ID: 433377
Cookbook: browseurl.jbs
Time: 17:54:29
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

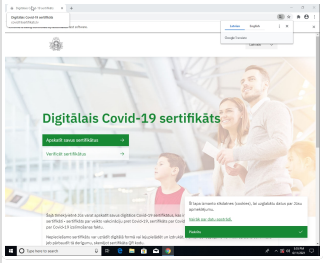
Analysis Report http://covid19sertifikats.lv

Overview

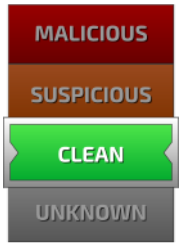
General Information

Sample URL:	http://covid19sertifikats.lv
Analysis ID:	433377
Infos:	

Most interesting Screenshot:



Detection

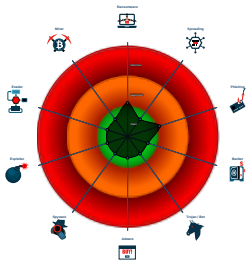


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6020 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://covid19sertifikats.lv' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5720 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1580,8389171160626933808,1445226050881952482,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1712 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

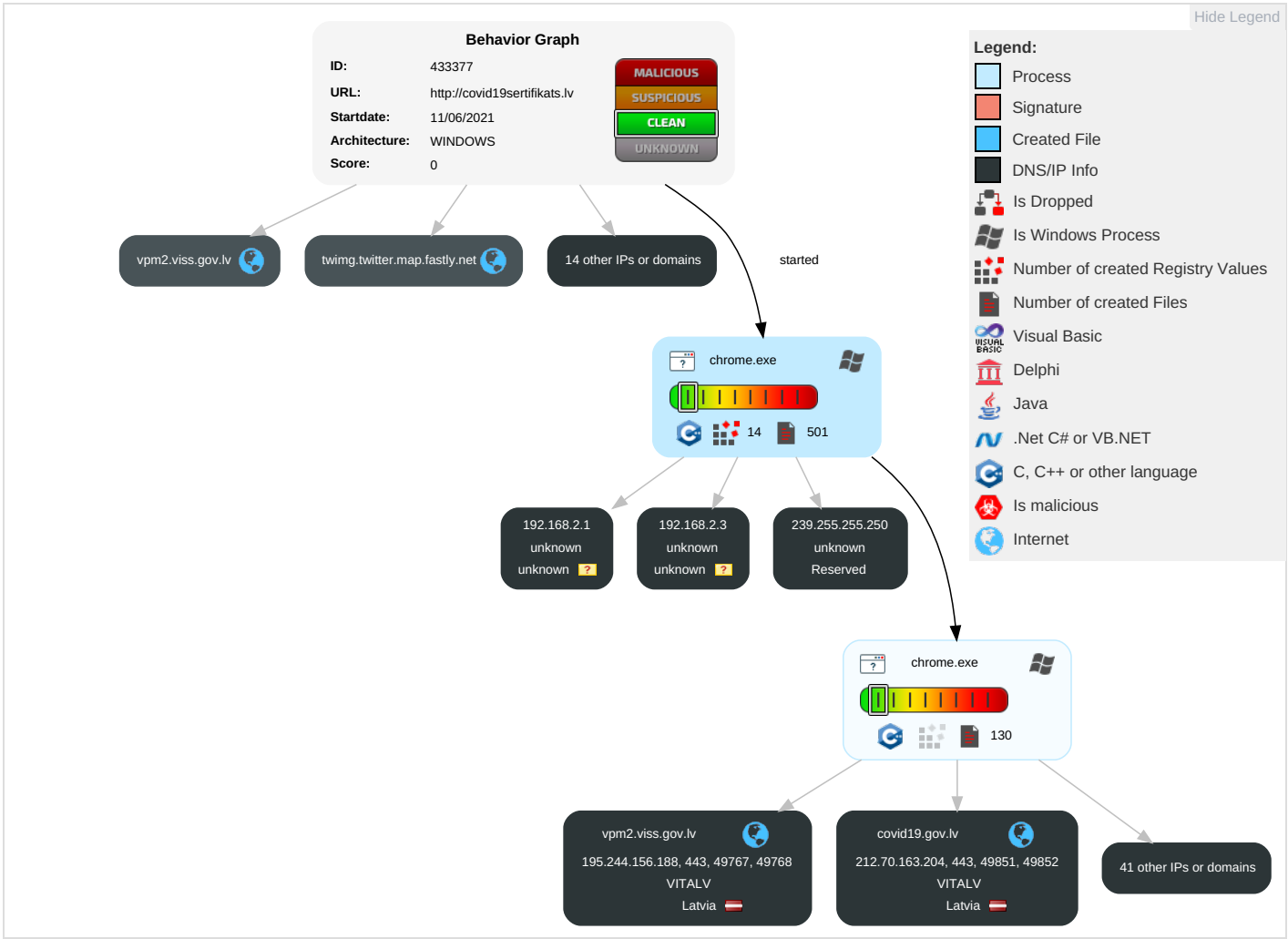
Click to jump to signature section

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	Impa
Valid Accounts	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	Modif Syste Partit
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	Devic Lock
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	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billing Fraud

