACC72601E78482097B01DCBE99189EBE23A97B95C80C3E1698566
SHA-512:	FD4CF9C762EE6825EC6727886E1429178DD3A111ECA63A17D30D946FA4E2647D867E1B0EBB8E96A2700FC3E92ED1F8ACF71BAC31FE287F340C714943235B225
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13273981333732093","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\437f1f73-8d37-4b54-a26a-8dd0f628969c.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1208
Entropy (8bit):	5.576198957991784
Encrypted:	false
SSDEEP:	24:Ypi9RAeUP36H0UhHKrfwUigHlG1KUa1z7aUeCpp7wUNRUeIQ:YpOieUP36UUhZUiHKUcz+UeCpxwUjUeh
MD5:	CAE90C935353F070449F54C2CCB293DA
SHA1:	754013DC4DD74E7328A4575B316CB267779A4579
SHA-256:	6A7B2D55E09F7B944D0B327F9D1A2423D14CC4575CF69F5C36BCEA52B5E2B935
SHA-512:	FF0C8E493631420665F8861069BD907548A0A5FCEF809AB99EA03AF33A626A95B6799D06C0DA8181C5E79587613D9250B80BB065CF280997701B061966E25FCE
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1661043772.037544,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507772.037548},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1640394141.210235,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507741.210241},{"expiry":1661043739.751378,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629507739.751386},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1661043737.991935,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\48e8deb3-e710-46d2-b560-178bedb55028.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19113
Entropy (8bit):	5.571427683063304
Encrypted:	false
SSDEEP:	384:AZetlLlv8XZ1kXqKf/pUZNCgVLH2HfDNrUIHGKxgdQ54F:VLlmZ1kXqKf/pUZNCgVLH2HfJrU8Gpdp
MD5:	D4A600CC682D969F0ED02C73B0A04F8B
SHA1:	18DB92317EED6E974FF484A77C7B69D25D027B55
SHA-256:	B59611D2338AD4A9C9CC4FBD3EE81651A703A2379D6FA1FF454F05A4A5C5A361
SHA-512:	E928973035FD970F42A9467647A9DF798E0876BB5B676AC7DBD94577606312992E1547C2AFB006D579F41BF5A572EFC8D905DFDBC383930CC8FD0594AE743721
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\48e8deb3-e710-46d2-b560-178bedb55028.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13273981333732093","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\491f846a-b293-4e66-a76a-7a14b1a1ed8c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1208
Entropy (8bit):	5.572214783787627
Encrypted:	false
SSDEEP:	24:YphA9RAeUW6H0UhHKrfwUigHlG1KUa1z7aUeCpp7wUNRUeIQ:YpaieUW6UUhZUiHKUcz+UeCpxwUjUeh
MD5:	14ED14431CB9E249540C459A64357EAB
SHA1:	3E8DE7D8CA009CD6552E1E1020BC868CA22E98AA
SHA-256:	8F65398CCD10BBDDE21AAF40C5F182F708E1AEAFD36AA2F6188D29D4643B1FFC
SHA-512:	4568C09CBF1BA57192C78A9CEE74EB8ED270775A9924125D2914B5A58591AB649B93CF2FB0F7BA2A8C0428FA202053DD20A58B13E8C6F987AC8BFCEED7937BF
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1661043782.106131,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507782.106136},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1640394141.210235,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507741.210241},{"expiry":1661043739.751378,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629507739.751386},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1661043737.991935,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\57f7610c-05ea-4c30-b300-6cf33b25772e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5175
Entropy (8bit):	4.882866320311377
Encrypted:	false
SSDEEP:	96:JOTXDHzw1FtHfozZEawEGuG/6VF6JaZbOGbGGF0AZK6rhZ2L3j6UhVD:JOTXDHzw1FtgzZEa3T06VF6JaZbOyG4Y
MD5:	ED82818457C0E92DF85743628B2F3990
SHA1:	00DB3B6DFBBEF6635970C86EB34B39240DDA6044
SHA-256:	4ED8F72E48B83C94E2F71B39AAF53C9EE6627214C8F2B070D435CBC11C060971
SHA-512:	3A87439BDA5F93700C78052C6D142FDD180D23AE09B791813F1D8F1FFF1F79201B901E6E3BB8262B5129B10498A1BECF7018ABC0E377BB39FC7BB30B4A0BE95
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13276573337991347","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13276573337991830","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13276573338159204","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13276573338159208","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c308ae8-d9e1-4244-9635-cd04a72776c7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5819
Entropy (8bit):	5.177975538475755
Encrypted:	false
SSDEEP:	96:nccrCoP9WcL4m9MSKItIk0JCKL8lki11Z67bOTQVuwn:nccrT985SXC4KAkiJ6v
MD5:	58864266358D99F273AF85C05CAE42E6
SHA1:	C74F7BCF17233B5C095AD6A0185174B4AF82C31C
SHA-256:	C1B419733CA371A57515968DD0E83AF960DD1CC54C44F259534ED014F584D01B
SHA-512:	AABE290EBB93CFBA18B418AABA02DE92B69376919935A3656DDFC69AEF8660AD50A72E18253CEF63024A41382A39035125576017396BD929766949CED51165A8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c308ae8-d9e1-4244-9635-cd04a72776c7.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13273981334122226","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6dab6b64-e017-4ee4-8dc6-3b0efa685416.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1207
Entropy (8bit):	5.5755253518975145
Encrypted:	false
SSDEEP:	24:Ypk9RAeUG+6H0UhHKrfwUigHlG1KUa1z7aUeCpp7wUNRUeIQ:YpcieUG+6UUhZUiHKUcz+UeCpxwUjUeh
MD5:	520C5E2E9D5E9245F3AD48CE7E7164CF
SHA1:	84F62CC43FFA481ABC3103DAF9759871BEEFCBF0
SHA-256:	68F5D7999F40F027E4B97D8F122BC2997B1A790D05D0D69CB60D3AC14C90237B
SHA-512:	5A26E15C09C4A2BC3AA4A1DBF558D1331A772FBF6E903579977EC07F35A03C87D86A8F35FEC1B1AD48D4CDABADF587D14214BEAE79EB2EC68700183EB5CD5DBF
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1661043740.373465,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507740.37347},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1640394141.210235,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507741.210241},{"expiry":1661043739.751378,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629507739.751386},{"expiry":1633013040.850112,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477040.850115},{"expiry":1661043737.991935,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\74d0f489-5e68-4944-84ea-f56f2a0770f5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5125
Entropy (8bit):	4.970988059971744
Encrypted:	false
SSDEEP:	96:nccrhAP9pSKIBIk0JCKL8lki11ZmbOTQVuwn:nccrU9pSnC4KAkiJU
MD5:	23B65008FA0AB21D6D7D43F8C21B348F
SHA1:	28395239C2C9FD49B788B024626BEBFD65A1614B
SHA-256:	F11901C103EB6FB2B78E7E05FBE80F8426D707DB094C4CEE0C14F9CD61E270B5
SHA-512:	CE0812E66F3E3279A33DA31BFB8F50F671DF6A2A24B9A486A05CF774C97430DC0E59AB0BCAAA1FBA81AFAFFA14F64179ED6206CB6759566A48DAE2F1B08653EF
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13273981334122226","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\816d09fd-b165-44bf-86a6-fd90b694cfd1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2715
Entropy (8bit):	5.595672296686505
Encrypted:	false
SSDEEP:	48:Yp7FUhzLUZZeUKJeieU9Y6UUhBPEUel1yU3Ui9KUB6pd5lUrPBsmUNbmUe6wUeC5:6UtLUZZeUK4ieU9xUUXcUe/yU3UAKUBq
MD5:	31D0425C18B861E86C206A966443FF24
SHA1:	0BE6D5FE2B99EAB83E12633B88BB39B1C3DADB63
SHA-256:	BEF21B8DDCB946DE171C64BA1540D066CDA194B33B4DB166EA30176023D5F83C
SHA-512:	2ABA2A544C692B6BE9711D2FB09A014162D90DD540A45A322E62898336A503731827A94650B574DD60827A973BB8D12C599447E3870E706ADEBCF33C69ED1232
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\816d09fd-b165-44bf-86a6-fd90b694cfd1.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1661043806.278082,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629507806.278087},{"expiry":1661043805.62458,"host":"l/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629507805.624586},{"expiry":1640394188.982516,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507788.982521},{"expiry":1661043792.529627,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507792.529633},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1645059799.123078,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\86dbcb54-689b-4d4b-b25a-4b6d4493c773.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8e37b1d2-b33f-46f3-a89f-fa33d8762ae6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	3050
Entropy (8bit):	5.593650849334915
Encrypted:	false
SSDEEP:	48:YpmFUaeLUNeUKJeieU9Y6UUhZaDwUEPEUel9yU7Ui9KUB6pX5lUKPBsmUN4OqPeN:xUxLUNeUK4ieU9xUUjUEcUeTyU7UAKUb
MD5:	76390AB4CA602545247CE2384FA8E0D8
SHA1:	BBF366300D52037B4FA30309551BE1EFBD199B7E
SHA-256:	D3C29A4EAF23FEAE03672E381F04A579252D061154BF3CD6AD1D7F0D453515BD
SHA-512:	A4A3D5F64F14D56F7B551533E46713DB51B783449C85EA5A0668F51ED3A2F9072CA979144FE41E303EE51D3E6B76F6FD78B53B8F834B8684E5EB03C0E1E17BB7
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1661043808.374176,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629507808.374182},{"expiry":1661043807.495406,"host":"l/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1629507807.495412},{"expiry":1640394188.982516,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507788.982521},{"expiry":1661043792.529627,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1629507792.529633},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1661043808.505192,"host":"RNsljhzQrppvtsaSJ2jzGCoQt5mAXe0MwslIjeUIK20=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9f5c0eac-ad52-4c9f-abed-1e4674720f43.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9f5c0eac-ad52-4c9f-abed-1e4674720f43.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.091206712488087
Encrypted:	false
SSDEEP:	6:mFfkqpM+q2P923iKKdK9RXXTZIFUtpkfbcZmwPkf6ZMVkwO923iKKdK9RXX5LJ:mHM+v45Kk7XT2FUtpWbc/PW6ZMV5L5KU
MD5:	16CAEE40815E34BCA9B5254493F0DB9D
SHA1:	7874D8F5B1E1ED06B59A233C2D50A3EA39B0031C
SHA-256:	DBDFB799AC8521772FA9208433E975D29DCA9492FD27D472D0125F2B3FF72D84
SHA-512:	5EF4017D89E7FB14861783CE8113F72A7E817EE51C7970013D34808A20C0F60C0D0C16C0B8D9FDB5E84392920D8ACCC0EFB1C2EDAB62767FB215CC83559405F
Malicious:	false
Reputation:	low
Preview:	2021/08/20-18:02:22.826 1afc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/20-18:02:22.831 1afc Recovering log #3.2021/08/20-18:02:22.832 1afc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.091206712488087
Encrypted:	false
SSDEEP:	6:mFfkqpM+q2P923iKKdK9RXXTZIFUtpkfbcZmwPkf6ZMVkwO923iKKdK9RXX5LJ:mHM+v45Kk7XT2FUtpWbc/PW6ZMV5L5KU
MD5:	16CAEE40815E34BCA9B5254493F0DB9D
SHA1:	7874D8F5B1E1ED06B59A233C2D50A3EA39B0031C
SHA-256:	DBDFB799AC8521772FA9208433E975D29DCA9492FD27D472D0125F2B3FF72D84
SHA-512:	5EF4017D89E7FB14861783CE8113F72A7E817EE51C7970013D34808A20C0F60C0D0C16C0B8D9FDB5E84392920D8ACCC0EFB1C2EDAB62767FB215CC83559405F
Malicious:	false
Reputation:	low
Preview:	2021/08/20-18:02:22.826 1afc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/20-18:02:22.831 1afc Recovering log #3.2021/08/20-18:02:22.832 1afc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.148392590938086
Encrypted:	false
SSDEEP:	6:mFfhZM+q2P923iKKdKyDZIFUtpkflLqZmwPkfKMVkwO923iKKdKyJLJ:mTM+v45Kk02FUtpWE/PWKMV5L5KkWJ
MD5:	DA457BC0CFDFA85E47E93DE93E021907
SHA1:	2EC8098A78D545AC139A2538C8EABD90ACEADD85
SHA-256:	794AD02A0ED56297FD4EF17AE02B7EE712A1FE93DD380BB57CE15D49F2C360C5
SHA-512:	7478E67BC9CB5A0B9E2F861DB0191FE32EB5E3B060E22FDAF46DB94E716D527D8B35DC8DEAE546BA4A448CAD83379B5AE49977ECE50BB1E4245AEA26A3BE30BD
Malicious:	false
Reputation:	low
Preview:	2021/08/20-18:02:22.790 1afc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/20-18:02:22.794 1afc Recovering log #3.2021/08/20-18:02:22.795 1afc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old (copy)	
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.148392590938086
Encrypted:	false
SSDEEP:	6:mFfhZM+q2P923iKKdKyDZIFUtpkflLqZmwPkfKMVkwO923iKKdKyJLJ:mTM+v45Kk02FUtpWE/PWKMV5L5KkWJ
MD5:	DA457BC0CFDFA85E47E93DE93E021907
SHA1:	2EC8098A78D545AC139A2538C8EABD90ACEADD85
SHA-256:	794AD02A0ED56297FD4EF17AE02B7EE712A1FE93DD380BB57CE15D49F2C360C5
SHA-512:	7478E67BC9CB5A0B9E2F861DB0191FE32EB5E3B060E22FDAF46DB94E716D527D8B35DC8DEAE546BA4A448CAD83379B5AE49977ECE50BB1E4245AEA26A3BE30BD
Malicious:	false
Reputation:	low
Preview:	2021/08/20-18:02:22.790 1afc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/20-18:02:22.794 1afc Recovering log #3.2021/08/20-18:02:22.795 1afc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\02ba43ee19ce173a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10709
Entropy (8bit):	5.680058637951392
Encrypted:	false
SSDEEP:	192:c1fYDJAmlPUHi/RDdCJ6DcknvKXPBST+wz6oCNgpHyer:cFYtAmlPhRkaZnvWMTddzpH/
MD5:	9427D4EF40F9384E9624CA2C483843C1
SHA1:	60922D9CFABF6EEA48AA22F6B6782D0BE13E4016
SHA-256:	EC41979FF0B9462559563332E90FABCDEB5B974A4EA3B63056D3A59F9F405C05
SHA-512:	184515AD82EEEA224904F0C586BFA979569CF164657E494231028DEDC4D37B691E169DABF63D132D76D95FE93173F9F5C744084CE3B2F823FDCB760E218CB042