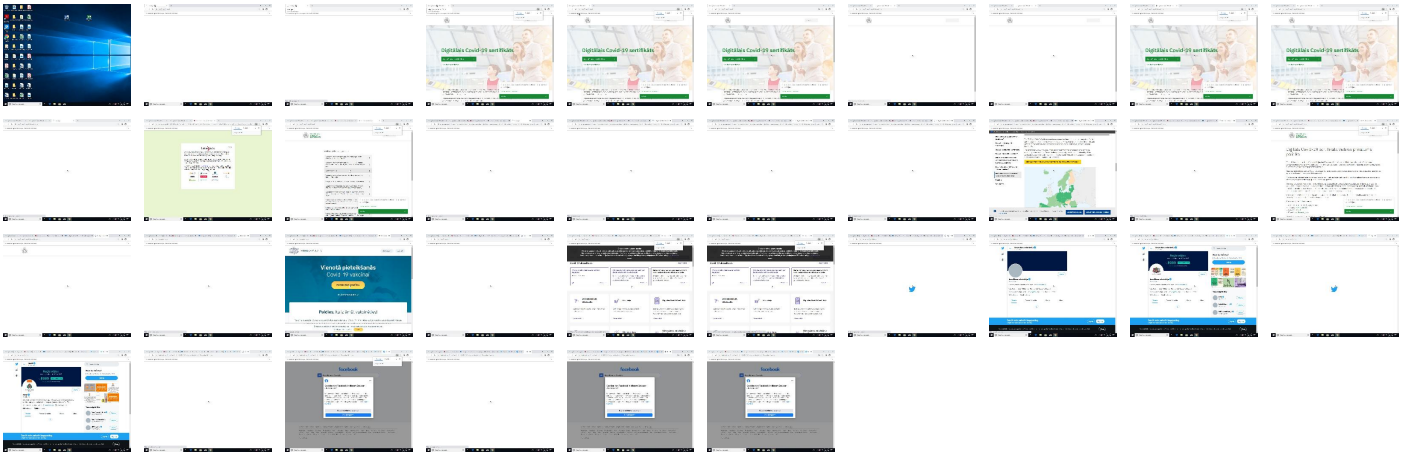
Behavior Graph

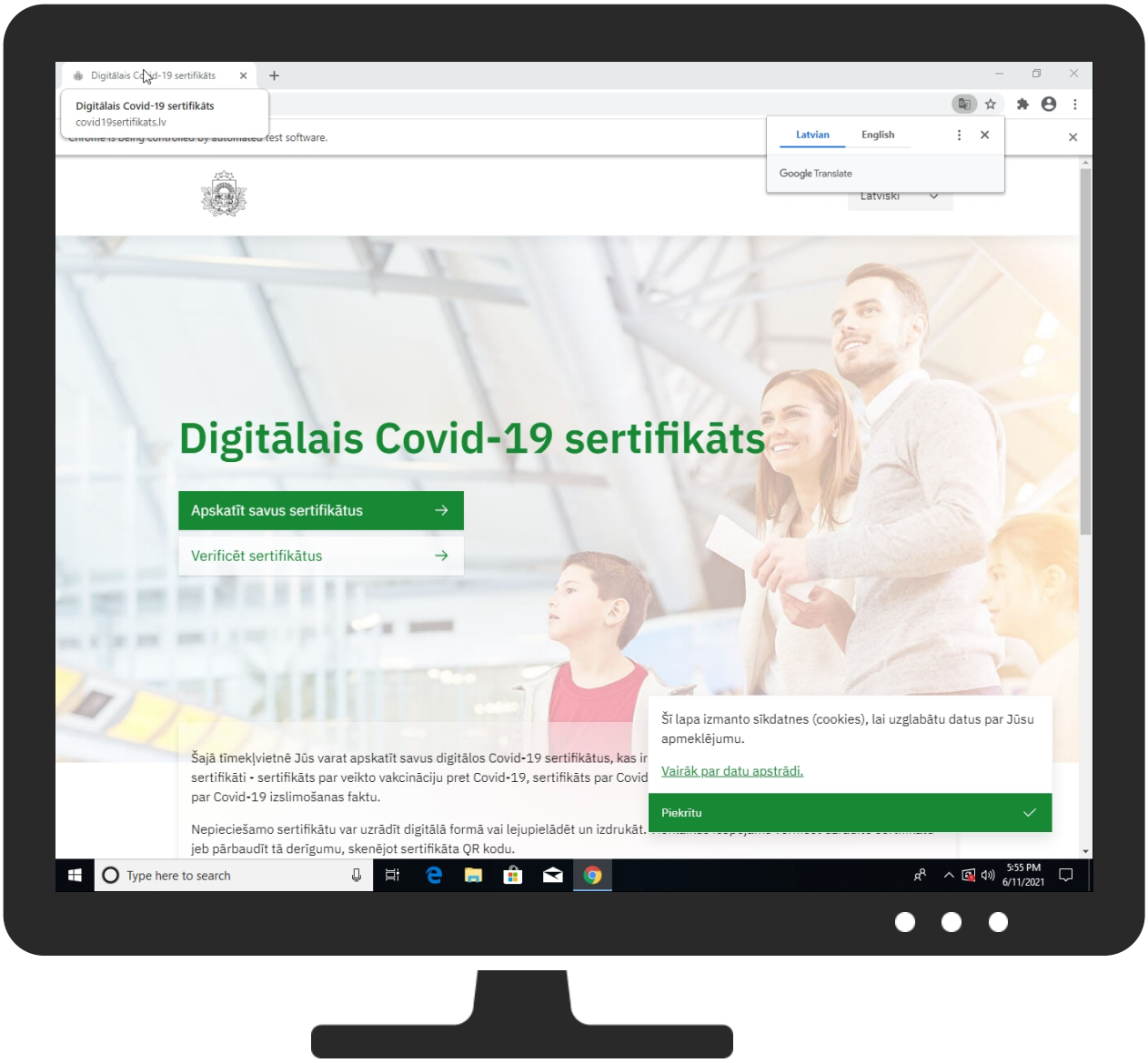


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://covid19sertifikats.lv	0%	Virustotal		Browse
http://covid19sertifikats.lv	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://redux.js.org/Errors?code=	0%	Avira URL Cloud	safe	
http://https://covid19.gov.lv/3covid19	0%	Avira URL Cloud	safe	
http://https://covid19sertifikats.lv/Home/Login	0%	Avira URL Cloud	safe	
http://https://manavakcina.lv/index.mv.84b7e3c4c2ad458fafc8.js	0%	Avira URL Cloud	safe	
http://https://dwo3ckksxlb0v.cloudfront.net;	0%	Avira URL Cloud	safe	
http://https://covid19sertifikats.lv/Home/AnswersJaut	0%	Avira URL Cloud	safe	
http://https://covid19.gov.lv/sites/default/files/js/js__Ta5swb09yQErhhz1adSh6m2iHvFEkgJlSZ-FbHozh0.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs531.wpc.edgecastcdn.net	192.229.220.133	true	false		high
star-mini.c10r.facebook.com	31.13.92.36	true	false		high
covid19sertifikats.lv	104.21.8.55	true	false		unknown
manavakcina.lv	104.21.35.245	true	false		unknown
twitter.com	104.244.42.129	true	false		high
star.c10r.facebook.com	31.13.92.10	true	false		high
cs45.wac.edgecastcdn.net	93.184.220.70	true	false		high
cs41.wac.edgecastcdn.net	93.184.220.66	true	false		high
covid19.gov.lv	212.70.163.204	true	false		unknown
syndication.twitter.com	104.244.42.136	true	false		high
europa.eu	147.67.210.45	true	false		high
lb-webanalytics-ec-europa-eu-768915372.eu-central-1.elb.amazonaws.com	3.67.90.247	true	false		high
tpop-api.twitter.com	104.244.42.2	true	false		high
scontent.xx.fbcdn.net	157.240.27.27	true	false		high
t.co	104.244.42.133	true	false		high
cdn.matomo.cloud	13.32.25.103	true	false		unknown
twimg.twitter.map.fastly.net	199.232.136.159	true	false		unknown
static.addtoany.com	104.22.70.197	true	false		high
abs-zero.twimg.com	104.244.43.131	true	false		high
facebook.com	31.13.92.36	true	false		high
vpm2.viss.gov.lv	195.244.156.188	true	false		unknown
ec.europa.eu	147.67.34.30	true	false		high
googlehosted.l.googleusercontent.com	142.250.180.225	true	false		high
cs510.wpc.edgecastcdn.net	152.199.21.141	true	false		high
www.facebook.com	unknown	unknown	false		high
abs.twimg.com	unknown	unknown	false		high
pbs.twimg.com	unknown	unknown	false		high
abs-0.twimg.com	unknown	unknown	false		high
cs.atdmt.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.twitter.com	unknown	unknown	false		high
static.xx.fbcdn.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
webanalytics.ec.europa.eu	unknown	unknown	false		high
video.twimg.com	unknown	unknown	false		high
cdn.syndication.twimg.com	unknown	unknown	false		high
platform.twitter.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://twitter.com/veselibasmin	false		high
http://https://twitter.com/vmnvd	false		high
http://https://covid19sertifikats.lv/Home/Index	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.70.163.204	covid19.gov.lv	Latvia		8194	VITALV	false
199.232.136.159	twimg.twitter.map.fastly.net	United States		54113	FASTLYUS	false
104.244.42.129	twitter.com	United States		13414	TWITTERUS	false
142.250.180.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
93.184.220.66	cs41.wac.edgecastcdn.net	European Union		15133	EDGECASTUS	false
31.13.92.36	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
195.244.156.188	vpm2.viss.gov.lv	Latvia		8194	VITALV	false
104.244.43.131	abs-zero.twimg.com	United States		54113	FASTLYUS	false
147.67.210.45	europa.eu	Luxembourg		42848	EC-ASLU	false
152.199.21.141	cs510.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
104.21.35.245	manavakcina.lv	United States		13335	CLOUDFLARENETUS	false
3.67.90.247	lb-webanalytics-ec-europa-eu-768915372.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
104.244.42.2	tpop-api.twitter.com	United States		13414	TWITTERUS	false
104.244.42.136	syndication.twitter.com	United States		13414	TWITTERUS	false
192.229.220.133	cs531.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
104.244.42.133	t.co	United States		13414	TWITTERUS	false
104.21.8.55	covid19sertifikats.lv	United States		13335	CLOUDFLARENETUS	false
147.67.34.30	ec.europa.eu	Luxembourg		42848	EC-ASLU	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
93.184.220.70	cs45.wac.edgecastcdn.net	European Union		15133	EDGECASTUS	false
104.22.70.197	static.addtoany.com	United States		13335	CLOUDFLARENETUS	false
13.32.25.103	cdn.matomo.cloud	United States		7018	ATT-INTERNET4US	false
157.240.27.27	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433377
Start date:	11.06.2021
Start time:	17:54:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://covid19sertifikats.lv
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:	9
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:	clean0.win@49/591@34/26
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://covid19sertifikats.lv/Home/Index • Browse: https://covid19sertifikats.lv/Home/Login • Browse: https://covid19sertifikats.lv/verify • Browse: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en#what-data-does-the-certificate-include-is-the-data-safe • Browse: https://covid19sertifikats.lv/Home/Privacy • Browse: https://covid19sertifikats.lv/Home/Answers • Browse: https://manavakcina.lv/ • Browse: https://covid19.gov.lv/ • Browse: https://twitter.com/veselibasmin • Browse: https://twitter.com/vmnvd • Browse: https://www.facebook.com/VeselibasMinistrija • Browse: https://www.facebook.com/VeselibasDienests
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:55:39	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
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 GM DS.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\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,....,qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j._iK..|[.w.M.!<- .}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vI..x.R4...L.....%g...<..}'{....E8SI...E".h...*.....ItVs.K..... .3.9.I..`D..e.i`....y...,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.1263750649191113