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....obU...._keyhttps://www.findemr.com/catalog/view/javascript/lightgallery.min.js .https://findemr.com/...../(/.....S?.c.#...u.^....EU..j...G...A..Eo.....p.e.....A..Eo.....'..`....O....H(.....p.....(S.8..`(.....L`.....(S...`.....(L`.....Q.@b8.....exports...Q.@...V....module....Q.@2|.....define..Qb6.Yd....amd...Qc.....window.....Qb..A.....self..Q.P:..F....Lightgallery..K`....D.....s.....s.....&.\.-....S...s.....&.(.....&.|.&.^.....1...s.....s.....s.....s.....%.&.\..-.!.....,Rd.....I`....DaN...r....$..g#.....`...p...0.....@.-....PP.1.....C...https://www.findemr.com/catalog/view/javascript/lightgallery.min.js.a.....D`....D`&...D`.....`....&...&....&.(S...`.....(L`.....0Rc.....Qb.u1.....e...`....I`....Da....T....(S.x.`.....L`.....TRc&.....Qb...*....I.....Qb2.j.....s.....Qb.'4o....t.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\062e658d1cdb5699_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	339
Entropy (8bit):	5.864016621623657
Encrypted:	false
SSDEEP:	6:mZYGLg68j0qUcSnZAm9Dfcp5m5npFhK6tQF4hs+VpETmdSXAU4cp5m5nPo:EBpcsFfkm5ptyWhVeTm8XL4km5Po
MD5:	EF6E068DF7CB63D49434E5A0E16CBB27
SHA1:	18FBB6712D8B6C1EF64BFF1F80B81AA02CB69F9C
SHA-256:	6B9C3D6D482C6B856EADA32954A31FA75A1434C2867D74FB1901E6B177E68172
SHA-512:	278AA3025FCBE9555C0EB063FCEAD85D075313B7DB3DE83CE25BAEEA5DA12C3771538F575A465B1F383E29B907219DAB17266242D8E7F35F89D4AF4B93E09005
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K.....*@...._keyhttps://www.clarity.ms/eus2-b/s/0.6.22/clarity.js .https://findemr.com/2.A..(/.....3#.....1F....M.....2...Yu-,R.M.2.....A..Eo.....A..Eo.....2.A..(/..-..4A26D8885DF5A12242A3A2D9F3A01B900209D80CE8E3C793501538BB7AC26B001F....M.....2...Yu-,R.M.2.....A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0803a96e55888102_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22207
Entropy (8bit):	5.697360270398044
Encrypted:	false
SSDEEP:	384:XGZ4eFt3hQTZGX2S7Wql0lalVDbQirlKUk44eup:WZtFSZc7WkmR4iryVc
MD5:	747BC2FB638618826C1A0B71D84A63D9
SHA1:	124FB4B5413440E32CD2D36D777874E1FF430F56
SHA-256:	620F9F26139E616DBF3425B86834415D846DDF9E25321E03B2AA738995BEABE6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0803a96e55888102_0	
SHA-512:	343915917AC0061C58594C99D85CA012E900B49E819D354CCFFE3B3A51991E0E639E2667DB40FC7C3E8709882F4B562F0A71EDF1C2D834572861F50D4567EB06
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....._keyhttps://www.findemr.com/catalog/view/javascript/bootstrap/js/bootstrap.min.js .https://findemr.com/.-8..(/.....V.....z. ...$.S..L'.#z\|.\|.A..Eo .....7.....A..Eo.....'.....O.... U..f<(.....,.....(S....`.....HL` .....Q.@>.d.....jQuery.....4QkFx.Q&...Bootstrap's JavaScript requires jQuery...(S..`.....$L`.....Qb.....fn....Qc..=.....jquery....Qc.....split.....K.....LQq...K>...Bootstrap's JavaScript requires jQuery version 1.9.1 or higher....K`....D.q.(..... (...&.(...&...&.Y....&..*..&.(...&...&.Y....&..*..&...i.....*..&...i...+..&..*..g.../..&...*..g...!..*..&...i.....&...&.%.e.....(Rc.....I`....Da....:....$..g!.....P.. P.. ..".."....@.-. ...\P.a.....M...https://www.findemr.com/catalog/view/javascript/bootstrap/js/bootstrap.min.js...a.....D`....D`....D`.....`~...&...&..Q.&.(S.T..`b.... L`.....8Rc.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\104107cc8e95f3da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.638286016393009
Encrypted:	false
SSDEEP:	6:m0R0nYk+f2pome3sCahmJ2x60RGvRvrsy04hyAQShK6t:E++amksCakJqMZtoK
MD5:	A5BA7AED65F149CCC409CE63BC22395B
SHA1:	3ED1EFE5B98F2506DF81B12E69E8ADCA88C2C9B8
SHA-256:	4FA26F7ABEA7BDF9D504FD5B6CEBB3C84B9EE133A81147A548BE76992920BD5B
SHA-512:	4F267AD9E20417D76323B5D9CF3F40C208FFCC4236452651E176BCE829893AECB7866B97E5043A0AA96F444E01F780C3D365BCDFEAFFA30329866D0733E5AD6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....K4Q...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yB/r/EijMuKTodlA.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.....(/.....m.....?#..4....?<.r..d&..(.. .vh.....A..Eo.....t.H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\126a7b581d23f314_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.514914237864433
Encrypted:	false
SSDEEP:	6:m8yYj018IrAr+VVpMqIAXxjQe8ahm4OhK6t:De1tUIV7Ce8aM
MD5:	82E77E49B61C6241CF840E33C54AD210
SHA1:	CB09746F80758F87449F46FB8E6F4E726D502A26
SHA-256:	DCF06BAE0DC8E0A6C92D814FD36FA8B4E11099E0E5FE89886FE47A145C2E6B60
SHA-512:	A52128C752EF1D72661F8A77AD1F247236C8DFE9DFFA06BCEB7771FAD56DEB402FFEDE3F4BB3593BA74356C7317ABF6186F130BFD265665297030598E49DF83
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.NewTweetsPill.68ab1ee5.js .https://twitter.com/.]w..(/.....G5.....J$..,z].wHO.. ....L,.Y..A..Eo.....a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\13bd2d851129203f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.604960746775201
Encrypted:	false
SSDEEP:	3:m+lPCOIOA8RzYkwIAd0CW/KNGKYG8VQML4nVfLxKF9tlHCaxdeLASaUmYe/tlpK+:mFO9YkvwytVQMEnNNQAax5SkYe/ZK6t
MD5:	D54052BC690F1910B14BC9DB302053C0
SHA1:	E164F606F694F1807E09F03B9D2A3D4EF609B2A4
SHA-256:	678C91D6039C80312698B309235EE4BFD5E4049B89E248E554F79F9C21374A51
SHA-512:	D77A0AEB2C58B1CDBF4DD66AA2329F82852833E33B89806DDF2041CF60F59E73A3EC65B9674155CA99D3C9E75937115A30D12CF633274D77B9A7576E7999AD1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.....9....._keyhttps://static-exp1.licdn.com/sc/h/ckvx8rxuibokruuyiz5ft17o7 .https://linkedin.com/#.3..(/.....k...N..BS....._@.6H8C.(...A..Eo.....rDy..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\13fa326e8005ee81_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\13fa326e8005ee81_0	
Size (bytes):	236
Entropy (8bit):	5.6118430912239345
Encrypted:	false
SSDEEP:	6:mwPYk+f2pomN/c7yhmJ2sFI66niQwdqDL/zrnDhK6t:pb++amN/cmkJn7TaD7
MD5:	AD37663A2F245EF212227CA8971ECE8E
SHA1:	BDFF3648E0EFA7A8BFCAD02C7112B027A7FBB270
SHA-256:	45D2B0C6132F25D33D4D72132AC0768F462DF4F4DBAFB5C937A91F1732741596
SHA-512:	0D266F071F427839F85F98BFB83A0A7C3C605A519C08CCF6EE728F6862DA9F81793005626185491ACEE16BF3DB00B2C416DC695B6036F0459FA6990EEDD69725
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...R.S....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yf/r/sMML78B7V0R.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.(...(/.....?.....<. .f.89..Fk..qK....x.Z ..d..G.B.A..Eo....._.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1438ee3dbbae37df_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.594923073343341
Encrypted:	false
SSDEEP:	6:mABp/VYGLSmXZCLR6VJAmmmfmll/sUo7FZyS15llZK6t:p1tJEtsUol5llT
MD5:	1D3E4C4554BBA55D6D6027F047D02716
SHA1:	C5D3DD2241699B809EB5DA297546DC6BA529568E
SHA-256:	DF522523E40465CC0A878EBF343ADBEB170FB09EC3FFE4346F42600E3B04FD5A
SHA-512:	82425F654DE105A2C3A4B21C3D73777EC6CE193E0DF8632EB29A7565F635FB462FB7901806389C5AAC8C67945F5A04850CABB8898A6041D1285A13FC8280C2F2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...*....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-55HZRN7 .https://findemr.com/.I...(/.....S.....B...';3..Z*.....d.A..Eo.....A..Eo .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\165e0fb56b073769_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.738424694616488
Encrypted:	false
SSDEEP:	6:mtEYk+f2pomZC4RI5hmJ2TK6/aiiF5RK6t:7++amZdRwkJyK7r
MD5:	EDD75D9C21A5610DA1DFE6C4812C59C8
SHA1:	79897CA620BB0FAD59862136E962CB22B3B369E5
SHA-256:	67345D70682097CBAD888578B0BBC9975F49014F414EB36C176D26FE2C4F4C3A
SHA-512:	07C93C88BAD708C5505C9F54AEA7823309A3E0957B5C6095B6EADE9255C25FBC75487D96ECF4E0F9AAF447EAFA8C148ACF5041DE2527555FDBEEF8D654840A 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yr/r/O8Xk3-VX5dI.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...(/.....B.....%..9..m.X..0..;...A..Eo .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\176e7d1d913270bc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.452760239886749
Encrypted:	false
SSDEEP:	6:mwh0lXYGL+MIwJJwMir3ZSJilxhm458J/bK6t:dGIwvMLZUD1xN
MD5:	8319E8386B1DF51A4052CA78EA9A21F2
SHA1:	C4E508E2999F6E8C3D8781D5323F95967710C45E
SHA-256:	24FEC2E10A4EE5AD4DA5AC842A1091B0B1ADA6DE4B2A2212E6E29C29D8F342EB
SHA-512:	6DE87A64E21D0E1E45924E270245DFE805AECF374D28A9FC7A097737DD372C3BE2F67BB7E3A1CF369E79B2E2161560522B2B2AF3D4A634654B2DB0944BB476B 8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\176e7d1d913270bc_0	
Preview:	0\r..m.....G.....I....._keyhttps://www.google-analytics.com/analytics.js .https://twitter.com/.K...(/.....:.&..L...jC...1UR@u<$mz.B...u..A..Eo..... ,Y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\185f65919f8657a6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.738847853388139
Encrypted:	false
SSDEEP:	6:mjtgEYk+f2pomJ2iGyhmJ2lbD8JwfrHrOuhK6t:eD++amJ2ivkJ+8GzHH
MD5:	8E0C4788F5AA22B12BB1FB5160975A3C
SHA1:	C557F353DA278F389354A504178E8F3A5A18A9D5
SHA-256:	278F48F9C5E7C2A6BED6DFCAE6154D16BA42B86E251631725AD1B3EC608B13D4
SHA-512:	92167D407399472B24EA227D1248F066C7C7810E0321443876F8B0ADFA67144CF441E27EAF2E5CBC9BC754FA8A0BDB434F09047DE0370AFB67B6C62459A47FB3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y9/r/ugD21mPGNBo.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/1....(/.....#...._.l.....).....~...._..b.A. .Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ada5ae8963a52d7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.71609018594361
Encrypted:	false
SSDEEP:	6:mhl/lXYk+f2pomdMCWXewhmJ2kA6yQ1nAcnK6t:IXz++amdzwkJENQF
MD5:	E7772738858D3E7AAD20C10171B9CE20
SHA1:	C126187A60BD67B14BD81154AFB929B012747C19
SHA-256:	BD68A4FBC55DBEA3B971B32A5D3CAC56802461BC1B70A7CCB4768E8F4B6EC0C1
SHA-512:	64551BD7B0B185066822D7101405751863D43A1D3EB7872DF58F4A469E6F720D9C64533D35B821B41ECDA7D36F6AAA3CE444B40F0DF4080FCA0607934E0475FA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...J..V...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yv/r/GG1Y0sYc7My.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...(/.....i...c..<.%...7.....T....#.!..- .A..Eo.....J.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1b3f46edece6a698_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.578130778895596
Encrypted:	false
SSDEEP:	6:mTpYj018lrAE8SADFvpMi1RPy7YgNpthK6t:kp1tgSIFZPy7l7
MD5:	D67BE3792146E4916384F2BB2A480BF5
SHA1:	E6FDDEF812332A3D6F8A38B624A268DF23DD0C66
SHA-256:	74E4746E93279458C04C25FB5F06AA1927EF8CA80C3F43FE3BA2A7EF99438910
SHA-512:	DA69EF0B35FA65CEC45DBC8F109197277E75518AEA1B67A1E748BD3313FE44B7810DB074EFF02C25BA4884A3F2D8CE77EB48BF7211D093E41F55F865E82A4FC 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...#....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.AppModules.0e5c2325.js .https://twitter.com/.Io..(/.....4.....&.r.....=.....kc ...2.V.A..Eo.....N$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1b6507849f4a04ce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.723443310916106
Encrypted:	false
SSDEEP:	6:mxYk+f2pomBB0yhmJ2kiN1QMwOOx1DbN/RK6t:Y++amb0ykJCjoxLD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1b6507849f4a04ce_0	
MD5:	6E97A132DD286CDC556662BECD3E221A
SHA1:	8B8496C25B215006E969FD1AD33D530D0D8A759F
SHA-256:	D0BA5558AED4A89D72FD0075D8883600E724DA5A70BA934B9DC4C3342DE681A0
SHA-512:	7B1239384A4927E7EDBC657291C2713242D40C59D08B9CB22DD5072430B7D93812C138D941B387589E1E25B729C0ABEF89E7E88388D18518CC8807EBAD98BA4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...B....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y7/r/WxDDRd9GhRI.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...(/.....j.....0.s...Jw[..N.oNB.r. .A..Eo.....1l.r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1de32f08c16e35d3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	98048
Entropy (8bit):	5.820143573029649
Encrypted:	false
SSDEEP:	1536:8sffGK9NW7EQavEznbUDML+dDbN23DTW6vfw8UZofrU5Hx5fCwpRVlmv:f2ANgEKwoYCkBmRv
MD5:	E742E420901BB594ECE3A439A1FF7FFF
SHA1:	532A2F53214280BFC50F50A27966E9BBB178CC57
SHA-256:	4C7ECBBDCFCF7233799E80E464F23567AC9A47114FD6DD46C86001751E870444
SHA-512:	3613A90515D53C04D268C9A0B90D8186F95CCCEBCD2FD129FA5D07577510A23F4EF91DE98B4BBF95543495AEB53CAB3530A2984644EE9A7CC69209CB172E468 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....e....10E01C1AC374F9F9DA2935774E80A8FB2086942937714EA7D52788C2CF15EEFB.....'..]....O!....}.....`&..... .....(S.X..`h.... L`.....(S.p.`.....L`.....0Rc.....Qb.>.....t...`....l`....Da....j.....Q.@^U[.....module....Q.@.....exports ...Qc.d$S....document.(S.....5.a.....Q....a.....a.....a.....a.....Pc.....exportsa..../...l..Q..@.-....\P.a.....O...https://www.findemr.com/resources/wp-incl udes/js/jquery/jquery.min.js?ver=3.5.1.a.....D`....D`t...D`.....`....&...&....&..A.&.(S...a&..`|L.....L`.....Rcd.....*.....QbJ.g&....C.....Qb6..@....r.....Qb>v.....s..... R.....S...Qb~.(.....n.....Qb.Q.\....o.....Qb.....v.....M...QbJ1.....l.....Qb.R.]....y.....QbR.....m.....Qbb..(....x.....Qb...9....E.....Qb6?.....c.....O...QbF?.....w.....Qb>Y.a....S.....Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1e4a37436bf7ba26_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.685568561203371
Encrypted:	false
SSDEEP:	6:mQPYk+f2pomWJxXzhmJ2KK62lFPBiw+4URK6t:lb++amoBzkJsoxL
MD5:	954E0C310DC708EF8B0AC5AEFD1F508B
SHA1:	385B0FC28AA479201A11025D0C79DDFD1023936C
SHA-256:	AED0D32C33590C3CF092EF6BC06A160F2C4CFC2DC20DA985A430CA7A8CAF7042