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Encrypted:	false
SSDEEP:	6:kK3e8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:v8kPlE99SNxAhUe3OMx
MD5:	01F83B1B240FD6C858C395980F701573
SHA1:	156E63104149120E8F27C3DCA2959FA042792F53
SHA-256:	B7A6C03C9EF1F8C54622B8B1FC512F8B78CC1014D8362D69336FBFE7039C4784
SHA-512:	F6D3F4FC0D287D972F31A13DF7F80D71E054F85BD44A86A964DC698FBB6873D46FD8E3F1F2FC13B545C36EA047EE85C0BB0C2D2C50EC9D7B98ACC31D07FAB E1
Malicious:	false
Reputation:	low
Preview:	p..... .....j.%_..(..... .....L.....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.0.e.6.c.f.e.3.4.c.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\11bd410f-4d56-480f-bd5d-27567db5ca9a.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):	375560
Entropy (8bit):	6.049473446705501
Encrypted:	false
SSDEEP:	6144:pCNja4iMHEDg/z2ZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinP:0lat1W0GNPUZ+w7wJHyEtAWW
MD5:	2E3B76D4162EEAD06E27E8546538E07F
SHA1:	0A07F6A9DF41220F0EFAF93AF12F1304196DAC4B
SHA-256:	E17CC346AD8305EE81E4EFBFF844909B1208CE753B4B0D2F6F22C7DFCC25E71D
SHA-512:	48D8C09729AA15F3317CA50D2200BB9031A4C38BACCA234FD7BAA9DBB4C7E8F5E2B4F4E233B783BF7331566D06109562DDA459939FFB670B2D00FCB525BD63 E
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.62345932036463 6e+12,"network":1.62342692e+12,"ticks":152313148.0,"uncertainty":2814878.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5i S+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_ password_blank":true,"os_password_last_changed":"13245952488209722"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\216cf6ca-33d9-4c89-9f02-43f27ec61f7b.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):	375558
Entropy (8bit):	6.049473614289265
Encrypted:	false
SSDEEP:	6144:iCNja4iMHEDg/z2ZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinP:nlat1W0GNPUZ+w7wJHyEtAWW
MD5:	5BD2CD59C43B863ADB4E22A0C0CBC905
SHA1:	74013D7A41C9F811BA1BFD69FA8F88CF443A3852
SHA-256:	8F4244D2E1D5AC060EB914B3A938799C7DBF8DD81DE4E2BAE5442B6AE371B229
SHA-512:	D2B3EEA21971643F09E7EC0DF736A801FC57F3F056793703113F92896880EA2CED727E8C95DB2970E4A294462FF8D9B4EFC96E3E440D33AA29A2A8EFD60E2C8
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.62345932036463 6e+12,"network":1.62342692e+12,"ticks":152313148.0,"uncertainty":2814878.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5i S+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_ password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\21d99673-c71c-4079-af8a-c38caa634fac.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):	367188
Entropy (8bit):	6.0283896779822905
Encrypted:	false
SSDEEP:	6144:ECNja4iMHEDg/z2ZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinP:xlat1W0GNPUZ+w7wJHyEtAWW
MD5:	2781BCD32A0F9B174DCE700F1673302A

C:\Users\user\AppData\Local\Google\Chrome\User Data\21d99673-c71c-4079-af8a-c38caa634fac.tmp	
SHA1:	0FCD59A8D68688493AD710E25CF01BA8AECE3361
SHA-256:	6BD5E6F611489BF4214494944A678BB078161E9FDA5E4CE52E4209882C3054F3
SHA-512:	711BBF40DE3F8F79CA541FD6564D16DF221CA594653433874FAA3C88754B09E8ECA13399FDF64C09240D498789D2DA487AB8B084A53CFD616EE4A341FFE750B
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":1.623459320364636e+12,"network":1.62342692e+12,"ticks":152313148.0,"uncertainty":2814878.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488209722"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\599ab456-1a66-4935-8b7f-489866b9e06c.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):	367084
Entropy (8bit):	6.028192625919255
Encrypted:	false
SSDEEP:	6144:KCNja4iMHEDg/z2ZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinP:flat1W0GNPUZ+w7wJHyEtAWW
MD5:	875FB1B1DB160CC8DE57A23E90C6EFFC
SHA1:	4004AFFD67B3B05F6FCE40D2C5614A430E261A47
SHA-256:	1215EE2BBC747C9D24FCB6C6A1425F5FEC846846C176FD092D3DDAE6BB764E32
SHA-512:	D28E4928CB722B56C7DD12176EC7452BBB6F005FF88043BA2DE93C4DF7626647833EABEB2FFDFBCE56B35D40A0523B92E85A155997348056D7256FB77AAFF65
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":1.623459320364636e+12,"network":1.62342692e+12,"ticks":152313148.0,"uncertainty":2814878.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488209722"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\60c55983-1742-4b1a-976c-d7b97c757b72.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):	367084
Entropy (8bit):	6.028193036893676
Encrypted:	false
SSDEEP:	6144:ICNja4iMHEDg/z2ZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinP:Vlat1W0GNPUZ+w7wJHyEtAWW
MD5:	3731FEE69362C0197B048812B1AAA23E
SHA1:	F8F0AF96669FF4EEA5C6F8E3AF8F9DCC69131D52
SHA-256:	B0F96B597D8659DAE067873B1F5B1AB60B9B1314BFB5AA7CB657778AED5FC59C
SHA-512:	38CD3E2AE52039F6C00C1B1A813D6297080D2592D9C7D73CD68683C6BB141AE86FCC26B216CC83AD1E5BBD4CD8BDFA529FAD267AD4458BA1AF9077DE84C1CF4
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":1.623459320364636e+12,"network":1.62342692e+12,"ticks":152313148.0,"uncertainty":2814878.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488209722"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\668ada50-862a-4467-a7c4-9c88b28e3ea8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94052
Entropy (8bit):	3.752276369487486
Encrypted:	false
SSDEEP:	384:ozE7bJ+0xS1JVKAHmNnrkvTZ3crN0HdwGoHryNj7xkNJpIrC/ma9O5Hr/EOVVzNm:ya69tShkEceDPBdcPrOhKfpbsr
MD5:	17F14501531E76447D7F5568A5E08DBA
SHA1:	6C3991E35C3396D7107FA1CE551B650E38B6D4B6

C:\Users\user\AppData\Local\Google\Chrome\User Data\668ada50-862a-4467-a7c4-9c88b28e3ea8.tmp

SHA-256:	484B266A71D530BC370E4637DE588D1921D532CA06E0D006C936E2D249235D22
SHA-512:	987A57BBB29F876C33662F7887E40BC332A75F3C04921ED5A36C00E99FB9E1B31FEB7E4C54922867A6EB7DA3CF6413A7D9E731B0C63CBB9DBF04C22FCC73F5 A
Malicious:	false
Reputation:	low
Preview:	`o.....*...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....<8.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\7221b5a6-c255-4986-aa7b-d9338afd360f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94772
Entropy (8bit):	3.752041049364031
Encrypted:	false
SSDEEP:	384:+zE7bJ+0xS1JVKAHmNnrkvTZ3crN0HdwGoHryNj7xkNJpIrC/ma+AO5Hr/EOVVz5:ca69tShEEceDPBdcPrOhKfpbs+
MD5:	DF42016323FFADC9162C6828F015D157
SHA1:	8288F8BED18311E4DB5AC8ADA8E0AB70C48A42D5
SHA-256:	A36011A62194EFAA8E078D4872597E5975F52E8C5566BE424B88CE77F8E5D790
SHA-512:	981ABF5E3891E1FA907E39A38E9D9CE8CDD56D0F729B1A1C0A2BD54B8C65092CF977D06FE41A1D8AC59E0850E2A8E58765847F863A261095C7CD269785C2668
Malicious:	false
Reputation:	low
Preview:	0r.....*...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....<8.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\76f24155-4449-4968-896d-d047d4bb49a7.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):	375557
Entropy (8bit):	6.049474075173929
Encrypted:	false
SSDEEP:	6144:TCNja4iMHEDg/z2ZG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinP:Olat1W0GNPUZ+w7wJHyEtAWW
MD5:	D9BDD4BB94B0F4CCB78F7529557B27B2
SHA1:	6D43362DD16BDECF64EFFC6A327428D8F9021C5B
SHA-256:	8B79D001C9944972C539EB121083FAAE923CAD8BD66DF410BB037F19C27BA08C
SHA-512:	22D9441487E3C2D2ED2E5516137E6E0A7CBD6874E89DE2F4D6B7FF0914AA259433FFCA7F061D5AFC58D00C8A88F1FB6B2C53206991F7E74334C9EA97048224A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time": {"network_time_mapping":{"local":1.62345932036463 6e+12,"network":1.62342692e+12,"ticks":152313148.0,"uncertainty":2814878.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5i S+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_ password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"displ

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:FkXEwozZHGftEwozZHGftEwozZHn:+EwozZHGVEwozZHGVEwozZHn
MD5:	4829695F153A750ADF50C6E979E8E8F3
SHA1:	2F697EF207460D03671E4B59670BC73328D60D6E
SHA-256:	1AACF1304FD42C84FF41DDD2F2252E5C0EDE7362352661B7957648F2EA4C2683

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
SHA-512:	6D16A6EF4BB20B25B1B14757C475E9F8C3A40D6181F718D563A628BA41DA9426E1B586C472D4F8729FD65FCA014151B7D46FBFAAE171BFF9A6D937DB7A7A2C(2
Malicious:	false
Reputation:	low
Preview:	sdPC......................y3..M.Y.NbD.sdPC......................y3..M.Y.NbD.sdPC......................y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\19c7ff54-4609-4ad4-8e78-7ec696476a72.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2! F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ac854df-9884-4eab-9424-cb46965975f9.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):	5830
Entropy (8bit):	5.18377777192483
Encrypted:	false
SSDEEP:	96:nfXbB0H22R8WtgwaAVVxk0JCKL8XkU1f3bOTc8Vuwn:nfXbJ2Rjb9V4KGkUBzK
MD5:	F891808182E8CFB21B9333897268C64D
SHA1:	A434F1F3AA2D3FEFC4F5DB84E12193924722AACB
SHA-256:	7B33587E457ECCDC26707FFA988C68DDBCDF13EABA29C457BA29A66B01B8D15D
SHA-512:	68F818874CCDD5E55B2E246E10598F0ECC170E7BFEF209FE6F100B0FF0C6DEA8C6B31C0777DADBD740D6446C8FA2812E576A862F2566180FD8909C0A0020CC!
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267932918456941","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2b8af370-18d1-4a35-81ec-1791332cbd54.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):	5838
Entropy (8bit):	5.183543725722396
Encrypted:	false
SSDEEP:	96:nfXbt0H22R8WtgwaAVNxk0JCKL8XkU1f3bOTcyVuwn:nfXb12Rjb914KGkUBzE
MD5:	A03E2BD91C3432409267AAADD6526EC7
SHA1:	C6FBC66E45F11580800EBB73E516BE28B48ACDDC
SHA-256:	57DBA9AC3630D0AD4EB5513E038FFB7C3CA22D999FD34C5DB2D4FBA0AA8ADF58
SHA-512:	2B88155E56A1B74B8553372CE25E6B8440F6D48D9492384075781E9FEC3C0BD4FBA8D47A73ECEFD0B724D85B623CDEAFF1001E2E6FD79969A9E0CDC86A7AFB 0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267932918456941","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2ba41208-b869-4bd1-8d0c-419dd0ae0426.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\353c4eb5-3696-4ec3-9f6d-e0ab4b60c5d9.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):	22594
Entropy (8bit):	5.535753598035655
Encrypted:	false
SSDEEP:	384:2aUtjLlYSX61kXqKf/pUZNCgVLH2HfDsrUbHGtnTpRubF4b:wLld61kXqKf/pUZNCgVLH2HfQrUrGtn1
MD5:	E056D8D03189FE7F6B56AF1BF43EC469
SHA1:	8E19DEE9F1C220001B0B10F73E96D04B45E8BD7D
SHA-256:	0BED9F428A657C514C048CA7AA17FE398F2BC97C2DFF63366F4054261931156A
SHA-512:	5057CAB5417C8DCFB4D6EBF6F9D415CABE2C6AFF5B7B84DE99A12B26269830C363AE68206D18FF9A17B37CECCFE17DBAD0795DC8C7F8E42F92A3367BB900EB91
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":"13267932918199795","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\40b0f0a6-074a-4e75-b9b9-93f9b4626325.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):	3968
Entropy (8bit):	4.869205332444408
Encrypted:	false
SSDEEP:	96:2lNnOTXDHzhocIPaFGeHOuLG+fx06g6k6ARKZje0NGKQhS:2lNnOTXDHzhocIPaFRuuLXfx06g6k6AS
MD5:	30BBBC728BD533F0FC0EBB8177F56462
SHA1:	6D01587D708C5715E32F76F7EC74F6B73F931165
SHA-256:	CA91B35E5397BD0329025390041C64B54CFE6C6CFFFECFE168EDDB8E638B7ED7
SHA-512:	3E5FE82A7E5E6DA593060C80B457A79DDB8032D18AC27B213DAA6B0E196A661D5C9629DECFDF8802612C42A3E7A19E68E1041172CC58A0796B116283210EDC2B
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"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":"13270524921052484","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270524921059437","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\51b73afd-5187-46df-99ac-31fd3b338050.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\51b73afd-5187-46df-99ac-31fd3b338050.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5830
Entropy (8bit):	5.18416412648244
Encrypted:	false
SSDEEP:	96:nfXb40H22R8WtgwaAVUxk0JCKL8XkU1f3bOTcNVuwn:nfXb82Rjb9q4KGkUBz7
MD5:	5A8E676D610FAB79280ECB3DAAE47DA6
SHA1:	A90AE876B23B137B26C34947EE47BE1FB59DF530
SHA-256:	EB1167798838CC2701CBC047ACB9733961BE81B445015DFF97560F635E37115A
SHA-512:	845C2E24B0FE31E3455B801E662E5BB4A00B82F07AD9976C54CF0FDD53D0D60D102799AA8195AB66F6B4081EDD8AD23A5A2B161BF73D28615558C6A09267A22
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267932918456941","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5569dd88-e744-4ab3-83f8-ea2f64a9c6d1.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):	1042
Entropy (8bit):	5.564967397692556
Encrypted:	false
SSDEEP:	24:Yc6H0Uhc7nh7UcYG1KUe4aUej7wUsk3RUeHQ:Yc6UUhcbtUcnKUe4aUefwUskhUew
MD5:	0CC0A9F13CA568988C24ED151C9D26A3
SHA1:	55A4206CD23BB208E603BFC6B2AFC804938C76F6
SHA-256:	0B6E0B327721BE4C71BFD0E947DB1CE26FEA16283ACA8538EB93EB9967E93BE1
SHA-512:	C962BFA6BDE36F395567FF64559642FD539566C37CF52A0D30ADE89D704D53009576E5D614642CB4C5885D46F9A17B9E64D7974189AD0A04B2773F686886DDF1
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1639529743.646702,"host":"clTnSQUViyiD/hUxhBWAV6mGm6JPIToPN7f/PK+cFFg=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459343.646706},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.52056},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.455726},{"expiry":1654995321.052961,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459321.052965},{"expiry":1633015352.814139,"host":"+ccWXqaoHJ9hfuXbleKV6FQUrBlyXAJ31BdqjNQJpHs=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5dd7d96d-2c9e-4493-bba4-c689aaa8759a.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):	5878
Entropy (8bit):	5.184333025259614
Encrypted:	false
SSDEEP:	96:nfXbnS0j22R8WtgwaAVExk0JCKL8XkU1f/YbOTcGVuwn:nfXbS2Rjb9m4KGkUB/wA
MD5:	5684BCD70B3BF296841D1E0EE94CBB41
SHA1:	2096569ADB4D1E2DA4875609715B13ADD2567992
SHA-256:	90AAFE4387775899783ABF321411C669B6ED278A6C90B517C014EBF2AF8EBC00
SHA-512:	2B8E0A2674EF249C39073CCAD49B8502EC6F07ED655675260A368F17A5E437EF859FA5837BCC02FEEF6B87C23FD721525D3D553823A0FEB071CC001855BCDEC
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267932918456941","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\62e80b6b-8321-4ad0-bd3f-f3a8cfe2efdf.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):	3051