SHA-512:	AF9B3967B4047B091B35AD4DAC0F72AC0CEA725C34876ABE790BA64291F368343D75DA85D1DC6847D505BC98E3D0AB2CAC6018E26DD7729E36C790D8A4D98F D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....=N...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yZ/r/4pC2DcdajL5.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.....(/.....o.....Y.....NV%.l.l.6.:*De. +..8.)...A..Eo.....^.!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f3859dbdaaea0e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	77448
Entropy (8bit):	5.992310580285465
Encrypted:	false
SSDEEP:	1536:qgkULBAEejaP7pL342aw9oZqgfDNOakyKLk6fa0zLGMCMIUJBa33:lhLGI3pFoZqgfDNOakylk6C0zLQ
MD5:	6E3DC1B81F238D67C097B403F2148620
SHA1:	695A538DAE77422B299975C5794BA439BE2BAF0C
SHA-256:	A4811E0D635623A987C0D56CA0B7300E8E2661C325860712D6D0F7C0B7B4CE9B
SHA-512:	452728383179BEB329713A6E8AE839D4D0E154A890D0CEC8D5EAE176D2E7F1D93818C932F6B9BD56F803DD48A662F0D722EAC45529E6F075523614B1032E442E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f3859dbdaaea0e6_0	
Preview:	0\r..m.....@.....1C0FA65886065ADC351A6159B1C2144B016C4466F66F26E9261EE1FFDFF81489.....'.....O....H-..j.....$...t..... ...@...H.....(...I.....\|.....(S.0..`.....L`.....(S.A..`:.....L`b....A.Rc.....F.....Qb~.....e.....Qb^.s.....n.....M...QbZ.....r.....S...Qb.%.....o.....R....Qb6.`.....s..... Qb*J.....I.....Qb.....c.....Qb.....d.....Qbv$.....h.....Qb.....p.....Qb.^.....v.....Qb...E....m.....Qb.m.....y.....Qb..~2....w.....Qb.....k.....Qb2../....E.....Qb6..$....S.....Qb.~. ....._.....Qbr..F....N.....Qb..aI....x.....Qb~7.e....I.....Qb.^cx....D.....Qb.....C.....Qb...K....R.....Qb.Hr.....z.....Qb.....L.....Qb.mM.....j.....Qb.....A.....Qb.....Y.....Qb.....X.....Qb. ..I....q.....Qb...E....W.....Qb.....U.....Qb.....P.....Qb.8 ....F.....QbfNyp....V.....Qb*..".....J.....Qb.!.....K.....Qb*.....Z.....Qb.M+p....Q.....R...Qb.n.....et....Qbj..i.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f930bc6b80317bc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10899
Entropy (8bit):	5.69966752296808
Encrypted:	false
SSDEEP:	192:vJSL9i/eAJOtyW2y8mdgT5Zsh/TXvGn9JMAQqF28x7BB:vJSZi/eAJSyW2QdEEh/TX2JbF7pn
MD5:	D50F5B8477555DDA10C6614392CE23D7
SHA1:	F2B1F1A7EDEE4F16F5971C5E3E1028EA3F1BA00D
SHA-256:	000140753A609BA3BDE3356735DCC89D58CBAEDB2ACC5ABAA1930A4AA0EED752
SHA-512:	AE5B1A0DE7D8991D3D1FF7E76BA59CF388F4CCD7518966CCE76A3EB9374AA90E1F9E5515DE4635D0AA13C0379DDE80076CBB38CF580C367F9399553AB549D4 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....*0....._keyhttps://www.findemr.com/resources/wp-content/plugins/jet-elements/assets/js/jet-elements.min.js?ver=2.5.6 .https://findemr.com/-....(/..... ....3dn.K....0....}.43...@.*.?...A..Eo.....i.....A..Eo.....'.I.....O.....(.....(S.D..`>.....L`.....(S.-..`.....L`.....HRc .....Qb.>..... .t.....Qb"Q.]....e.....S....M.c....$.....I`....Da.....a.....Qb..d.....initC..Qev.....widgetCountdown.C..Qd.;.....widgetMap...C.$Qg.0.....prepareWaypointOptions..C..Qe bd|.....widgetProgress..C..Qe>.2.....widgetCarousel..C..Qd~t.....widgetPosts.C. Qf*a.R....widgetAnimatedText..C. Qf.M>....widgetAnimatedBox...C.,Qi6.%.....onAn imatedBoxSectionActivated...C. Qf.....widgetImagesLayout..C..Qefo|.....widgetPortfolio.C.$Qg.W.-....widgetInstagramGallery..C.$Qg.....widgetScrollNavigation..C. Qf.? .....widgetSubscribeForm.C. Qf...o....widgetProgressBar...C..Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2070b6ac91e9aa10_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.710992290016928
Encrypted:	false
SSDEEP:	6:mZYk+f2pomHo7whmJ2GBv6Z2kpqWxw/m4phK6t:Q++amBkJ5BK2CqWxxO7
MD5:	AB6AACA2FD0E444743F3A2AF89B8720F
SHA1:	20EAF62B1CD23A5E1EAEC6FF32442680BC3AB3F8
SHA-256:	C0FE8AFBCA64ADF4FD82A95927D9262B1850414C65A74A6FFF95B4C9D000D0B3
SHA-512:	67D79019958AD24B34ED329CC16392DBF929BE56AD0A556988760DEBC036823D11F51D66BAFCBBD8E8A61376B6CB455355573B6C081A90D4A86D4417706DE78
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...f....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yl/r/dH0i5mMgCSJ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/E....(/.....<.....Y..).p.;...X.....8o.Z.K. .....p..A..Eo.....;.3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\21e8ff0e2ad64668_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.58579149829892
Encrypted:	false
SSDEEP:	3:m+l7WjlzA8RzYj0KKKXlMMIrASM2prvlMRUKl9tlHCz/4G+i5Lv3RbwqYEmyJ1pD:m59Yj018IrASNMG+AEW5TRsnyJDK6t
MD5:	9F7808064949636B26B2E94FB27D8C0D
SHA1:	AECB5D8F36EA9FD45CC478C93379F847573FA4F8
SHA-256:	A61ACB18687DEF894436AB8B09B15EE9B6C89A67C962ECDC54ADC813CC07C291
SHA-512:	E81C8A64EFF98DF2A0F77671F5261E8B4A64D5EB1AF29E21AE2EBD71323299C3D72222F91CB4CD1290533011D18DC230580894973B6332CE13EED77AC07EDF5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....3....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.WideLayout.987c83f5.js .https://twitter.com/.]w..(/.....\..cj#....~`;y..q.J.P... ...>/2.A..Eo.....>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\225638b00cf84bd2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\225638b00cf84bd2_0	
Category:	dropped
Size (bytes):	77440
Entropy (8bit):	5.99284411765826
Encrypted:	false
SSDEEP:	1536:r6YB6ULl87FXDEuM1342Z/jqFDgfDNOakyKLJ6Mfwd2jMrMFWEwPK3E:2qjL8+3pRqFDgfDNOakyIJ6Gwd2o
MD5:	C171DABA1089C123DABD88042393CBAC
SHA1:	5654BAC0CB238EB05DB452A5782E13C6487DEB40
SHA-256:	6D20FB80F3BB4AF8EB9F0C987D810C65281ED8A02ABAB193BBC6DD0A6B8EAE3C
SHA-512:	5E5B9563772EC1969B6B730906349A56BE5D9705C4D376DDECDBAA4233D5ACC4256EA77C30711589746C72776240D6A634DDC671549FA50FAF4928FCCF47C43
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....G.....90148DE92D156B2E4DE2CC4EED10767C99D37EF9F004CF0CDE027238F97F96AF.....'.....O....@-...k@.....$...t.....@...H.....(...I.....|.....(S.0..`.....L`.....(S.A..`:.....L`b....A.Rc.....F.....Qb^.....e.....Qb..i....n.....M...Qb.....r.....S...Qb.;.B....o.....R....Qb.z.a....s.....Qb.....l.....Qbn..n....c.....Qb...%....d.....Qb.ew.....h.....Qb>.....p.....Qb.&.....v.....Qb.....m.....Qbn.....y.....Qb...y....w.....Qb.....k.....Qb...g....E.....Qb.....S.....QbF[......_.....Qb..0.....N.....Qb.[.R....x.....Qb.....I.....Qb...1....D.....Qb.o.....C.....Qb..R0....R.....Qb.pm.....z.....QbJv.....L.....Qb.....j.....Qb&l.Y....A.....Qb6..!....Y.....Qb.X(P....X.....Qb.Q.....q.....Qb.....W.....Qb.A.....U.....Qbj.....P.....Qb>..0....F.....QbZ5w.....V.....Qb.Q.L....J.....Qb~.....K.....Qb..&i....Z.....Qbz..i....Q.....R...QbJ.s.....et....Qb./...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\23bc59a8a2ad9a2d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	396
Entropy (8bit):	5.910662879965327
Encrypted:	false
SSDEEP:	6:mcyEYGLQ1PWPYAkFbCTRWHP0kPTbAmIdyEm/b81JhK6t7WVrJ/Cs/b8z/:vtGbCeHPTbgaIl6JKC+/
MD5:	A023FBBBF9BF7A8560FF0E5D2D5DB53B
SHA1:	408EB4AB73A3217192311A0AACD33A532DBFE5EF
SHA-256:	D6D08788C41F1BAD7D8D14B30A5E5C27DD7B386A73441ABBE991A89797CCB499
SHA-512:	94268DC541F3D444BC379149CA0289030ABDE33B4D922A36CA31D639ED0ABFDE1D755E549F4F6931B0CC8B46B8E7CB90F8757A8FD8C9943B1C5CA9F1196A96A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....)......_keyhttps://www.findemr.com/resources/wp-content/themes/jupiterx/lib/assets/dist/js/frontend.min.js?ver=1.23.0 .https://findemr.com/r....(/.....M.u".2R#4.h?.IB...tW.1...A..Eo.....{.....A..Eo.....r....(/.h...3AD5057BC30B189C0376D333E4EBA7563755466F87BBF714FBA8CFBC91C08010...M. u".2R#4.h?.IB...tW.1...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\257a24dd847e48b6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.616225467241978
Encrypted:	false
SSDEEP:	3:m+lSal08RzYkwlAd0CW/KNGKYoVqEPAXPJOVNLxKX9tlHCSil3iQg3bqmFfmulXB:myVYkvwyIqQAfwnN+AFlSqYOqZK6t
MD5:	4AEA69FF245B39EC491012E59E612412
SHA1:	AB85B575444642DC65CCF27D7D34D4DFE1333358
SHA-256:	139B5D53B5B813F6FFA7886A83CC71D5D9CD749E6FF85E46EDC701C8FDA9E51F
SHA-512:	BA5499CFD0F04190D63D9B4D43FFEEFE122066C15D4EA72539A4C3A20639149F89D57153227E279F970B04FA2ACB2D965057086056E0B731C0DC24042FD451F4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....3z...._keyhttps://static-exp1.licdn.com/sc/h/98lptr8kagfxge22q7k1fps8 .https://linkedin.com/%VG..(/.....7.....B.^....ZQ..>?..<,~.l9..Tx.Z...A..Eo.....$..g.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\264a7c94609a57ee_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2332
Entropy (8bit):	5.7154436270888755
Encrypted:	false
SSDEEP:	48:7TVVOxTVKsxTVRVxTVHKxTVqFxTVCexTVUCxTVXe1xTVCRvxTVFxxTVi4:Ps
MD5:	D19BE18A837AC58037F5906218F60233
SHA1:	F5E28F725F30120EF9D6DDA2F07227389E100483
SHA-256:	9B0CDBFCE84EAFEA2EC67DA5729B1C3522639CFD9D14529629564FDA2046169B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\264a7c94609a57ee_0	
SHA-512:	B332A6BB73C7D54329326BE2226C2E2BA1AFE125BA55C1B53A8CD86A7CDFF7C850CAE0578F6EC31C764242AA8421DAB32A8CBCF9D8EAA116EC9ADB0014D0E 7AC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...W....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-N679RDP .https://findemr.com/g.;..(/.....4.....S.2M...O...E.nb[.e.....A..Eo.....h.5.. .....A..Eo.....0\r..m.....P...W....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-N679RDP .https://findemr.com/....(/.....4.....S.2M...O...E. nb[.e.....A..Eo.....8..6.....A..Eo.....0\r..m.....P...W....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-N679RDP .https://findemr.com/.....(/..... .4.....S.2M...O...E.nb[.e.....A..Eo.....Y.....A..Eo.....0\r..m.....P...W....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-N679RDP .https://findemr.com /O.:..(/.....t!.....4.....S.2M...O...E.nb[.e.....A..Eo.....+1.....A..Eo.....0\r..m.....P...W....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-N679RDP .https://findemr.com/.wo..(/.....!/.....4.....S.2M...O...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a6b34e7fd5d46e5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.905493188265503
Encrypted:	false
SSDEEP:	6:mC2YpEWuVnfjlRpK7B5nRgMiTE36cVxG0xMJ2AOllcXjYHH/llhK6t:L/H0nZH05CTE3bG06+l7H//7
MD5:	46A83F8133242C0C14B2183A912A7B78
SHA1:	9D64BDFC7173995EE482C6B94F4466BDB4832AC2
SHA-256:	54FEF0841944C22CCF8569B9127F6040450DB63998918BFDA4B2801CA5F3B0CD
SHA-512:	C6D5EC6B73C071349189BB32852F287FCD457F6DF325D078412CB2F6E2D37689A60575CB2C9C9CC2ED6ABC04E243850E9F6A558D088C0FCB627BD722D4370B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D%j...._keyhttps://apis.google.com/_/scs/apps-static/_/js/k=oz.gapi.en_US.4sn9RO63fqo.O/m=auth2/rt=j/sv=1/d=1/ed=1/am=AQ/rs=AGLTcCO5G qPeHrbNQGs79bP09BnjVkdwag/cb=gapi.loaded_0?le=ili,ipu .https://twitter.com/5xi..(/.....:j.Y}x.>.-)i...D%...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2acdde753f4d732b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.393069747623845
Encrypted:	false
SSDEEP:	3:m+lSGlta8RzYCJhmHfor7RMRA3uG4ItlHCy4ll3KQAMzkE8sa3B4g4mNl/lllpK+:mSltXYZHfY7nuG4rJ5LnerPbK6t
MD5:	D6D319C50B4A1A71A47789DABEB840F6
SHA1:	4822DECC7BB14D019BE4EB0566BEF4D49F027774
SHA-256:	402CDA5FD7E1CC012DA0B9600C0A8F8EC39CA7CA1542A68560B57A1CCEC30F3C
SHA-512:	ADD020BD38715FD8AD411D1860C998C3B294A9A79FA14FA3A5DFE358C0E4EA0901175659CD58894CF86FDC6CDFC580584280A941D43687AAD8422F77A340847
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...Y.M....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/46/1/common.js .https://google.com/>7...(/.....k.n.....J...<@Q.....Q+.h.JO%\\..A..Eo.....<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2b6014ed89b4564e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	26379
Entropy (8bit):	5.589762817436366
Encrypted:	false
SSDEEP:	384:xsTugbHgO2xqOWtj5LgRb0Yy8sFAcRwZGkkJohRqklXX:6TPOWdcOAHZGks81
MD5:	BF911BF1510404259CC38A3C0543E619
SHA1:	86081A2C9CD0A7A0C2A59166559F63AC5B06784F
SHA-256:	62210B67E4752F76FD6046BF74ACAEA12385ABF7ED026266DD8E5EF3C04EB782
SHA-512:	271601D1FFF756F4088218A7E77B2BC5F4C70BA1D1E99899F1119AB75332B194233A18788610A9F5AD11C2A114C46FB2D852914B98D1B47CC72C1A8CFE2F4A95
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c.....Y...._keyhttps://www.findemr.com/catalog/view/javascript/jquery/ui/jquery-ui.js?12 .https://findemr.com/.r6..(/.....b.....;....2...-...!.X.7.....`..}=…A..Eo.....- .....A..Eo.....'.\.....O....he..M.....(S.8..`(.....L`.....(S.T.`^.....L`.....Q.@~s.D....define....Qb..E....amd.....`.....M`.....Qc. .=.....jquery....Q.@>.d.....jQuery....K`....Do.....s.....&.(.....&.z..%&.^.....&.].....(Rc.....I`....Da.....d.....P.....@.-....XP.Q.....I...https://www.findem r.com/catalog/view/javascript/jquery/ui/jquery-ui.js?12...a.....D`....D`....D`.....`z...&...&....&.(S.!..`.....L`.....xRc8.....Qb.....A.....Qb.N.....t.....Qb.%.M....e.....S ...Qb..&....n.....Qbf.f.....s.....QbNVWe....o.....M...Qb.....r.....Qb.<=X....I...i$.....I`....Da.....(S.....Iau.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d04863fbd3162f2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	79672
Entropy (8bit):	6.077866513171963
Encrypted:	false
SSDEEP:	1536:nQrbVlDFePn9UqLWaYx2EXzLTOMCJWAINxraMSF9dz0:QvVXyn9OafEX3qM+WDnrhSF9y
MD5:	FE674C3D05CE321968A1CE58814F800D
SHA1:	D6934FDF67BCDEC1567F428C60B0D76E1693D607
SHA-256:	9F758870D336046FFB39E7A6ABB2029E1EC52333985E922D2D607EE080AEA511
SHA-512:	5847C6E3DEE1CEE8F2044241BA7062F82DEF955491D921CD18EF6E299BB88C60F05A12F52F69756C34D4EE6582D11289F8B6B2CF09140F88973796598346363B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....84C740B630AD9BC7BF28A9B848E0D9519275D4ACB9E790F5D529C98E55DC609F.....'.....O.....5....Aa.....8.....`.....D.....(..... .....,..... ...|.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....QbvC.....n.....QbB..,....q.....Qb.t.....r.....Qb..b"....t.....Qb.....v.....Qb.).<....x.....Qb. .....y.....Qbn.....z.....Qbb.2.....A.....Qbb.....B.....Qb.o._....C.....Qb.Q.....F.....Qb:.(.....E.....Qb*v#c....D.....Qb..u.....G.....Qb..}....H.....Qbn.....J.....Qb...5....I.....Qbf.....K. ....Qb..!.....aa....Qb.....L.....Qb>.....N.....Qb.....O.....Qb*.....P.....Qb&7.C....M.....Qb.5\&....da....Qb..:.....ea....Qb^o#`....Q.....Qb.D.....S.....Qb.....R.....Qb..t.....ia....Qb..C .....U.....Qb.....ha....Qb.G\.....T.....Qb*#.:.....V.....Qb..P.....W.....Qb.n._....Z.....Qb.....Y.....Qb&.....X.....Qb6.....ba....QbnU.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2eda40ed6b465eb3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.469726748555415
Encrypted:	false
SSDEEP:	6:mYr/Yj018IrAzyvL5VpMIcB+ihm4hjDK6t:FT1t/LwonY
MD5:	89719BD5760B7C9D19FCF3104AED2EAF
SHA1:	E5607127272650D3845834FD231711E284109B48
SHA-256:	CC28077441293 97AF65F2ADB2B344D73BBEB5767F0793ED8ADD2D0E5D2CC5693
SHA-512:	1484A75ECF8A30F8D8CFFE9DC2FEF3E1C47D76843388DCE215EDE6B149BA2A23763479F6288A4721A3C4F3D258BC378776C2C4BD335098FE6B0D38AC94F45B C
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...>j.,....._keyhttps://abs.twimg.com/responsive-web/client-web/polyfills.fb7f2a05.js .https://twitter.com/..e..(/.....l.x..../>..X,...C.Qnq..)H...w.A..Eo.....d .U.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3076b464af1e7f12_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1114
Entropy (8bit):	5.489690414279915
Encrypted:	false
SSDEEP:	24:cG54ZZSuMfsz4RVgAHG5VXp2W9RtZBXVajTeRwuj:cOf+GOzNXAS2C
MD5:	C62D6879105609622029583CD620AA19
SHA1:	917C077C5D9DD0E2620B6F5F0363C3F884DE42AA
SHA-256:	4919F0E142B60AB9BDB91991F01C8C7D6D2A4749F48A51A5FB48D3B653C2959A
SHA-512:	9B273DA61B64A616EA2A2C2E6E0FB8EDD088C340CDECD467EB3788F1A3CC1B49846C384F393BE2DEFACBE678B48DFA163A6797FCDA2E9B23A011849233090 FF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z...o....._keyhttps://www.findemr.com/resources/wp-content/plugins/cf7-redirection/js/wpcf7-redirect-script.js .https://findemr.com/Y....(/.....q~..... .m..#U.b..m.6...!....A..Eo.....G:.....A..Eo.....Y....(/.....'.~.....O.....c..$.....\.....(S.T..``.....L`.....L`.....(S.....Iao...d.....d.....$.g..... .....,Qi..J6....wpcf7_redirect_mailsent_handler.E.@.-....IP.....`...https://www.findemr.com/resources/wp-content/plugins/cf7-redirection/js/wpcf7-redirect-script. jsa.....D`....D`....D`....,..`....&...&.(S....Ia....E...IE..a.d.....&.....D&.(S...Ia....~.....d.....$Qg...R....htmlspecialchars_decode.E.d.... .....D`....DI]d.... (.....`.....`.....Q.@.v.X....jQuery....Qc.d$S....document..Qcf".....ready.....K`....Do .....&.'..a9.....&....&.]...&.(...&.....&.Y....&.....$Rc....`.....Ib..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\309e4b792578e647_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.743934310865275
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\309e4b792578e647_0	
SSDEEP:	6:mJRYk+f2pomWr2KN57ehmJ26K4r118P4gXhK6t:a++amyN57ekJ3Izr
MD5:	0BB9C391D2C33B1DCD940BA2EF165F1F
SHA1:	77CABAD27930D1ABD57E658FA607777C2B08A0E8
SHA-256:	83C0E0376EAE4E0B18E033BFCA23AC8AC0BD7BF9768F2F77EC0CB70D3B72ED4C
SHA-512:	2CB6454707C9C87A28A75C2C8E1F2494FB38D42137AE0FCBBB71AC8A81F0030F5CB5D84D3526208C5DA42B6ADD5951A21EF44CDA3D67B592D3DD7F337FBC5D5D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iN_84/yY/l/de_DE/suwOLbpGGk-.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/3..(/.....#..F..q..-.d.i.....m_.<.j..<O..A..Eo.....n+.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\30e1c08eb2678435_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.75441807389961
Encrypted:	false
SSDEEP:	6:mk9Yk+f2pomwxXVhmJ2jNK6fly5GT32YuK6t:x++amKFkJMhy8SD
MD5:	77B22C2A1E169DF28873F1D0ED3F2706
SHA1:	D96AD6824FAB9028861E2EE823D3831D26413E3B
SHA-256:	066490A462111B72C34CAC1EFC4081EA2F0D427C8FFD07B887869A4A1DAF980E
SHA-512:	C0BBB15E47A303B0D1F40C704D177F47C5029D38536396C76BD4856471748E18AB952805F8DF00A646E3EF8408A0240705D2942F41A3E972178A1BB12D107A7A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....D...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yH/r/IdnLC1drx_P.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.$...(/.....{O.E.WZ.1.6.....m^....O..m.7.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\338e768743bd97da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.535031131785142
Encrypted:	false
SSDEEP:	3:m+l1Mv8RzYrSLQ1tpjxCvTOYfPOyRW273AmTAKl9tlHC7aoNHpNxvS4GJoyRmA/R:mYBYGLQ1PsTtRRW2rAm0KlAHntAhK6t
MD5:	238F8E0E3E817A7A6A7492B8FB0EEF0F
SHA1:	8ABBC7A12B608503752BAD30827F07166E8BDECA
SHA-256:	EBE842EDBD4B9DA3FCC4365E2CEA3ED2BE0F8406F3693B75607E0D8E9D7A38FB
SHA-512:	1A36A963AD140777228B1C8F794A421043DFE49129ED1B170A1D8E30699EB645D378068A778DCE06380DDC9028D36399C93175E6CC8AB49A3742BB3700AA3A93
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...&.Gw...._keyhttps://www.findemr.com/catalog/view/javascript/ajax_load_products.js .https://findemr.com/....(/.....Yz.(...J..O.C.....pO.A..Eo.....{..=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3862146bd7a47fe6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270
Entropy (8bit):	5.650310738376888
Encrypted:	false
SSDEEP:	6:mwAPYj018IrAMUowfs21fvspM78tDBDtt/glhK6t:C1thUU22u0rY7
MD5:	2F427897B19724B0B96CC4FDF6528B74
SHA1:	5233224B2FE5252E826D8C3D442AE85D4E8884BF
SHA-256:	7FC2B41DE5FA27206DD7236C4AD7B178A7951EFEEBC3337480E8EE7516F76D9C
SHA-512:	C06CDCF54629B17C27F27C96999DFCEB8FB192F5DED1C81E9C122791EF9D700F6E88A4739AEAF52A7537593214981ED339DBB8EAA18E6BF39CBCBB5910F5BEA5
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~ondemand.EmojiPickerData~ondemand.EmojiPicker.760cff75.js .https://twitter.com/|L...(/.....]N...5j?.^-<...$..ES5.B..[.+...A..Eo.....@../.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\389003c03ef6608a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.581266249279611
Encrypted:	false
SSDEEP:	6:mIxYj018IrADfHsGSdMkYrX4hLezJ2HEQL9bq/9K6t:51tafCYiezJNOy
MD5:	9C0C98EE50752A8827E639E26C509766
SHA1:	3E0831199C5E360DE21F9C67C140968C7ADFDE14
SHA-256:	139D9DAB8ECBE598F4D72C5B49D08173075D262F24EE93091D1BA19807025FE6
SHA-512:	A9EA0D5397B047C30E0A074519B763DC7DF3DEBA00FF15370A468E1A5E1783DA16ACA6A27CEFB0327ED75B40792FE42ECE7519BF2D710A9BA18313374156EE(3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o.....d...._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.CarouselScroller.dc7b3b15.js .https://twitter.com/.....(/.....2.....o.@.M....._.{ .x..?....>..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3d1fc56eda670323_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4611
Entropy (8bit):	5.72172525727614
Encrypted:	false
SSDEEP:	96:2fOXcMznnGaX0lKc20mGYTzdMEb/fUahwFidEca1:2OLnGaklKb0mG8zdXDUgcCDa1
MD5:	805BC7427370CC21779FFCADF2DFD093
SHA1:	B87EC3534E128340AD085C6A57A7E822DEF9B06A
SHA-256:	536A8BB7027AE1A4AFD1CD5FF02AB93C30FDA1EF9B3359AA41DEEA12EBCC73EB
SHA-512:	4AA87674D7D6CFF5B9F7F71CBB61281006575B490C12B049CABEE328B7F7555B0528C98D3AC69CB5F7A35750E84F6B7D637C42F74E6295476082C50EDB0C043I
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V..P...._keyhttps://www.findemr.com/resources/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.2.2 .https://findemr.com/c....(/..... .....=M.)..x.=,A:....J...k..W..A..Eo.....4o.....A..Eo.....'.....O....X.....-.....(S.0..`.....L`.....(S..`d....hL`0....PRc$.....&.....Qb"Q.]....e. ....Qb6..@....r.....Qbnt.....`_.....Qb.>.....t.... Qf...k...__webpack_require__.d.....l`....DaP...:%...(S.....lah.....a...!..@.-....xP.....i...https://www.findemr.com/ resources/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.2.2...a.....D`....D`....D`.....t...`6...&...&....&....&.(S.....5.a.....QbVK .....t..a.....l.....d. .....@.....D&.(S.....a.....a...Qb.A.....d..a-.....l..!..d.....l.....&.(S.....a.....QbF.....e..a....l...l..d.....l.....D&.(S.....a.....Qb..Q.....u..a`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\43312066019b883e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.759384843216628
Encrypted:	false
SSDEEP:	6:mhl9Yk+f2pomWzV2AOa6hmJ2fVGCiJngentdbK6t:Ull++amEOFkJ+Gpt7
MD5:	EDA2D5BB74EF3006A3679A5C4C3DDE8F
SHA1:	C0062FB986A50F8BBF3D139CF6340629C3B41950
SHA-256:	A64738123D6307CEC7EFEC106C9FA3DCE1C6F7E3DBDE94DF3835D9ADC7842F3B
SHA-512:	8809B6134F7EAF41FCEACE2335DC19F7DC51F5F6966150BB914750FEDE0EA30D87C116A289C9B898A965B99784C36D5918E1C127D34C639B88E89520FEE3029I
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...Rn....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iVab4/yz/l/de_DE/kBZhXLbv7No.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.....(/.....'.n....}6k..j ...W.....{.v.a..A..Eo.....s..).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\44e272aba0ec4472_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.75384611627634
Encrypted:	false
SSDEEP:	6:mJ4JPYk+f2pomWwetVwhmJ246910nTRK6t:ZB++amOtVwkJm2Tr
MD5:	5580A0B5E34F0999B8924D5BD2A08B0E
SHA1:	72301FE97CF837C85BAE4923D9BEDBE69A147114

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\44e272aba0ec4472_0	
SHA-256:	FBAB7D5ACC883BE202DC705B684E8EB7B6BAB54C68CDE206C35E3140702790E2
SHA-512:	03E39502477BD1E539479544754F0FAADD1543AECCEE058471F76E343D2679C0B05E9450D3C303C40452C4F245EAD505798E5E0F7CFA91F129E85B377BAB7836
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....D...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i5ED4/yj/l/de_DE/PtMz54lN6G7.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/%#...(/.....k..N...w.....O .yz..^...F..b.?.A..Eo.....Gl.A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\472cb5026948f4c9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	15833
Entropy (8bit):	6.049859734392295
Encrypted:	false
SSDEEP:	384:/Ew/1vmObR741SPoUGisClypFnKU2UTGavhVhG8JC6:5UOISPut4G8Z
MD5:	2A59CD47BD528133DBD0CDA4E6CDBADB
SHA1:	300EBC49BD806F464D4968A23F3C365C2CF54492
SHA-256:	4B782BA5F8E1B276BCDE4069FA7A115CD258EF23725E5EA421F421709D3563EB
SHA-512:	74B232C4769EFB27056730A646DCFAFADD823C6814CC5DDA36EC765C390F9B9802E993763B29FB823963D36C80C0E9C39136300F0F592FE972C9FE06FC12A96
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q.....]L...._keyhttps://www.findemr.com/resources/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2 .https://findemr.com/.l...(/.....n.".0..W._;%. T...\.W.9.L..A..Eo....._.....A..Eo.....'..+....O....8<..t..y.....\.....8.....(S.P..`\.....L`.....Q.@.v.X....jQuery....Qdr..5....migrateMute..(S... `.....4L`.....0Rc.....Qb.>.....t...`$...l`....DaR.....Q.@.....define....Qb.wHv....amd.....`.....M`.....QcNYu]....jquery...(S.....Ia.....I.....@.-....dP.....W...https://www .findemr.com/resources/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2.a.....D`....D`....D`.....!....`....&...&....&..A.&.(S.....`.....L`n....Y.Rc.....L.....Qb~.(.....n.. ...Qb>v.....s.....Qb6..@....r.....R....Qb.Q.\....o.....M...Qb6?.....c.....Qb.....d.....QbJ1.....l.....Qb..'....p.....Qb.Q\]....f.....Qb.R.]....y.....QbR.....m.....QbN..y....h.....Qb..... ..v.....Qb..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4743998f7347e853_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.674330328993765
Encrypted:	false
SSDEEP:	6:my9Yk+f2pomnaYWIhmJ28Tn5849k4rOK6t:X++amna8kJN58J
MD5:	995F1511E32E0E8925B836EB4C6D074C
SHA1:	4A237782486C9B885BB4BD3129BCAB1E97110DC1
SHA-256:	A29D1F4611F1C869A6E685E9A98B213A24AF41AE82BCDB16F08BBCFE5C402F55
SHA-512:	4507BCDCD1ECA881A7FD16E398A11E05A364FF62D3194559170E1CB494F249D6E13A0604BB04720174FC82A71365F3B1BC6FA78FE764649FA3B38922A4C9C754
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....7...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yc/r/wXSoDaesTZV.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/k....(/.....#eK ..{..5E.N..9So.. u,.b..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4968a97794866320_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.391055558321941
Encrypted:	false
SSDEEP:	6:mMnYGLg68j1hHqUcSnZAm916mfvufF63/ZK6t:VVuHpcs11fWfl/T
MD5:	9C4771AB95EF92FA506787F4AD00AB01
SHA1:	5B282607940EB6A033DFAF1ED976EC4D08D571F7
SHA-256:	9C5A319830F7FBE5ADB8F12E51E678F464D7BF949738A54FCE90DEBDE79262F6
SHA-512:	6D256459885584C2117A8CAF575FC3836882502D289EB8679494AD7F9F12887CC1669111F036CCB18F2AC7A36DA192B8BE3D95B04F6C4ABF18F1B2BD351BFCE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...([dA...._keyhttps://www.clarity.ms/eus2/s/0.6.22/clarity.js .https://findemr.com/.\w..(/.....tr.....; .^.E.\.oU.....(..E.h.....M....A..Eo.....B}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a8a84f095ed7c73_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a8a84f095ed7c73_0	