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\62e80b6b-8321-4ad0-bd3f-f3a8cfe2efdf.tmp	
Entropy (8bit):	5.590539077526432
Encrypted:	false
SSDEEP:	48:YrBFUhJU1UkxLUCDUvieU0p6UUhcCOUjTijUFk2tUbyUSU07KUeJH5lULCaUefwQ:UUbU1UkxLU0UvieU0wUUatUjejUFkSUS
MD5:	D2CCC52FE46BEDE4B593AA5A5FB465A1
SHA1:	8B273B5ADA304EFAEA02C455C160C242B77DF55A
SHA-256:	D0F9180D2245D7FE3F669C84C9A32BA709D2D4BF7047B59AD8918D9C7570990E
SHA-512:	3C41D155BD0C2BA87CAA35EB801CBB7DBF45F46A9FA1C9235E36ABFC6D5EDCA8D8D2014CEA8614E8BD80FF44DE3FA5B0492434D1A649ACFCA0A1F9A50526BB4B
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1654995406.65653,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459406.656534},{"expiry":1654995399.538869,"host":"C6hhjoa/UfPQDtK7OhzQayqV5YYV+Gd1zl/FgGIO4iI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459399.538871},{"expiry":1639529802.469521,"host":"Hz3u5e/0OvonbzKxpwGRW5pHRzx3H6Okuh6uuA4p4KI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459402.469525},{"expiry":1654995405.671928,"host":"l/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459405.67193},{"expiry":1639459394.080658,"host":"MFddpJY+raI7hVp8ouF/0Zxwww7coad4RrFj8Om6ixA=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623459394.080663},{"expiry":1654995397.262966,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\65659340-147c-4856-a07a-4ccd0476ddbc.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):	3555
Entropy (8bit):	5.593178114149962
Encrypted:	false
SSDEEP:	96:uUgU1Uk65LUxUvieU0wUUa2U+HUjejUFkSUCyUSU07KUQnUvUpaUQrUMvUsuZ+UB:uUgU1UJLUxUBU0wUUa2UiU0UzU/USU0o
MD5:	1716983C2EE1F26ED532E11AB5BF13D9
SHA1:	B5C02E2D92E2844B08E67BCE2AB835D9BCC94C31
SHA-256:	46908F6FB71B70B66F1A932959A6C270A4CA78379F1413B627C135C1D74B8FF8
SHA-512:	9A79514665A6AEF336CBF0539F86CBF469B9F94C1108C3B64BBEA1F890F672196ABEEC8D47D3F69E5C71943E9D9FB407906B38BF5217DBBEB2B4CB69666297F
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1654995416.671329,"host":"AYn/0RUuCA+dtfJ8evM2C7EY0gUuiaPUwyQjHng621k=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459416.671333},{"expiry":1654995399.538869,"host":"C6hhjoa/UfPQDtK7OhzQayqV5YYV+Gd1zl/FgGIO4iI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459399.538871},{"expiry":1639529802.469521,"host":"Hz3u5e/0OvonbzKxpwGRW5pHRzx3H6Okuh6uuA4p4KI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459402.469525},{"expiry":1654995416.220888,"host":"l/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459416.220892},{"expiry":1639459394.080658,"host":"MFddpJY+raI7hVp8ouF/0Zxwww7coad4RrFj8Om6ixA=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623459394.080663},{"expiry":1654995397.262966,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\799219af-50ee-41ac-b587-b695bed9c5c9.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):	1377
Entropy (8bit):	5.571604661208686
Encrypted:	false
SSDEEP:	24:YdrUO6H0UhcCOUjWnh7UDG1KUe4aUej7wUsk3RUeHQ:YJUO6UUhcCOUj+tUOKUe4aUefwUskhUD
MD5:	D441EF19823540E1FDCE225570263AD5
SHA1:	1871A3856B165294928FDF69B91D6740A143ECB0
SHA-256:	92D3CCD88FE7A0539DF6A90C17D85F44999B697424DCA9084E97F537CA668F71
SHA-512:	1CAA93A6A26DA7046A89AFBE28CCB06A78AC29451B9B2B8C59805550D8A5C60DDB77D2043D345ECFAB35F47D7572168EC7A79F2EF7D2E2D676E31F01A297C4B5
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1639459394.080658,"host":"MFddpJY+raI7hVp8ouF/0Zxwww7coad4RrFj8Om6ixA=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623459394.080663},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1639227384.268191,"host":"VMy90+5OQNYDejoSpUoJrf2GLOpkal3il1JxdxniiWA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459384.268195},{"expiry":1639529790.677657,"host":"clTnSQUViyiD/hUxhBWAV6mGm6JPIToPN7f/PK+cFFg=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623459390.677661},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPI6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.52056},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_o

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):	340

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Entropy (8bit):	5.2126612395432055
Encrypted:	false
SSDEEP:	6:mw+ElL+q2PN723iKKdK9RXXTZIFUtpD+VWKz1ZmwPD+V8lLVkwON723iKKdK9RX3:SEIvVa5Kk7XT2FUtpCVWKz1/PCVY5Oav
MD5:	268BE5F722583829D404F1A3F5D3D1B5
SHA1:	A9207BFBC3D29AC434757203FAC94AF0DD9A5883
SHA-256:	C886DC712F9E5621F557D157FB1A52CFDD5C851F34F7EA03A0C7D2A354559AA5
SHA-512:	8998358146F5A7317DDB63EB0109293B500715A2D5C46B6AE01890ED5E218365B6C2B22098EC9F2810865884C2A24F96A78F89384BAC33DCD8472AA6AD27086B
Malicious:	false
Reputation:	low
Preview:	2021/06/11-17:55:22.881 1758 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/06/11-17:55:22.923 1758 Recovering log #3.2021/06/11-17:55:22.928 1758 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):	324
Entropy (8bit):	5.188831271752377
Encrypted:	false
SSDEEP:	6:mw+RHlL+q2PN723iKKdKyDZIFUtpD+rQ1ZmwPD+G4lLVkwON723iKKdKyJLJ:SBIvVa5Kk02FUtpCrQ1/PCnz5Oa5KkWJ
MD5:	A9E1F258FA054137D5040572CE74C86F
SHA1:	9977C0CEC43E91515A234FA2C5082760BB0A4637
SHA-256:	2891A7042332AD9FE0DF976DE2F61C8DA0C2A1EE8EEB331AE9704B4BDF95BA37
SHA-512:	27DF775FF5C34A4EBA3B983228FCBA3F0A1334549BA86D7C2D2D2CACE5659381BD2CAB5E02240743310940FAFAA5669FD39E9DCFDCAD82C6C17D08D533E5D5B
Malicious:	false
Reputation:	low
Preview:	2021/06/11-17:55:22.871 1758 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/11-17:55:22.872 1758 Recovering log #3.2021/06/11-17:55:22.873 1758 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\0151747867121a2f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4112
Entropy (8bit):	5.757864820380474
Encrypted:	false
SSDEEP:	48:mi4u4x2YTPuciiZwwDlFVvWNeKlYzcw0v6/tq7dsf6yLJLzw2denf3mrcenJsn0N:mv9PucheNeKCg6Fq7GCyL5hdenf3NLtO
MD5:	AFBC76EFD398A3FF8BFB2F9F0C2B1E80
SHA1:	2C340E1F6648557837AEACF7E85B4AC2E70844A7
SHA-256:	71A22D184DB02713D88160319BE3A12D968CA40A295F939F882097226A7AC2AE
SHA-512:	AFBD7CF7135D6B76BBFF658C7CBBC43B5A977F6DE6AC9B082234414FEE2B78F09067D47ACF3E36240685A105BE2529582E8F02145C331B0B5C66336760E0D3B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....ZX.N...._keyhttps://covid19sertifikats.lv/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js .https://covid19sertifikats.lv/}#.\.#/.....8Y.....EZ_....{....h.c.m....\...w.<b...A..Eo.....Fh5.....A..Eo.....}#.\.#/.....'.....O.....5.Dq.....(S.0..`.....L`.....(S...`.....HL` .....Rc@.....QbF.!.....e.....Qb...:<....t.....Qb.W.....r.....Qb".G....n.....Qb.S.|....c.....Qb.dG.....o.....M....S...Qb..y.....l.....R....Qb.....f.....Qb.E.u....d...k.....I`....Da.....(S....Ia#.....@.-....hP.....\...https://covid19sertifikats.lv/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.jsa.....D`....D`....D`.....4...`....&...&....&....&.(S.t..`.....0L`.....Qd.........Qd6.....innerHTML.....Qd.....childNodes....Qd&..O....getAttribute.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\03d628a7a533ced1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7911
Entropy (8bit):	5.5895655524685015
Encrypted:	false
SSDEEP:	192:yx4q9BuAnZNwB7OMYrB6irMzFflNyCYdK:fMIKsiAzFfnyfK
MD5:	EB4DC322C9D705C8D430FB085B744B32
SHA1:	D563F862F88D401D309E958BE9466292C6FD8072
SHA-256:	6E167F86639952D0C02D80C24F834617DD0509FB14449892F5419FD4872A3363
SHA-512:	15822728B0CFC39FD07280F758D41DAC235EF734441BAF45ECDAF2C95A7A3775135D95290B2059E8017F421C785F14FB664530056B7C6B346DCB7FF00674666C
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\03d628a7a533ced1_0	
Reputation:	low
Preview:	0\r..m....._..........._keyhttps://abs.twimg.com/responsive-web/client-web/polyfills.07bc4455.js .https://twitter.com/.].a.#/.....#.....v....a.....+...T.[j..l.+....9n.A..Eo..... ..US.....A..Eo.....'.s ....O....`.....L..... .....(S....`.....@L`.....QcV..G....window... Q.pb4....__SCRIPTS_LOADED__....Qc...0....runtime ...Q.PJ.f"....webpackJsonp..Qb.....push.....`.....L`.....`.....Ma....@...`.....`.....L`.....`.....M`.....Qb.m.....w92O`.....$..a.....Qb~..'....QrtfC..Qb2.....fRV1C....C.(S.L.`N.... .L`.....4Rc.....QbB.C.....t...a$.....a.`.....5.a....+.....!....a....%.....a....$.....q....a.....a.....Pd.....push.Qrtf..a....~<...(S.@..`<.....L`.....4Rc.....Qb..... ..e...`$..l`....Da....P<.....(S....`.....L`.....Rcf.....*.....Qb:..Y....n.....Qb.@&.....r.....S...Qbr.v.....o.....Qb.....s.....Qb.....c.....M...Qbv.....h.....R