Category:	dropped
Size (bytes):	9176
Entropy (8bit):	5.533861878123211
Encrypted:	false
SSDEEP:	192:w4OUKGWIabzHOhOPm2SAiBdf3BMsR8PSS:OUKewOsJ/ihmPR
MD5:	CF60FEE04E097C26932E0A34FD957A25
SHA1:	F4476C251EF6ED4E6282D49AADC79944624E50DC
SHA-256:	2059B599BE705DF0056DF75A156D0502A2C606D4BC3EF5ECD9E23719E532DA0F
SHA-512:	72B2946477391C634BE5EFDE566BB22C9AE0823869132B07E1687B95AFC536BF0B2C0674102C670D81403DE5A2822E612DBFB12946E0B99FC163D911BA6AC5A0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....._keyhttps://www.findemr.com/resources/wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js?ver=4.0.2 .https://findemr.com/.....(/.....Y.Q.X.D|.....U8.-S.>^.....F.....A..Eo.....{p".....A..Eo.....'../....O...("..~.-.....(S.T..``.....L`.....(S.U..`b.....L`V....@Rc.....Q.@..P.....Waypoint..QdR#7.....keyCounter....Qd.R.....allWaypointsb.....I`....Da....,...(S.....Ia*.....!...!..@.-....|P.....n...https://www.findemr.com/resources/wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js?ver=4.0.2..a.....D`....D`....D`.....`...&...&..a.&..1.&.(S.....5.a.....a.....Qd.g@[....queueTriggera....P...I.....d.....@.....&.(S.....a.....!...Pc.....triggerat.....I..!..d.....@.....&.(S.....a.....Pc.....destroya.....I..d.....@.....&.(S.....a.....Pc.....disable

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d7197ef73378c42_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	93760
Entropy (8bit):	5.772961787278996
Encrypted:	false
SSDEEP:	1536:qxHWQ52MbBy89RhNm7rifXf+EBxkaorPJZXhHnZoGeOiG:CHX2z8B87Yv+EBPknP/7
MD5:	584BA793DE20B8CB65B344645A90BAFB
SHA1:	A1F097F267493C0E2F3EDE5DAB12A072153AE642
SHA-256:	61AA31A526DCA97054422F8AF8D928CE8026187C6BE32102724D260AF3EB7D8B
SHA-512:	4B6BC315B5F22F592C34D5AADEF000A22843C448BDD5D273C488607A27EF28998A5FE07673CA9110EE95CB5FDDCC41035A4FF07DE167825C1F6D5E5C55CD652
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....1.....4F1459C14D5E4673F3830F0B492C5B7C2D5B051795AE15B0F4F1986A59253849.....'..I....O ....I..I.....".....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....L.....Q.@>.}P....module....Qc...!....exports...Qc6.....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.... ...I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.jsa.....D`....D`....D`.....`d...&...&..!.&....&.(S....".`.C.....Q.L`.....q.Rc4.....M...QbF.....d.....Qb.%.M....e.....Qb.....f.....Qb..".....h.....S.....Qb.....j.....Qb.....k.....Qb.<=X....I..Qb..&....n.....QbNVWe....o.....Qbndkl....p.....Qb..5.....q.....Qb.....r.....Qbf.f.....s.....R....Qb.A.[....v.....Qb.....w.....Qb..).....x.....Qb.....y.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4dee3d99323264fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.629961199430886
Encrypted:	false
SSDEEP:	6:mdEYj018IrAojOcFxMAkllSIuzJ0qmonOf/ZK6t:v1t6cKlSz9fOfr
MD5:	2BC5EF5DD7C2065E707D3553EEDA1C16
SHA1:	9E6EFBF1D3B470CB17F6A08427743CBEB4CD9FDD
SHA-256:	2560491CE887E5B16E7E094030D05A3D7D70AD062C470002D42519DB0C3C42D7
SHA-512:	82CD8DA1D93C27DCEAA7908179EC7BDA94E8866F6344DF1DD4671758280AF8B784935E3C79CA8DA39ED1DC6B8CC719C8D976A5F1699EF1C80A87B8F52ADC440
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m.....f...._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.ProfileSidebar.f97315d5.js .https://twitter.com/.<...(/.....!.f...glv.8..2.9....:#k....q.A..Eo.....$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f8bf1d5ee520d01_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4088
Entropy (8bit):	5.705066354875568
Encrypted:	false
SSDEEP:	96:r/zkTZjHONzKCIa6XrtNhL5fdenfJMUtpzL:rbkZ6NzKIOrtNwJMGL
MD5:	7C86DA1367BC6ABECA40ACCB9B2D1083

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f8bf1d5ee520d01_0	
SHA1:	2F50486544C369A1DFF6ABEBACBF5A2643BE3C7F
SHA-256:	D6E0041265C84E60AB1C0F6E58C3AF53DA38C95DFC31809F822E40D996651F4B
SHA-512:	39091C4D605235AF18A885C4EE016F1874F600E514F67DC2AE71B841023B41B0D3D96BCE32C4BF742DCC89FCC5D5532F2B584FFD91965E95BF4975F867239A4(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p...dd.T...._keyhttps://www.findemr.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js .https://findemr.com/..|..(/.....H..|B4.....1.I.`. };.m!d.7..}(.A..Eo.....E.....A..Eo.....|..(/.....'.....O....x....(.....h.....(S.0..`.....L`.....(S...`.....HL` .....Rc@.....Qb"Q.]....e.....Qb.>.....t .....Qb6..@....r.....Qb~.(.....n.....Qb6?.....c.....Qb.Q.\....o.....M....S...QbJ1.....l.....R....Qb.Q\]....f.....Qb.....d...k.....I`....Da.....(S.....Ia#..... ..@.-....dP.....V...https://www.findemr.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js..a.....D`....D`P...D`.....4...`....&...&....&....&.(S.t..`.....0L`.. ....Qdn.6.....<a href=".....Qcff.G....replace...2L...Qc.:u<...."....Qc..U.....">....Qd.-.P....innerHTML.....Qd.....childNodes....Qd"..a....getAttribute..rT.I..K`....Dw0....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ff33f85f891a5dd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.868682261930593
Encrypted:	false
SSDEEP:	6:m09Yk+f2pomWKNYguxzhmJ2iAunjhB1EUTWjhO7DK6t:zl++am7NYTkJXBCU4kp
MD5:	C3714FC60BD5E2F97CF469B861E38AE9
SHA1:	FC93F685C695A4AD80CE95687D21D33C0A0FCEAD
SHA-256:	00560B019F07B860DF3257F6CCBBB7D10A7B7532E35B5F16B1CBFC7AEDAB2049
SHA-512:	92EB95D8A82339653222E88689C70553AFC008DF95F7D018F5014B57CECB32C91FAE83ECFEEBA9CC21BF8CFEE2415F54A6A1693A442ACEE5F8176F0835407C5D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...4..^...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ipSB4/yP/l/de_DE/wI1GDHO4qg9.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.....(/.....{.....}.|.gB.4.'.~C .q..i.....^..Z.O.A..Eo.....!JR.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\541c8064642a335a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14187
Entropy (8bit):	5.508434809681141
Encrypted:	false
SSDEEP:	192:SEqzuDN4XSGEI5KdmYbxm79rdgvgdoPIEZKcwJE/WFV2LC+MS1WOAU:Sy6uZapgodvE/WX+MS1WOAU
MD5:	41681E7DE6BE5E8CE24BFA430F955B67
SHA1:	84D5E9FCF9C0491E8DD4DB33B45E5C217AAC5039
SHA-256:	98C65FD4F10DEE94D415FEA07E3C0509955ABA30163565054A81ADCEDE7E78EE
SHA-512:	E1DD6BAE2E16EF50E2584CF627A4440727A886993EEE6F17CF9DDB99E7702C53A0B89BF1A363F628CACE4C5AFC198930EDE39CEA6D8AE5485AF3958DF5A47463
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...cv$....._keyhttps://www.findemr.com/resources/wp-includes/js/jquery/ui/core.min.js?ver=1.12.1 .https://findemr.com/=....(/.....J...4@..n.7.w;i.1....> +.!f.;...A..Eo.....w.....A..Eo.....'.3Q....O.....5..N.....(S.8..`(.....L`.....(S.T.`^.....L`.....Q.@.....define....Qb.wHv....amd.....`.... ..M`.....QcNYu]....jquery....Q.@.v.X....jQuery....K`....Do.....s.....&.(.....&.z..%&.^.....&.].....(Rc.....I`....Da@.....d.....P.....@.-....`P.q.....Q...https ://www.findemr.com/resources/wp-includes/js/jquery/ui/core.min.js?ver=1.12.1...a.....D`....D`....D`.....`....&...&....&.(S....`.....L`b.....RcX.....$.....Qbb..(....x.....Qb.> .....t.....Qb"Q.]....e.....Qb~.(.....n.....Qb..~?....W.....QbJ.g&....C.....Qb.Q.\....o.....Qb>v.....s.....Qb6..@....r.....QbJ1.....l.....M....S...QbN..y....h.....Qb...9....E.....Qb.0S.....H..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\54d8f6d393f18101_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.716525205861818
Encrypted:	false
SSDEEP:	6:mZEYk+f2pomJE6h0hmJ2z6X/4LZeYnCXhK6t:P++amJE6mkJrSZeYCX7
MD5:	E60B7A522AD71342B3B9B1EE73DDC9FB
SHA1:	8AC274A0719638F4B18F841FD4907631EA02002B
SHA-256:	99DDE1FCCCB3385FD4A976EA4D421327F81DAC48BC2DF13D99A0997EA0639955
SHA-512:	3CFF34F72D4C42B489207CCC9D28E9003E5ED8160468DD066E073484B7CAC900929058D66433954C644715216580B3441C3C36BE42DDABCCB0EB5A2AFA8E361
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\54d8f6d393f18101_0	
Preview:	0\r..m.....h.....U ...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y9/r/zembomw19DT.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.'...(/.....#$!P....6B.!.X7.....).[d..x8.A..Eo.....u.e.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\552e1aae4bcf9ae5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	337
Entropy (8bit):	5.936623244596967
Encrypted:	false
SSDEEP:	6:mf2iEYGLg68mGHqUcSnZAmwD4raFxO0f4zhK6twP2YQ9nBhfZmv1xO0f4Kp:kA5GHpcsYD3FxLu7qP2YqXfIv1xL
MD5:	3B51D7B52F978D15684E41B3BB6B7066
SHA1:	76FFDE3F186C8D8E4792E3AF0E4FCA2E711E8C4B
SHA-256:	F1829FE0B4784C19486177D0B53B4BEA0DF32AAD24E8DCB2CDACBECEFDA24FF8
SHA-512:	2571556BEB177599160DDC84A5A34A76E57A4FFCB3D5013303D7F20166FC8703F29F5C2630946F92C8D6A3B24567B80894D23596E46E6918940C90B6776762E1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I.....M...._keyhttps://www.clarity.ms/wus2/s/0.6.22/clarity.js .https://findemr.com/...(/.....J.J.....E.h.....U..k...A..Eo.....A..Eo.....(/..&..4905CE6D50F851CEEBFA5582AFE7D2587B1A588C6A9D68416AE9307C2465919B.....J.J.....E.h.....U..k...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\571707e954e02bb3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4949
Entropy (8bit):	5.7166307738057975
Encrypted:	false
SSDEEP:	48:eE8MykhrJsYIa6NhCuy6nBQtUHh/cEJv6v6cKAYvEcdaucgMrse9g/OVZP1rweGi:zhrJsYInmuy6nNGI6DCj3ei6ZNr9Gi
MD5:	76C3AB462C20FEAEB3BB4F418C12A665
SHA1:	88E37048989802B23C75431558638450BB71C815
SHA-256:	99D915E68A4C84AEDE1C13F88FE208DB0D225519843FF79F71334E6F5801213F
SHA-512:	C4B54D6DE50287F19C120CB2E3911C1385F88F3E4DE2D5604153A4292154A1A88609AF60575BC36DD8072EDF9CCB7F19774E0850F030FF91B9E31632B796A3B5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...j.i...._keyhttps://www.findemr.com/catalog/view/javascript/lg-thumbnail.min.js .https://findemr.com/.....(/.....?8..7E....T.v....k..HO...+..:c.A..Eo.....8.3z.....A..Eo.....'.L$....O.....(S.8..`(.....L`.....(S..`.....(L`.....Q.@b8.....exports...Q.@...V....module....Q.@2|.....define....Qb6.Yd....amd...Qc.....window.....Qb..A.....self..Q.PF.u>....LgThumbnail...K`....D.....s.....s.....&.\..-....S...s.....&.(.....&.|.&.^.....1...s.....s.....s.....s.....%.&.\..-..!.....,Rd.....I`....DaL...n....$..g#.....`...p...0.....@.-....PP.1.....C...https://www.findemr.com/catalog/view/javascript/lg-thumbnail.min.js.a.....D`....D`(...D`.....`N...&...&....&.(S.I.`..... L`.....0Rc.....Qb.'4o....t..`....I`....Da.....H...(S.x.`.....L`.....TRc&.....Qb.4.u....o.....S...Qb.u1.....e.....R....Qb^.....r

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\571bdeb7bbe1a277_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.776661792484434
Encrypted:	false
SSDEEP:	6:m1l9Yk+f2pomWgFVLShmJ2A9AdaxJTgJ4XlZK6t:4ll++am9V+kJg4JUU1
MD5:	86E6FF5ACCFAA74665A329F8A2387C95
SHA1:	7474C372010EA770DDBB252CDEF0D724F015AF4B
SHA-256:	5E9AC591D2F3257307A3D3B953547DFA94FBC61E827AFADBAEE634F7777051FB
SHA-512:	1CCFF2547E825453C33036A9E11D52B9B60CA3A00FFED0155C3AE9B5219677150F94DE6AB8CAFE3080DC76E892E41899B1C2253591AE7E8D666C630BBACE63AE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....0...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i2UN4/yB/l/de_DE/0g-h6QmT-I2.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.....(/.....8.....X.{.g.LFf?g.6..|.....w%.|>.....A..Eo.....K.|g.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5a716fde02d6ccab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	77456
Entropy (8bit):	5.992515534957305

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5a716fde02d6ccab_0	
Encrypted:	false
SSDEEP:	1536:EkIAW4kLxGzXJ6wP+R53422qGkfCgfDNOakyKLp6+Y4C6LMSIITb8CT30:CAILXL3pkkfCgfDNOakyIp6f4C6cl
MD5:	C525022DE4F2275D00A5E385E74DE668
SHA1:	68BAEB92B3FD7523A67354F248F3F784BB792FF6
SHA-256:	23C6F4B1EFDAE6A32C8C5411AF87AC260CE300B1CB31BFD46963A2717D119BD0
SHA-512:	D915F72D90BD21E1D39479960A1894BC755566398D8C72E2B48325AAE7DF95F2168B10ABA2A44553453880822D7A857E734FF41B67286B607575077101B0047F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....y....4A26D8885DF5A12242A3A2D9F3A01B900209D80CE8E3C793501538BB7AC26B00.....'.....O....P-..^. l.....p...t..... ...@...H.....(...l.....|.....(S.0..`.....L`.....(S.A..`:.....L`b....A.Rc.....F.....Qb..)....e.....Qb"......n.....M...Qb.....r.....S...Qb...s....o.....R....Qb..xI....s.....Qb ..#.....l.....Qb.....c.....Qb.r}.....d.....Qb..4.....h.....Qb..2>....p.....Qbz].....v.....Qb^[.....m.....Qbz..`....y.....QbV.i.....w.....Qb*..A....k.....Qb.6.....E.....QbN.*(....S.....Qb.2....._..... Qb.M.....N.....Qb.g.....x.....Qb.g.....I.....QbF.....D.....Qbr..q....C.....Qb..kj....R.....Qb.....z.....Qb*.....L.....Qb.$.x....j.....Qb.N.....A.....Qb.L$.....Y.....Qbn2C.....X.....Qb.<4..... q.....Qb.....W.....Qb".....U.....Qb.e.....P.....QbV=.....F.....Qb..d.....V.....Qb^.Y....J.....Qb.u. ....K.....Qbz.....Z.....Qbz.....Q.....R...Qb2.w.....et....Qb~"...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\64973bc3db40fd49_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	56930
Entropy (8bit):	5.573611035222091
Encrypted:	false
SSDEEP:	768:8kPqdu1jPLZGQy4og/QHB4l9HWoj3O6wncdmKNHmrWgYUzN:8GqdAjlTy4og/QHBuWG3O6/0aHmK3UzN
MD5:	D9C0B3EE81CE6F14886CBC1C9A0A27A7
SHA1:	F69A2E333C83B99A00E901E952286BD028BC74B2
SHA-256:	3C4E08B158E9A6551837AB1B0E62D5F1F442FF48D35B3CB128F0E13691A2968D
SHA-512:	9845FC517D060082E6F260267FE1A0D91B7154C39027DAE4AF0E95C232988C338C39B75AD7B7E44C30F06F2F7FDFDBBBE3F019D670E97C796063552DC35CE1A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x.j....._keyhttps://www.findemr.com/resources/wp-content/plugins/jupiterx-core/includes/extensions/raven/assets/js/frontend.min.js?ver=5.7.2 .https://find emr.com/....(/.....t..*.L.e....0....`9..M..wS..A..Eo.....s.....A..Eo.....'.....O....h...IL|.....X..... (S.....`.....L`j....(S.x.`.....L`.....PRc$.....QbJ1.....l.....Qb6..@....r.....Qb.Q.\....o.....R....Qb6?.....c...d$.....$.....M.`....Da....X....(S....`.....4L`.....4Rc..... .Qb.>.....t...`$....`....Da:.....Q...Q.@f..,....require..... Qf*.....Cannot find module '..Qb..l....'.....Qe".....MODULE_NOT_FOUND.9.....a.....Q.@.....exports....a..... .Qb.C.....call..Q..(S.L.`T...]..K`....Dm.....&.....&...*..&...*..&.%.*....%.&.]....,Rc.....l`....Da(...`.....q.....c..... .....@.-.....P.!.....https:

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\684984884ad03667_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	196
Entropy (8bit):	5.432547329114921
Encrypted:	false
SSDEEP:	3:m+lpxUla8RzYrWPJupp4DFKVRlMRBr4l9tlHCdal/6zf3/qJfCgK5m2vpK5kt:mOxUVYpS0VLMj2d5znqJagK42RK6t
MD5:	70839A07C74A040381CB9431300E460E
SHA1:	0202A6B8EC46A900604FB7159CA41804F5C5D495
SHA-256:	59E8EC44EBE528B5F113929C4B87F565F1ECA00634F10868ED8D6CB5555026B5
SHA-512:	E251B92EC138A71B3D758A3054EC292E2DE684ABF9DF515557EFF6F6F3DAB65181109CE962D02C0764799E6EEFF74B5F36C1E2253732CBD312FDCD83C482E11
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....T....._keyhttps://apis.google.com/js/platform.js .https://twitter.com/{....(/.....v..z...)..r.,.U..M..H.n#m+...'..A..Eo.....(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68a7a6f56553da52_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.687902567005494
Encrypted:	false
SSDEEP:	6:mePYk+f2pomKo2hmJ2QaItHQKrLzM//EzbK6t:X++amKo2kJvtz3MXEp
MD5:	EA23E85B00C3FD59DA2A28601CD889F4
SHA1:	04C8EE7CB539E859255F601119F7F5710DB8EB83
SHA-256:	63D47D3CAB5D089C838A8BAD506D6127AD854A628EE9A7DB3AEDFD4365E2667E
SHA-512:	B0CC9F6236150D1757B405B75C61E51EC088A250F555C236889DA13894EA5463D6C7D0EB894093313FE766DE4C29624D5E0C79B3954CE3188E39F703FCCC2F1A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68a7a6f56553da52_0	
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yy/r/lGAfVW6pT4t.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.....(/.....yT.5b.dU.?@....v..g....Z .|tq...A..Eo.....R.^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6d9ba87a21b4038f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	902
Entropy (8bit):	5.467868839804748
Encrypted:	false
SSDEEP:	24:c8YlcvilKOtKSlIkBcPgaH4M0Hv6eAqEvg1:uIisY/6O753gg
MD5:	032A044FC43042E86A29F6B841B403D0
SHA1:	62E89FAFA067430206C4C362CA89D310FCCC3D6E
SHA-256:	059B6112BE68251C2112BBDE95D9974CBF62316DEF3975A643FA63C3AC945FF6
SHA-512:	07FC4628A71427B303B1AA533B41B83ABFE65B3AD7D50C81586314B10CEC26D622D9067B5208FE8209A9FC474D42C68515F79C9554CDF473DC522C3A20302834
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^...<.%....._keyhttps://www.findemr.com/catalog/view/javascript/search_suggestion.js .https://findemr.com/.u6..(/.....V.....,D.?k..-6.A.C...f.u.{.4.#L.C.-..A ..Eo.....A..Eo.....u6..(/.`.....'.....O.... ....k@.....(S.H..`H.....L`.....Qc6.....document..Qcr.....ready....(S....Ia.....@..I+.....\... .....d.....d.....$.g.....IE.@.-....PP.1.....D...https://www.findemr.com/catalog/view/javascript/search_suggesti on.jsa.....D`....D`....D`.....<...`....&...&.....D`....DIJd.....K`....Dl .....&....&.]...&.(...&.....&.Y....&.....$Rc.....`.....Ib.....c.....@.....d..... .....,D.?k..-6.A.C...f.u.{.4.#L.C.-..A..Eo.....l.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6e1ed7af945ee8b4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	70160
Entropy (8bit):	5.694165106531578
Encrypted:	false
SSDEEP:	1536:Li3GSZuXdx1p9BFut7Dx+iyl8UQ+KlLfTw:8A1pFgDx+i0hjlL8
MD5:	069E344EF159AADF5BF350EC6BF94A2F
SHA1:	78240359AC6F0DDDF16B423AF5493DC21BF18CA0
SHA-256:	5D0D56D6E973B34935E6C978650ED8DBB83CE33D64D56ADB1ACDBDC737F58DB2
SHA-512:	9E16EF2D9FEEF4B5FD442AD04BDD29ADFFFCF26342748C6F243E9FD3424AA8405C35D6A7FD5E368AFD181EDD15D25703ED2AAB0A48A839670005B41F3E3934 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...&..I....3AD5057BC30B189C0376D333E4EBA7563755466F87BBF714FBA8CFBC91C08010.....'.....O.....iOvq..... .....8.....(S.....`.....L`x....XL`(.....QcR*.{....jupiterx..Qb...M....Util.(S.....Iaa,...-...$..g.....'@.....Qe...b...._objectSpread...E.@.-....xP.. .....j...https://www.findemr.com/resources/wp-content/themes/jupiterx/lib/assets/dist/js/frontend.min.js?ver=1.23.0..a.....D`....D`v...D`.....9....`....&...&...(S.h.`.....0L`..... <Rc.....Qb6..@....r.....Qb>v.....s...b.....I`....Da<... .....Qb..k....xyz...Qb.\|.c....test.(S.....Ia?...F...I.....d.....Qd~K.....\b_super\b....Qb..m.....*...(S.$..`.. ..]..K`....Dc.....,Rc.....I`.....Q.@.....Class...a.....d.....q..(S..`.....(L`.....@Rc.....Qb"Q.]....e.....Qb.Q.\....o...bd.....I`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73c2126721515754_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10538
Entropy (8bit):	5.425717887372443
Encrypted:	false
SSDEEP:	192:/TdHstGkr+dweFvlaH3xgYF4GBOnqDczB/O3tqHBNPkp:rdUSlaCtAOnoeB/O3tCI
MD5:	7BC6DB5A3B7C64CF7D3306390C31239D
SHA1:	4E17E3749CBDF9D54F416F9F36EF5350D388601C
SHA-256:	A1C54DE498FDE462D626AE44DA9593B73453594B5072555559CE04AE2F62334F
SHA-512:	BDACE721E12B19D388D8DA0A8D742711B163EC2245AEB7359DC18A19D6FD9267EB788E6ECEB2F0655C5240053CB58A96F10224793AD942CC84FE945682AB171 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}....._keyhttps://www.findemr.com/resources/wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js?ver=4.8.1 .https://findemr.com/7....(/..... ..4..0..J....G..F...Vc.+.....A..Eo.....W.....A..Eo.....'.o*....O....x'...WH.....T.....(.....(S.I..`.....$L`.....(S....`H.....L`.....8Rc..... ..M...Qb6?.....c...a$.....I`....Da&....S...,..a.....Qd..%....widgetsTypes...a.....Qe.....createWidgetTypeC..Qe.....addWidgetType...C..Qe.....getWidgetType...C. (S...`.....0L`.....@Rc.....Qb"Q.]....e.....Qb.Q\]....f...bd.....1.`.....5.a.....a.....a....\.....Qcf*.D....Widget...(S.8.`*.....L`.....K`....Dh.....&...&.(...&.Z. .....0Rd.....`.....a....4.....a.....b.....@.-....tP.....h...https://www.findemr.com/resources/wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js?ver=4.8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73e8cdbe92231fbe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.652264238015241
Encrypted:	false
SSDEEP:	6:mSEYk+f2pomD9Utru5hmJ2mw+AXJRsXj2YthK6t:FU++amCc5kJvtlXj2i
MD5:	25C408693E6B234464E9813A43F90DF2
SHA1:	AEB2282FBBFDDBB8A559771EE48D73A3F9EC757C
SHA-256:	B9D2162BAD70286578F4251E27C54C4077EE506380F41DBC9C7AA6FE17A57616
SHA-512:	5E95B9D23162444501015DFC980CA8C02D4906A528022EAF2B5E487EF493AB571EA50FD22F223B4CE18B098AD3BE0A4F066C7825B384A5BC2D847BBAFCFA0DA E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....Ub...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yh/r/l14koXizyE3.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...../(/.....VwtBk.../..r.qI...l..UC. ..n...A..Eo.....-.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76e1b6c82fa65f57_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	107232
Entropy (8bit):	5.924630716055161
Encrypted:	false
SSDEEP:	1536:hIxVvbnYtNSEMNQqFL9Utzb7WebM0gRcteHkS5cHNujkSPK:hIx5DYt4fNx6tzb77eYeZcHNmlPK
MD5:	7D870B9DD21969EEE62834C87D457D32
SHA1:	D963CE628A6E790015D5D39BC070BF607FEB0B0F
SHA-256:	EE73FF2EDF76CD5BF65657D94974E3B468F092CB3B8027ACA81E1C4822837B95
SHA-512:	06C15133F4D00C39DCE2281E5786CF5347F5AFEFC03AFE0E955F8C7ED9398792FD571796F43E363376584AEC965935C792448CAE7486AEC30A8DDC2D0662049I
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...O.....57CE015EA45427248BBCD0541D594829BB35F916ADE34322FEE2F78040DDC452.....'..d....O$.....%o%a.....@ ....p.....p.....\|.....0.....(S.0..`.....L`.....(S...A .`:@.....L`h.....e.Rc.....Qb6.....data..Qb.5\&....da....Qb.....fa....Qb>.<.....la ....Qb...c....oa....Qb..L.....qa....Qb..>{....ra....Qb~.....sa....Qb.w.....ta.....Qb.xC4....ua....Qb.T.....wa.....Qbn.+.....xa....Qb.....ya....Qb.X.*....za....Qb..Q^....Aa....Qb. F.....Ba....Qb./7.....Fa....Qb.....Ia....Qb.K.....La....Qbjp#.....Ma....Qbz.....Na....Qb.....Oa....Qb^.....Qa....Qb.-.....Ra....QbB9.....Sa....Qb.-^q....Ea....Qb.y.....Ta....Qbr*". ....Ua....Qb...U....Va....Qb&.TK....Wa....Qb..d.....Xa....Qbr.Y.....Ya....Qbf.`.....$a....QbBQ.....bb....Qb..g.....cb....Qb.....eb....Qb'".....db....Qb.....fb....QbF.S.....jb....Qb.. .B....mb....Qb.....n

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7bbf9dd8a4c8a7fa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.583193230740875
Encrypted:	false
SSDEEP:	6:mqcYj018IrAWDAQCvpMVKyD13ycMl+4uK6t:c1tBXXM+T
MD5:	044FD18C095CDB00BBDC3035F3078E24
SHA1:	B9BA712D92A368F30976D9B52820C45524C441E9
SHA-256:	5FB18D3D65D0817CBA9C65E73A042A226401641F6AD6C2303333F7FE6E06ACC9
SHA-512:	B81BF087E98D10FB88CE7D57381A53B3B15F99EF30B219140D43E3E852D820B02611A8AEC8B33A4C947FD5A521DD2706AA77335CA8D169340CAAAC21AD72813
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i...G....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.SignupModule.4ff55fb5.js .https://twitter.com/.n...(/.....&.....,....s\.>..RQ&j.z" 4Y.C..w.A..Eo.....1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7cd448c14e7bf356_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2568
Entropy (8bit):	5.756554843729337
Encrypted:	false
SSDEEP:	48:OL4/8TILczILDILuuILMILuILZILNILxOILCILcfkvL5p:OL6LcML8LKLpLLLaLmLxrLXLAyL
MD5:	AB171450440C3C3D80CCB8129BEF6774

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7cd448c14e7bf356_0	
SHA1:	EEC5C22F6D6EFE976F4F557D074190A66B3E299C
SHA-256:	161A415D2E50E92519CEDBF99050E3D4777177F1DC6E5BC9DC01CE1C893882DE
SHA-512:	4DFB089640225FCEB4161EEF234DEAC51922F1E4F01FE94641B6655C8C2C280AFA1F49F591ED8E51EEAE2E902D94814776CD4A9C6BEFDE38EA41F37DFA7FC7 59
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G....._keyhttps://www.google-analytics.com/analytics.js .https://findemr.com/(%...(/.....g.....}....?u....g..S.7..9-..Od.....A..Eo.....R.....A..Eo..... .0\r..m.....G....._keyhttps://www.google-analytics.com/analytics.js .https://findemr.com/....(/.....-.....}....?u....g..S.7..9-..Od.....A..Eo.....]....A..Eo..... .0\r..m.....G....._keyhttps://www.google-analytics.com/analytics.js .https://findemr.com/n...(/.....*.....}....?u....g..S.7..9-..Od.....A..Eo.....A..Eo..... .0\r..m.....G....._keyhttps://www.google-analytics.com/analytics.js .https://findemr.com/,....(/.....}....?u....g..S.7..9-..Od.....A..Eo.....A..b.....A..Eo..... .0\r..m.....G....._keyhttps://www.google-analytics.com/analytics.js .https://findemr.com/..?..(/.....A".....}....?u....g..S.7..9-..Od.....A..Eo.....Y.....A..Eo...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d50675751195852_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.5843623433451945
Encrypted:	false
SSDEEP:	3:m+l2S8RzYj0KKKXlMMIrARc/NdJQIDlMRatlHCAnd42C+xVODFP2kRm2pzlllpK+:m9Yj018IrA6/PJQIpM/s9yDQhAnK6t
MD5:	C17F3E0BD4CFA546BA65A42A8AD21B25
SHA1:	F700F697BE0FFB1056FFE0923922B12285D712EA
SHA-256:	04F5216F7AF1126025CB40BDD3E20C299715494B65AE1DC06C84316A6475144D
SHA-512:	D1AC017A99A8DF3444640FA6C73048F6347A4033D9768A246D51914C6CD1E86607BB84FF155A4172BEEAFF07BDD9E714789EF0161B8FF493EEB18FE36E1D34D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...@8uQ...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.Typeahead.8be5b3e5.js .https://twitter.com/?a...(/.....%.....8.....[.9Q..j..f.....PK.. ..n.A..Eo.....U.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7e96d7fa999285b4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	300
Entropy (8bit):	5.596890253328018
Encrypted:	false
SSDEEP:	6:mekM9YZHf/Vpe5r1BpKuEPAMWcrQofLoRCu4l6kR3ExoR/EkhK6t:b3c/C5r1BojhBroxwxo97
MD5:	F585D28720ED2AACE0257A63EE050146
SHA1:	94557E42DDDC0717029FC77367E010B7F6856885
SHA-256:	6D773081E144E38DBCE6811FDA7F1E439E8F346780EBB9F63625171327C5C185
SHA-512:	027364B97734C71E981D6B74F5A1C0C34C56F103FF0658C1BF6E7B2646424DD15EA442E37A846841C50D7CDADCDCECD98C08ABF22DB16FF1E37BB8C09D8D9 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z.a...._keyhttps://maps.googleapis.com/maps/api/js?client=google-maps-embed&paint_origin=&libraries=geometry,search&v=3.exp&language=en&callbac k=onApiLoad .https://google.com/O...(/.....b.`S.....6..;8....(.qA..4.A..Eo.....M.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7f58c6b64ba329a0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10165
Entropy (8bit):	5.51795619464168
Encrypted:	false