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\08c402a54ef9a06c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	54928
Entropy (8bit):	5.660162136829413
Encrypted:	false
SSDEEP:	768:Y6Evq7oeg9zJdURgc6PJNwuXbY6rYaG6W408DAJHRzrinvti:Y0Opmg9PZXRrRnW4080cQ
MD5:	643EEF138B3C880EF27F25EB37790E28
SHA1:	7435BDBD5D063C78F5DCE4E2E1560E3ADEC3DAA3
SHA-256:	3F39DF8728326F6DD311F21D61F4B2362BC015A556A6F60926E50AF37C34034A
SHA-512:	70E574E39954C270644A53F8FA9F702FCD9194960154365B6B7E4A643F22CB903D35A1EAE5454558272AD057CCA2273BEE0FC06EABF0870679F3FEA09CFF81D2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`....f.f...._keyhttps://abs.twimg.com/responsive-web/client-web/sharedCore.8be6fa25.js .https://twitter.com/U.a.#/.....('.....-..l.u.l.%8.#..).O.Y..}..&gt..A..Eo..... .....A..Eo.....'..v....O.....^.....(...L.....|=.....h.....(S...M...`N$.....u.L`.....QcV..G....window....Q.PJ.f".... webpackJsonp..Qb.....push.....`.....L`.....`.....Ma.....`.....e...a.....Qb~.....+TpoC..Qb*.V.....0+qkC..Qb.w56....0JWCC..Qb^.@....0PHdC..Qb...;....0mK8C..QbrV.H. ...0mVXC..QbRZ.....0pUJC..Qb.5U.....0rY8C..QbJ-3.....0yYuC..QbF<.^....1AUCC..Qb.....1auMC..Qb..XB....1bnCC..Qb>.....21TwC..QbzE.....24HDC..Qbf.?.....2My+ C..Qb.L.....2c5uC..Qb.D....2qJZC..Qb.rv....2qZsC..Qb.....3A2yC..Qb.N.....3JQtC..Qb*).....3Lh0C..Qb&..7....3nOAC..Qb.....3rWKC..Qb.....3wZRC..Qb6.x.....3zeGC..Qb .us.....4bW+C..Qb.....4hQ9C..Qb.....4q8GC..Qb.]......4z

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0915368a311ce8e2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	108768
Entropy (8bit):	5.797752825300902
Encrypted:	false
SSDEEP:	1536:k1xCAZ+HtqBmQjs/VWhLtJ3GPclqYwrnpXw/VclpZvA/mmyQNNAt6EU:RAnCVWrkklqYwFgajZY/FhNNPEU
MD5:	5FD4521DC04DCC1078784947957DDFD9
SHA1:	1E6C4D89A9CAFC444C486F1710F7C6A36AAB65C6
SHA-256:	F82A6962F5127D9BA559E7067F5D399A9F85BF1EBF410F22708F93AB178A8C65
SHA-512:	895FF4CAD2CCCE0BB3A2E6E8F54A66735FBCFBF0213FD5C6B299B74B9F33C0780B203C0A5A7EA44ED1B9A01DD2F3528B114E30C74D0041E080C886F6FA3BDF 9E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...*.E"....6A910BA184DB86BC9F3656836AFB3480F35BD7C3B977B3BD578476F7A08060C5.....'..r....O%...x....(.....T...$%.....p..... .....(S.<..`4.....L`.....L`.....QbV.x.....site.(S....`.....L`.....XRc(.....Qb.W.G....e.....Qb.R[E....n.....Qb.....r. .....S...Qb.....o.....M.e.....I`....Da"...6.....QcZ.1 ....window.....QbJ.m.....self.(S.P.`\.....L`.....4Rc.....Qb..K.....t...`$..l`....Da....b.....(S.P.`Z.....L`..... 4Rc.....Q.`....I`....Da.....Qc&.d.....document.(S.....Pd.....t.exports...a....s...I..1..@.-....hP.....Y...https://covid19sertifikats.lv/bundle.min.js?v=RBChujdmhI DI2ZMrjLlOGNm9q6GEDofzToHYAUIP14U...a.....D`....D`....D`.....-...`....&...&..Q.&....&....&..Q.&.(S...%%..`.J.....L`.....Rcf.....*.....Q.....S.....M...Qb.1r....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\099b18f56e07077d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7912
Entropy (8bit):	5.664201501231015
Encrypted:	false
SSDEEP:	96:4DoaLALMU6Opz6C2z/I5+JvDlTCk+vVa1KBY0/6fr9ujovUfef/C2urXu:4Doa8g4uoACk+dsusvUfQ0+
MD5:	FF410157488E12FBE5ED0C2E99EDAFB2
SHA1:	039908A01BB0AE3467B734030C6838F821758160
SHA-256:	1738F66B20BC71E053858DBC343441D98A1C3FE25C53871678E7298144882270
SHA-512:	E745638F011C80E7A0675EE08BD04BB22824A9F4931DFD64C3682322265270A69C43CDC1CC732A31B384F28CCF37D09B9485CA4BCBC8AFE4103B0D462CAB64E 0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\099b18f56e07077d_0	
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/ys/r/G4IM2M9gECd.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..3b.#/.....~M.....I..(.....W.tl..B.m.::...ZV..A..Eo.....A..Eo.....'..1....O....X..... e.....(S.M...`N.....L`>.....Qbf.:....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`.....M`.....Qc..Jt....EdoW9lL...Qb.k.d...__d..(Qh.aO....EventEmitterWithValidation.....`.....M`.....Qe.l.....BaseEventEmitter.(S.L.`R.....L`.....0Rc.....`....I`....Da.....(S.....Ias.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/ys/r/G4IM2M9gECd.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`,...D`.....u....`....&...&..A.&.(S.....Ia....Q....f.....@.....@. ....I...!.d.....@.....D&..A.&.(S...`.....hL`0....@Rc.....O...Qb.h.....h...b$.....I`....Da.....(S.....Ia....p.....M...q..d.....@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0bc82c421f946785_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	15952
Entropy (8bit):	5.710101432518219
Encrypted:	false
SSDEEP:	384:kWVDw8WHITvKnGEtF2p5nxbaP0Up2VT4h7Jue5kO:kWVDw9uvUHtWxbk0U0VTA7JuA
MD5:	002133A1D389369B5E33360E100D6136
SHA1:	CD6CE607354AE7B2CEEE9715EE5B3B55EE778409
SHA-256:	C8291133F0E05E3B44D66483E20564ED78329042C65ABBFF687D0AB3DF763EBE
SHA-512:	4BEE2294F5C2596A78051AA5C7FD0808B781B8E7CFFBEE374A2FB1CF8BBC45F973531B8A2BA528839AEB66120A31073FA7EF40DDC1C220339C9EA1BBB3C73611
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....V.o...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y2/r/yoPEcJTVHGk.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..<b.#/.....fN.....OO.....%...,p-;..6>L_.Z./.../...A..Eo.....J.....A..Eo.....'..f....O.....<....y.....$.....(S.e...`.....L`@.....Qbf.:....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`.....M`.....Qc.L.....BAVMM6Q...Qb.k.d...__d...Qc...v....Toggler....`.....hM`0.....Qb.$R.....csx...Qdr.....invariant.....Q.@f.....Arbiter...Qd.....ArbiterMixin..Qb.4.....CSS...Qe6Z.....ContextualThing...Qb:B .....DOM...Qd. ~.....DataStore.....Qc.B.#....Event.....Qc.n;.....Focus.....Qb..%.....Keys..Q.@&@}.....Parent....Qe6.....TabbableElements..Q.P^.(.....TimeSlice.... Qf.....createArrayFromMixed..Q.`..n....emptyFunction.....Qb.D.....ge... Qf.....getContextualParent...Qe.\.....getObjectValues...Qd2.G.....killswitch....Qc.6P.....mixin.... Qf.....queryThenMut