SSDEEP:	192:SCmAGhH8AC9FNziqFT67Xyt6hns9f9D/E5LOyZxoaR6NL:vm7J899FNiB7XytKs/E51ZqEoL
MD5:	D4B0E21C72F39779C24981C53A1BC4F3
SHA1:	6A16A264131FF538313AC72A032FAF7FC5935483
SHA-256:	B4A995DC8C2F020D1341388101643E58FD4764E9E9C9B82629F81BC802114DA7
SHA-512:	ADFDEE736BBE773BB80780B847553EBF3068531DECBA944427CBCC22955C7E5023D5928D7B113D2863B16993A0CC4262394FCE0536F5F4E165AB4F924A3D48E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7f58c6b64ba329a0_0	
Preview:	0\r..m.....'....._keyhttps://www.findemr.com/resources/wp-content/themes/jupiterx/lib/admin/assets/lib/webfont/webfont.min.js?ver=1.6.26 .https://findemr.com/i.{..(/..... ....s.....>PB.r.....$m...9.:..o.9..A..Eo.....h..N.....A..Eo.....'./0....O.....&..;.....(S.0..`.....L`.....(S....`.....L`.....A.Rc.....Qb..| _....aa....Qb.2.....ba....Qb..'....p.....Qbvu%.....q.....Qbr.....ca....QbN5.z....da....Qb.>.....t.....R....Qb.....v.....QbF?.....w.....Qb.R.]....y.....QbF..x....z.....Qb...1....ea....Qb.R.]... .A.....Qb.ZNa....B.....QbJ.g&....C.....QbF.....D.....Qbf-.J....F.....Qb...9....E.....Qb.=.....G.....Qb.0S.....H.....QbR.....fa....Qb.....J.....Qb.TT^....K.....QbF.d.....I.....Qb&..w.. ..ga....Qb.....ha....Qb.!/.....ia....Qb.|.....M.....Qb6..+....L.....Qb.....ja....Qb&.....ka....Qb..@.....N.....Qb..j?....O.....Qbn.....P.....Qb.2.....Q.....QbJ.....R.....Qb>Y.a....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\845191cd846726ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.553722054284304
Encrypted:	false
SSDEEP:	6:mARyEYj018IrAE7uP39ELMXrLcXCRSE3+9kH4nf/ZK6t:J1tnuP39J0XCRVHAj
MD5:	10A8EF9ADD47D1CFB9C46223E406C15D
SHA1:	8F719B4CABEF2EB7B2FABECA7F8A9817DFE50ECD
SHA-256:	C4A566542811569C93839E4185D91163E4B3C65BED24AFFE3D4D007F3D7C836A
SHA-512:	214AEC63CAC203885B13E14A8871FC1B96AA8CF065060807C415705F21FCE95F032481F6687BF19A0E1DE9C97EB706853E78B2680F598A9A4BDC54FD8DAFADC B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...M.2....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.AbsolutePower.e700c795.js .https://twitter.com/*O...(/.....V7...0G.w...O..#..SL ....._.G.A..Eo.....4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\849c3de6865d8565_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.413841092288075
Encrypted:	false
SSDEEP:	3:m+lrlaK8RzYiMRLyM6IpMRv91/tlHCJll/5Xrvj8IcNup5+/z4mGtpK5kt:mEanYiMs8pMZqJ/1j8IcNupgLrQK6t
MD5:	E28003F0B7FBE7467D2E32E646181FFC
SHA1:	F97332C01AC20A77FDFDA1F856ABF5856A55A8C5
SHA-256:	EADD32B601D5DD57CBAAA7E378B58619F4ECB51AF418015B297F90C74DAE00DE
SHA-512:	E918986DF76CBE04AFFAC4548C76D217A6BE05B99648300E8147EA9712746BAFED0C5EF6CC2C194E8A07FF72198ED18E9BDC0FACE2734B68859771C41A74C8 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....._keyhttps://twitter.com/i/js_inst?c_name=ui_metrics .https://twitter.com/8.z..(/.....n.....D...L...9..g.....-...m...oN.B.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\852958fa27c32c2a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.499473494835764
Encrypted:	false
SSDEEP:	6:mepYk+zuFrAmY609S31zikAdi5/lbK6t:H+sQf9UzPNhT
MD5:	D1E720D77DD66D580166E4B0D335EC2B
SHA1:	EDA2C6FFDDBAF1BE394E66A85302F910E847244B
SHA-256:	0D8912FA6B998CFF85BD669335E67C6A8A30ADBE6849E3D9A992A18DA7737012
SHA-512:	8BB8C815DA1CB5C357C7EF07D4E70D8DB486F0B845853E55B8660733614C875E393FD66C8FD0DD5916A75EF2C4F742F28C03C58D48BDA2F2D9DA2D2C1901BD 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....1q....._keyhttps://static.hotjar.com/c/hotjar-1184109.js?sv=6 .https://findemr.com/.Gu..(/.....q.....].ZZD.n....t.>...c...t...n,...=..A..Eo.....A..Eo..... .....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 20, 2021 18:02:17.803899050 CEST	192.168.2.5	8.8.8.8	0x8c6f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:17.807825089 CEST	192.168.2.5	8.8.8.8	0x8815	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:17.814852953 CEST	192.168.2.5	8.8.8.8	0x5d2	Standard query (0)	nxm7qtkm.r.us-east-1.awstrack.me	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:18.801739931 CEST	192.168.2.5	8.8.8.8	0x9336	Standard query (0)	www.findemr.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:19.959963083 CEST	192.168.2.5	8.8.8.8	0x18b	Standard query (0)	www.clarity.ms	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:20.923897982 CEST	192.168.2.5	8.8.8.8	0x521c	Standard query (0)	c.clarity.ms	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:21.576781988 CEST	192.168.2.5	8.8.8.8	0x55b	Standard query (0)	f.clarity.ms	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:22.722090960 CEST	192.168.2.5	8.8.8.8	0x97f8	Standard query (0)	www.findemr.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:22.923738003 CEST	192.168.2.5	8.8.8.8	0x89f6	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.346615076 CEST	192.168.2.5	8.8.8.8	0x4f40	Standard query (0)	img.youtube.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.244338036 CEST	192.168.2.5	8.8.8.8	0xd125	Standard query (0)	img.youtube.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:08.648283958 CEST	192.168.2.5	8.8.8.8	0x1ee7	Standard query (0)	apexsol.us	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.200171947 CEST	192.168.2.5	8.8.8.8	0xc8d4	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.401180983 CEST	192.168.2.5	8.8.8.8	0x3116	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.455245018 CEST	192.168.2.5	8.8.8.8	0x7445	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.455322027 CEST	192.168.2.5	8.8.8.8	0x2033	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.609579086 CEST	192.168.2.5	8.8.8.8	0xb620	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.668631077 CEST	192.168.2.5	8.8.8.8	0x9bcd	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.670916080 CEST	192.168.2.5	8.8.8.8	0x1ee7	Standard query (0)	apexsol.us	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.935923100 CEST	192.168.2.5	8.8.8.8	0xec36	Standard query (0)	in.hotjar.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.938813925 CEST	192.168.2.5	8.8.8.8	0xdcd	Standard query (0)	vc.hotjar.io	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:14.155189037 CEST	192.168.2.5	8.8.8.8	0xed34	Standard query (0)	apexsol.us	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:16.542185068 CEST	192.168.2.5	8.8.8.8	0x1891	Standard query (0)	web.facebook.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:16.743838072 CEST	192.168.2.5	8.8.8.8	0x7dcf	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:17.212112904 CEST	192.168.2.5	8.8.8.8	0x391e	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 20, 2021 18:03:17.472800016 CEST	192.168.2.5	8.8.8.8	0xb5a3	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:19.725666046 CEST	192.168.2.5	8.8.8.8	0xec11	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:19.750447035 CEST	192.168.2.5	8.8.8.8	0x7124	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:20.823411942 CEST	192.168.2.5	8.8.8.8	0x69b4	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:21.886590958 CEST	192.168.2.5	8.8.8.8	0x9275	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:23.256362915 CEST	192.168.2.5	8.8.8.8	0x7d3a	Standard query (0)	media-exp1.licdn.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:23.848121881 CEST	192.168.2.5	8.8.8.8	0x1373	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:24.174380064 CEST	192.168.2.5	8.8.8.8	0xc34f	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:24.185235023 CEST	192.168.2.5	8.8.8.8	0x633c	Standard query (0)	media-exp1.licdn.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:24.823015928 CEST	192.168.2.5	8.8.8.8	0x37bb	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.146104097 CEST	192.168.2.5	8.8.8.8	0x20f5	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.172480106 CEST	192.168.2.5	8.8.8.8	0x157f	Standard query (0)	api.twitter.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.172513962 CEST	192.168.2.5	8.8.8.8	0x602	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.206793070 CEST	192.168.2.5	8.8.8.8	0xacf	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.230084896 CEST	192.168.2.5	8.8.8.8	0xd446	Standard query (0)	video.twimg.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:27.670670986 CEST	192.168.2.5	8.8.8.8	0x164	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:28.339931011 CEST	192.168.2.5	8.8.8.8	0x268b	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:31.866581917 CEST	192.168.2.5	8.8.8.8	0xb1fc	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 20, 2021 18:02:17.841412067 CEST	8.8.8.8	192.168.2.5	0x8815	No error (0)	accounts.google.com		172.217.18.109	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:17.848141909 CEST	8.8.8.8	192.168.2.5	0x8c6f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:17.848141909 CEST	8.8.8.8	192.168.2.5	0x8c6f	No error (0)	clients.l.google.com		216.58.212.174	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:17.852679968 CEST	8.8.8.8	192.168.2.5	0x5d2	No error (0)	nxm7qtkm.r.us-east-1.awstrack.me	r.us-east-1.awstrack.me		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:17.852679968 CEST	8.8.8.8	192.168.2.5	0x5d2	No error (0)	r.us-east-1.awstrack.me	r.delegate.us-east-1.awstrack.me		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:17.852679968 CEST	8.8.8.8	192.168.2.5	0x5d2	No error (0)	r.delegate.us-east-1.awstrack.me	baconredirects-elb-1w79jy7i6g0wf-1154668140.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:17.852679968 CEST	8.8.8.8	192.168.2.5	0x5d2	No error (0)	baconredirects-elb-1w79jy7i6g0wf-1154668140.us-east-1.elb.amazonaws.com		3.229.3.83	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:17.852679968 CEST	8.8.8.8	192.168.2.5	0x5d2	No error (0)	baconredirects-elb-1w79jy7i6g0wf-1154668140.us-east-1.elb.amazonaws.com		34.194.248.184	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:17.852679968 CEST	8.8.8.8	192.168.2.5	0x5d2	No error (0)	baconredirects-elb-1w79jy7i6g0wf-1154668140.us-east-1.elb.amazonaws.com		18.206.70.26	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 20, 2021 18:02:18.846302032 CEST	8.8.8.8	192.168.2.5	0x9336	No error (0)	www.findemr.com		172.67.179.161	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:18.846302032 CEST	8.8.8.8	192.168.2.5	0x9336	No error (0)	www.findemr.com		104.21.18.20	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:19.696764946 CEST	8.8.8.8	192.168.2.5	0x6cd0	No error (0)	gstaticadssl.l.google.com		142.250.184.195	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:19.988485098 CEST	8.8.8.8	192.168.2.5	0x18b	No error (0)	www.clarity.ms	clarity.azurefd.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:19.988485098 CEST	8.8.8.8	192.168.2.5	0x18b	No error (0)	clarity.azurefd.net	global-geo-afdthirdparty-unicast.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:20.623202085 CEST	8.8.8.8	192.168.2.5	0x6172	No error (0)	www-googletagmanager.l.google.com		142.250.186.168	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:20.967394114 CEST	8.8.8.8	192.168.2.5	0x521c	No error (0)	c.clarity.ms	c.msn.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:20.967394114 CEST	8.8.8.8	192.168.2.5	0x521c	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:21.377654076 CEST	8.8.8.8	192.168.2.5	0xefbb	No error (0)	www-google-analytics.l.google.com		142.250.186.142	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:21.612646103 CEST	8.8.8.8	192.168.2.5	0x55b	No error (0)	f.clarity.ms	vmss-clarity-ingest-eus-b.eastus.cloudapp.azure.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:22.774671078 CEST	8.8.8.8	192.168.2.5	0x97f8	No error (0)	www.findemr.com		172.67.179.161	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:22.774671078 CEST	8.8.8.8	192.168.2.5	0x97f8	No error (0)	www.findemr.com		104.21.18.20	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:22.967350960 CEST	8.8.8.8	192.168.2.5	0x89f6	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:22.967350960 CEST	8.8.8.8	192.168.2.5	0x89f6	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.161	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	img.youtube.com	ytimg.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		216.58.212.174	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.74.206	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.186.46	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.186.78	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.186.142	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.186.174	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.184.206	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.184.238	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		172.217.18.110	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		172.217.23.110	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		216.58.212.142	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.185.78	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		172.217.16.142	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.185.110	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:32.390409946 CEST	8.8.8.8	192.168.2.5	0x4f40	No error (0)	ytimg.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	img.youtube.com	ytimg.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		216.58.212.174	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.74.206	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.186.46	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.186.78	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.186.142	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.186.174	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.184.206	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.184.238	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		172.217.18.110	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		172.217.23.110	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		216.58.212.142	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.185.78	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		172.217.16.142	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.185.110	A (IP address)	IN (0x0001)
Aug 20, 2021 18:02:39.285574913 CEST	8.8.8.8	192.168.2.5	0xd125	No error (0)	ytimg.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.256525993 CEST	8.8.8.8	192.168.2.5	0xc8d4	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:09.256525993 CEST	8.8.8.8	192.168.2.5	0xc8d4	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.256525993 CEST	8.8.8.8	192.168.2.5	0xc8d4	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.256525993 CEST	8.8.8.8	192.168.2.5	0xc8d4	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 20, 2021 18:03:09.256525993 CEST	8.8.8.8	192.168.2.5	0xc8d4	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.446118116 CEST	8.8.8.8	192.168.2.5	0x3116	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:09.446118116 CEST	8.8.8.8	192.168.2.5	0x3116	No error (0)	static-cdn.hotjar.com		52.84.174.89	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.446118116 CEST	8.8.8.8	192.168.2.5	0x3116	No error (0)	static-cdn.hotjar.com		52.84.174.60	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.446118116 CEST	8.8.8.8	192.168.2.5	0x3116	No error (0)	static-cdn.hotjar.com		52.84.174.94	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.446118116 CEST	8.8.8.8	192.168.2.5	0x3116	No error (0)	static-cdn.hotjar.com		52.84.174.115	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.483059883 CEST	8.8.8.8	192.168.2.5	0x7445	No error (0)	www.google.com		142.250.185.164	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.498511076 CEST	8.8.8.8	192.168.2.5	0x2033	No error (0)	www.google.co.uk		142.250.186.163	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.652650118 CEST	8.8.8.8	192.168.2.5	0xb620	No error (0)	script.hotjar.com		52.84.174.78	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.652650118 CEST	8.8.8.8	192.168.2.5	0xb620	No error (0)	script.hotjar.com		52.84.174.89	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.652650118 CEST	8.8.8.8	192.168.2.5	0xb620	No error (0)	script.hotjar.com		52.84.174.19	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.652650118 CEST	8.8.8.8	192.168.2.5	0xb620	No error (0)	script.hotjar.com		52.84.174.14	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.711893082 CEST	8.8.8.8	192.168.2.5	0x9bcd	No error (0)	vars.hotjar.com		52.84.174.120	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.711893082 CEST	8.8.8.8	192.168.2.5	0x9bcd	No error (0)	vars.hotjar.com		52.84.174.118	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.711893082 CEST	8.8.8.8	192.168.2.5	0x9bcd	No error (0)	vars.hotjar.com		52.84.174.22	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.711893082 CEST	8.8.8.8	192.168.2.5	0x9bcd	No error (0)	vars.hotjar.com		52.84.174.96	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.827794075 CEST	8.8.8.8	192.168.2.5	0x1ee7	No error (0)	apexsol.us		217.79.240.66	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.961174011 CEST	8.8.8.8	192.168.2.5	0xec36	No error (0)	in.hotjar.com	in-live.live.eks.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:09.961174011 CEST	8.8.8.8	192.168.2.5	0xec36	No error (0)	in-live.live.eks.hotjar.com		52.51.140.204	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.961174011 CEST	8.8.8.8	192.168.2.5	0xec36	No error (0)	in-live.live.eks.hotjar.com		63.34.251.77	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.961174011 CEST	8.8.8.8	192.168.2.5	0xec36	No error (0)	in-live.live.eks.hotjar.com		99.81.27.250	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.961174011 CEST	8.8.8.8	192.168.2.5	0xec36	No error (0)	in-live.live.eks.hotjar.com		34.247.193.249	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.961174011 CEST	8.8.8.8	192.168.2.5	0xec36	No error (0)	in-live.live.eks.hotjar.com		54.75.159.38	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.961174011 CEST	8.8.8.8	192.168.2.5	0xec36	No error (0)	in-live.live.eks.hotjar.com		52.49.237.17	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.961174011 CEST	8.8.8.8	192.168.2.5	0xec36	No error (0)	in-live.live.eks.hotjar.com		99.81.42.58	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.961174011 CEST	8.8.8.8	192.168.2.5	0xec36	No error (0)	in-live.live.eks.hotjar.com		52.210.84.221	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 20, 2021 18:03:09.974577904 CEST	8.8.8.8	192.168.2.5	0xdcd	No error (0)	vc.hotjar.io	vc-live-cf.hotjar.io		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:09.974577904 CEST	8.8.8.8	192.168.2.5	0xdcd	No error (0)	vc-live-cf.hotjar.io		52.84.174.67	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.974577904 CEST	8.8.8.8	192.168.2.5	0xdcd	No error (0)	vc-live-cf.hotjar.io		52.84.174.28	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.974577904 CEST	8.8.8.8	192.168.2.5	0xdcd	No error (0)	vc-live-cf.hotjar.io		52.84.174.9	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:09.974577904 CEST	8.8.8.8	192.168.2.5	0xdcd	No error (0)	vc-live-cf.hotjar.io		52.84.174.90	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:13.675215006 CEST	8.8.8.8	192.168.2.5	0x1ee7	Server failure (2)	apexsol.us	none	none	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:14.187735081 CEST	8.8.8.8	192.168.2.5	0xed34	No error (0)	apexsol.us		217.79.240.66	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:16.580737114 CEST	8.8.8.8	192.168.2.5	0x1891	No error (0)	web.facebook.com	star.facebook.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:16.580737114 CEST	8.8.8.8	192.168.2.5	0x1891	No error (0)	star.facebook.com	star.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:16.580737114 CEST	8.8.8.8	192.168.2.5	0x1891	No error (0)	star.c10r.facebook.com		31.13.92.10	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:16.786736012 CEST	8.8.8.8	192.168.2.5	0x7dcf	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:16.786736012 CEST	8.8.8.8	192.168.2.5	0x7dcf	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:17.246648073 CEST	8.8.8.8	192.168.2.5	0x391e	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:17.246648073 CEST	8.8.8.8	192.168.2.5	0x391e	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:17.505111933 CEST	8.8.8.8	192.168.2.5	0xb5a3	No error (0)	facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:19.758548021 CEST	8.8.8.8	192.168.2.5	0xec11	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:19.758548021 CEST	8.8.8.8	192.168.2.5	0xec11	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:19.788362980 CEST	8.8.8.8	192.168.2.5	0x7124	No error (0)	facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:20.848548889 CEST	8.8.8.8	192.168.2.5	0x69b4	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:21.927288055 CEST	8.8.8.8	192.168.2.5	0x9275	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:23.299217939 CEST	8.8.8.8	192.168.2.5	0x7d3a	No error (0)	media-exp1.licdn.com	2-01-2c3e-005c.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:23.881210089 CEST	8.8.8.8	192.168.2.5	0x1373	No error (0)	accounts.google.com		172.217.18.109	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:24.211632967 CEST	8.8.8.8	192.168.2.5	0xc34f	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:24.217775106 CEST	8.8.8.8	192.168.2.5	0x633c	No error (0)	media-exp1.licdn.com	2-01-2c3e-005c.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:24.848992109 CEST	8.8.8.8	192.168.2.5	0x37bb	No error (0)	twitter.com		104.244.42.1	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:24.848992109 CEST	8.8.8.8	192.168.2.5	0x37bb	No error (0)	twitter.com		104.244.42.193	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 20, 2021 18:03:25.180679083 CEST	8.8.8.8	192.168.2.5	0x20f5	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:25.180679083 CEST	8.8.8.8	192.168.2.5	0x20f5	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.200701952 CEST	8.8.8.8	192.168.2.5	0x157f	No error (0)	api.twitter.com	tpop-api.twitter.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:25.200701952 CEST	8.8.8.8	192.168.2.5	0x157f	No error (0)	tpop-api.twitter.com		104.244.42.130	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.200701952 CEST	8.8.8.8	192.168.2.5	0x157f	No error (0)	tpop-api.twitter.com		104.244.42.194	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.200701952 CEST	8.8.8.8	192.168.2.5	0x157f	No error (0)	tpop-api.twitter.com		104.244.42.2	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.200701952 CEST	8.8.8.8	192.168.2.5	0x157f	No error (0)	tpop-api.twitter.com		104.244.42.66	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.224221945 CEST	8.8.8.8	192.168.2.5	0x602	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:25.224221945 CEST	8.8.8.8	192.168.2.5	0x602	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:25.224221945 CEST	8.8.8.8	192.168.2.5	0x602	No error (0)	cs2-wac-eu.8315.ecdns.net	cs672.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:25.224221945 CEST	8.8.8.8	192.168.2.5	0x602	No error (0)	cs672.wac.edgecastcdn.net		192.229.233.50	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.231975079 CEST	8.8.8.8	192.168.2.5	0xacf	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.231975079 CEST	8.8.8.8	192.168.2.5	0xacf	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.231975079 CEST	8.8.8.8	192.168.2.5	0xacf	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.231975079 CEST	8.8.8.8	192.168.2.5	0xacf	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:25.263773918 CEST	8.8.8.8	192.168.2.5	0xd446	No error (0)	video.twimg.com	cs296.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:25.263773918 CEST	8.8.8.8	192.168.2.5	0xd446	No error (0)	cs296.wpc.edgecastcdn.net	cs2-wpc.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:25.263773918 CEST	8.8.8.8	192.168.2.5	0xd446	No error (0)	cs2-wpc-eu.8315.ecdns.net	cs531.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:25.263773918 CEST	8.8.8.8	192.168.2.5	0xd446	No error (0)	cs531.wpc.edgecastcdn.net		192.229.220.133	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:27.703581095 CEST	8.8.8.8	192.168.2.5	0x164	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:27.703581095 CEST	8.8.8.8	192.168.2.5	0x164	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:28.373970032 CEST	8.8.8.8	192.168.2.5	0x268b	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:28.373970032 CEST	8.8.8.8	192.168.2.5	0x268b	No error (0)	plus.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Aug 20, 2021 18:03:31.898996115 CEST	8.8.8.8	192.168.2.5	0xb1fc	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:31.898996115 CEST	8.8.8.8	192.168.2.5	0xb1fc	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 20, 2021 18:03:31.898996115 CEST	8.8.8.8	192.168.2.5	0xb1fc	No error (0)	cs2-wac-eu.8315.ecdns.net	cs672.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 20, 2021 18:03:31.898996115 CEST	8.8.8.8	192.168.2.5	0xb1fc	No error (0)	cs672.wac.edgecastcdn.net		192.229.233.50	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- apexsol.us

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 3108 Parent PID: 4756

General

Start time:	18:02:12
Start date:	20/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://nxm7qtkm.r.us-east-1.awstrack.me/L0/https:%2F%2Fwww.findemr.com%2Fresources%2Femr-software-pricing-covid-19%2F/2/0100017b644021e1-e46e8282-c9b4-471e-8ced-e85be6830ecf-000000/X8kT0A8I5y43QpMcpToFLRdF4Mk=232'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 4892 Parent PID: 3108

General

Start time:	18:02:14
Start date:	20/08/2021

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 --field-trial-handle=1608,9865191421646431568,12435009540188830314,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1672 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Disassembly