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d1a5c04da6aa504_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.405690190906457
Encrypted:	false
SSDEEP:	3:m+lOO308RzYrSLLiMIwJJSMkTAg+9tlHCYy3Qi5DKhInAkRmllXpK5kt:mWVYGL+MIwJJ21aS2aDQItAllZK6t
MD5:	8686850974AEB6D03B8782187050EED7
SHA1:	FBBBA8A5E8ACC6735082EEF61F3961F115C3D75C
SHA-256:	58ACBF377D2BB5A0D95F9278EFE7425A10B7649F09ED0B8BA36F05665F76E08D
SHA-512:	B05BE21806F69DBAD563F3B42E727478DE08561EBF6C8AB09D1C78116CEEF4600D83508455C1E04FF0C5DEB5D01DF070CDA3096722FADC39DDC902765010805D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J....._keyhttps://www.google-analytics.com/analytics.js .https://covid19.gov.lv/s.>a.#/.....=.....L.GC...#. ..k.B\....6..E....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0eb0b9bf0910724f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	107584
Entropy (8bit):	5.581437017860984
Encrypted:	false
SSDEEP:	1536:u3OQWf8x95eP4dKYpH6mouJ4Z+2zlqQjMPeHTg0MBSA5FHNvBA25RpNAHYLr2yag:KZrx8+2cm9Uq34LFarwm2iKz
MD5:	A72DFC9EF732EEC0B45B05E4AA1D7C1B
SHA1:	345FF2D041516F4305E1FF787A75A121B4DD1FB9
SHA-256:	77696DA9BB4A2F364EBB37B11197CBF1E7D32FDC289F95FBEDC1023441F4E22D
SHA-512:	86A0AD6654EAA4684CE6FCC6A5898F8CCBDED31393E1E4267F39A9DD8844BF9C147C982B7A29B5EBFED984173735AA0970E704918A3BF8CFFEFB9DC54F7C43A0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@..../M....31C18C1DC77D3B93B8108BEE26E1B40B56AFE1A0B44B4DE7AD92816ACACE42A6.....'.....O'.....~.w.....(...`...,.....`7.....T.....(S...a...`|(.....L`>.....QcV..G....window... Q.pb4.....__SCRIPTS_LOADED__....Qd.~+4....polyfills.....Q.PJ.f'....webpackJsonp..Qb.....push.....`.....L`.....`.....Ma.....`.....e...a.....Qb..O.....+/1jC..Qb...U....+/eKC..Qb...r....+E13C..Qb..3.....+KXOC..Qbn.....+d3dC..Qb>....+h/3C..Qb..R.....+kY7C..Qb.E.....+wNjC..Qb.v.~..../1ytC..Qb..t\..../2CmC..Qb.t$...../4m8C..Qbfg!#..../GyzC..Qb.8.K..../NU0C..Qbb..x..../x6eC..Qb.;...../ywFC..Qb..^....065xC..Qb../.....0FSuC..Qb..F.....0m3qC..Qbz.....0vv5C..Qb.a7.....0xiiC..Qbn.V.....0yigC..QbJ.....1Mu/C..Qb.'.....1htFC..QbN.....1odiC..Qb.`[.....1wVrC..Qb^.....1xLlC..Qbb.u.....20IMC..Qb.y.m....2G9SC..Qb...}....2g+pC..Qb...)....2gZs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f5ea9e66d6ff170_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.849239496118251
Encrypted:	false
SSDEEP:	6:m4Yj018IrAoMMDLMeaSGekPOqYeC0ZzbK6tCF0k5SjsQkOqYeC0:h1tzVDraXiOQ6jjp
MD5:	96602A955C8F81296C4C74AFE8BB1216
SHA1:	EEA0FF3546758FDA4195832C5011F51CDA804E66
SHA-256:	CE3AB2FE4A0702B2C18C3AF59E019D8C6B139289B73CAF82A0906EEF1F12E766
SHA-512:	ADECCAB55C587A6CFDE47033FB10399D4DC901C3BBD283B12C82DA67B29EC6B1D1E6D596679A0C028F7CB75854917DE6DBB8A59F51358258FCB97E1D28291 1C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....=4....._keyhttps://abs.twimg.com/responsive-web/client-web/main.35f93a45.js .https://twitter.com/.V.a.#/.....&.....u.A._.5o.b_f.....z.=...,]..(.A..Eo..... .....A..Eo.....V.a.#/.....EBEDDCF42E2D593AB2596DC45EF722847635D3A41978AEF58C6955E77A49C6BEu.A._.5o.b_f.....z.=...,]..(.A..Eo.....JU..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0fc2865fa5f9f0de_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.378720362412191
Encrypted:	false
SSDEEP:	6:mncYKxDCVA2HSqXGUG31cQMMdyavAdgK6t:xgHAUGGc3f
MD5:	ED64F55C2F1DCFFBE5C6254CC5621346
SHA1:	AC8AECFBC094EFC2B5B22BD0A176E4B28F200660
SHA-256:	0BC7CB08C806FBC9735AA58389010F1CC0A507B9A15E6EBE05F1F8FD547B82FD
SHA-512:	FBC29D5AC359BDAB35BADD0CE003F337351E4E8720EE33097519F9336348484C0284FB91A8071442A280B8C18AC4BCC4D0FC0459947FA91B1CED5B609EAF0D 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D...O.\e...._keyhttps://platform.twitter.com/widgets.js .https://covid19.gov.lv/.x=a.#/.....P..c..4>.G.g.y...+i..8...8W>.A..Eo.....9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\10b3ccc13ac07800_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3137
Entropy (8bit):	5.972530238682304
Encrypted:	false
SSDEEP:	96:qxD2Di8l58HtBmpwi83TSR+KZYMIVWo/c:qw2e8Hrmpwi8jSxok
MD5:	AC99B30EA04AEF8BFF1E58BED057A22B
SHA1:	6981DC8A5CA9B924CE27A7D56873AD1F988B1721
SHA-256:	8F8CBC5B4B49D0ACDC44D0ACA82F1707C24E8C6013079496D42D30EF397CF9C7
SHA-512:	D6B828AF8FE5A66A98DC7345511A7038016B57E95E1E33F1070C0FA7E2F3E46D99F4667CA520B6A90E5254A9817E8AFB1368AB1E8EE086A5D1762F7E44DD3602
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.SignupModule.4264f8a5.js .https://twitter.com/...a.#/.....",.....<W.c.. L.J...l9.Mo... .a.D.....A..Eo.....J.....A..Eo.....a.#/.....'.?.....O.....(S.l..`.....$L`.....QcV..G....window....Q.PJ.f"....webpackJsonp..Qb.....pu sh.....`.....L`.....`.....Ma....6...`.....a.....Qb..3.....sojcC.(S.u..`.....L`>.....Rc@.....M....S...Qb.@&.....r.....Qb.&.....l.....R....Qb.k.@....m.....Qb.g@.....d..... .O...Qb..sh....y.....Qb^.j.....k.....Qbv.....h...k.....`.....Pd.....push.sojc...a....x.....$Qg.....SignupModuleContainer....(S.(..`.....L`.....Q... K`....Dd.....,Rc.....l`....Da.....@.-....\P.a.....O...https://abs.twimg.com/responsive-web/client-web/loader.SignupModule.4264f8a5.js.a.....D`....D`6...D`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\12cca61b18eb1b9e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2928
Entropy (8bit):	5.65301681984428
Encrypted:	false
SSDEEP:	48:JXjzp/Au1qQteH0/oEwF5PHnKBywIsY7dAhVvptF:Jzz9LZteBEwrIJuA7jF
MD5:	70D49C21A34C9CFC3E60FA65214D1BA3
SHA1:	364C30FFC8648999881114EDE5CE35E6D77FE613

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\12cca61b18eb1b9e_0	
SHA-256:	A41BE504ED84C41033577AC903AB13FFCF176E553E5E10AEEA016FDB00C3B598
SHA-512:	71824EC84A366950ECA4CC18084F4DEB3167908C93854275FCFD811EE4F8607D01A3AFAF5C9E748DCF03C9DFF130167C26904537E9B5EF69670B9F46D745F4F7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...8g....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yh/r/y83BxGAqyln.js?_nc_x=lj3Wp8lg5Kz .https://facebook.com/.+<b.#/.....N.....(.:1...vV.....7.v`... .....V..A..Eo.....x..w.....A..Eo.....+<b.#/.@.....'.....O.....(S....`(....DL`.....Qbf.:....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`. .....M`.....Qc:..5....jEC5wxO...Qb.k.d...__d..,Qi.B.....ContextualLayerUpdateOnScroll.....`.....M`.....Qc.B.#....Event....(S.\.`r....$L`.....0Rc.....O.`....I`....Da..... (S.....la....2....8..k%.....d..... ...I.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yh/r/y83BxGAqyln.js?_nc_x=lj3Wp8lg5Kz ...a.....D`....D`V...D`.....`>...&...&....&..A..D&.(S.0..`.....L`.....(S.....Ia.....M.E..q.d.....Qc...W....exports...K`....Df....8.....&.%.-.....(Rc.....I`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1544f8b493f213d6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5835
Entropy (8bit):	6.073954152836843
Encrypted:	false
SSDEEP:	96:B8ssMzYMpyKZsD41B4arJXP8Fv7zQLkxV7fVO66o/D:B8ss6Y5aVP8FTzQLkxVkob
MD5:	B073140B40F68CE82762231BDD69529B
SHA1:	949205851BDAD48F81D59FAF424B5EFA33D1B0D7
SHA-256:	806F9C6881BE142803E7832BEFAC4509559F4B89194C4AFD8D592D1A36AB590C
SHA-512:	7EDD9B3C16A97F9870E07E7CA3AA50C3B37DA71A16038738D0F81A21B603386FFE4E43F89D8054D26C52C007420AA904AFB979450069D262EFBB642BF90914F0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...R.;...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.ExploreSidebar.d117df05.js .https://twitter.com/!..a.#/.....,.....CL[>t...M.$..O....}d. ...F.0.3..3.A..Eo..... .....A..Eo.....'.....O....8...(rE.....(S.l..`.....$L`.....QcV..G....window....Q.PJ.f"....webpackJsonp..Qb.....push .....`.....L`.....`.....Ma....&...`.....a.....Qb..v.....A+RPC.(S....`.....U.L`.....Rct.....2.....Qb.....s.....Qbr.v.....o.....S...Qb.....c.....Qb.f.>....p.....Qb.k.@....m.....R....Qb.C. ,....f.....QbV.q\....T.....Qbr.(.....E.....Qb..sh....y.....Qb.b.;....M.....Qb.....I.....Qb..E.....U.....Qb.....R.....QbZ.z.....D.....Qb...~....B.....Qb.0."....L.....Qb.....N.....Qb.v.... ..J.....Qb:.....Q.....Qb..V.....W.....Qb>s.....X.....Qb.).....z...x.....`.....Pd.....push.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\15dba8d7b656e9c2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	368
Entropy (8bit):	6.016588559315647
Encrypted:	false
SSDEEP:	6:mTbIEYk+f2pomFUzhmJ25uSktm4OjQEalSK6tQOC/j74jQEalq:UUU++amFUzkJjsEEaKitn4EEaU
MD5:	CF0EF074ED1EF2039CAE77BD85B526EF
SHA1:	D021851EC5374838F5288FC27D29B6571D66A30B
SHA-256:	0FA40EC5FBBD1761048D61EABC55D40023DD5C1DBBE88F6073321775AE9EF92D
SHA-512:	475F013861271E4BEC5C006A8E251DDED19A5D5E3BEF1E7CC7073586CB1D22272A253C2CCEA60751F29827D0E118BE9AA79B5C030503300EC07695423817711
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....E.<...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yO/r/RC4Bv8Ta_qo.js?_nc_x=lj3Wp8lg5Kz .https://facebook.com/*,<b.#/.....N.....e..X.... IK5.....?O.Mkm.i.A..Eo.....}`.&.....A..Eo.....*,<b.#/.....C41EB8FFCF6BB6746A4244522405A72D27D103EB67C070CAD0CFB5C2CA246323....e..X.... IK5.....?O.M km.i.A..Eo.....f...L.....

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):	406
Entropy (8bit):	5.465956153799468
Encrypted:	false
SSDEEP:	6:mwh0lXYGL+MIwJJwMT3+9SsSJilxhm4J2K6tWwh0lXYGL+MIwJJwMKHa1/S41xSF:dGIwvY91UDVnGIwvaa9JxUDh
MD5:	B2FF4F13DC51C8A86AA9DD25BD8F33B3
SHA1:	7F596176A23DE9748FB5AC54E25021654A5A7803
SHA-256:	B0177597E4E3C6B2DDC9266581A10A8F85A0795114952A677D8417301FC5BE6D
SHA-512:	BC7B7668588B597F72E819D8DE68AD7E5607BA9AC5C03C6B5B50D0210498A9ACE6524F3886F732214C33C12FF987D129E5C3CACF29401BC7DC6FA949A3BC26A B
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/.m.a.#/.....g-.....:.&..L...jC...1UR@u<$mz.B...u..A..Eo.....Z>.Y.....A..Eo.....0\r..m.....G.....I....._keyhttps://www.google-analytics.com/analytics.js .https://twitter.com/.P.b.#/.....MA.....:.&..L...jC...1UR@u<$mz.B...u..A..Eo.....[..r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17aa24d3b89bc74e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1424
Entropy (8bit):	5.7637154607732715
Encrypted:	false
SSDEEP:	24:znV9LzSnQTBNK/74R5H/UvoX1cnV9LTcm5x0iJT3thv:znSn8NK/74R5MvoODRTDv
MD5:	19974FB4E275D532A47E19C1E573C11A
SHA1:	D3E59B78B7D33D01F75223FC9F66A72177681DFC
SHA-256:	71FADEFA4767A3BE54077D4EDF90AA55FDF3B2DDADFC26149F94CD7868C1979C
SHA-512:	5A439F5998BAD1E385C876281C41800B055D616FE24771FDAFE267120FFF0301A718FAC5CDA7E993EDF12192490DDE220D1F4A227E7A0E4381DF0265B7B8075C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....3...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yu/r/Ht6sBdnumQZ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/P.<b.#/.....yN.....&..b.....5;..F%.....W..v .Hb..&!..A..Eo.....Wb-.....A..Eo.....P.<b.#/.`.....'._.....O.... .....(S.d..`.....(L`.....Qbf.:....self..Q.`F.!....CavalryLogger.....Qc.g.c....start _js....`.....M`.....Qc.,EX....CGkH4FY...Qb.k.d...__d...Qb..4....Rect...`.....M`.....Qdr.....invariant.....Qc.wD<....Vector....Qc..i.....react....(S.T.``.....L`.....8Rc.....O.a$.....I`....Da.....A..(S.....la....H.....A..... ..I.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yu/r/Ht6sBdnumQZ.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`P...D`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17f746c00eb704b7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.484431005744999
Encrypted:	false
SSDEEP:	6:mhXYS66b7E+7QsOJ8FdbC/SZQhLGFeZg4EK6t:YNhbdfOJaC/mQhgeSt
MD5:	8E73E737252CCDD734D4BFCC8A3E59F7
SHA1:	F20B6348CB8A28A397F37C27723CD2B3F2876E93
SHA-256:	001E69892A973176F9E1DE98A260970A53B66771B085F3DDFB0BD1C42B188A83
SHA-512:	EB564515D69B0EA75127B328002A3B4B42240B69C928A09663D6C56046E80588B8641DC7B42761968019264383CFD38DBCE47FDF306162C9046D6CF98C07BD3D
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://ec.europa.eu/info/profiles/multisite_drupal_standard/modules/contrib/field_group/field_group.js?quhwsu .https://europa.eu/4.3`.#/.....|3y*Y|...S..B.R..F`d.k.....|...A..Eo.....W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\198d0a9f12dc9037_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.594150923263841
Encrypted:	false
SSDEEP:	6:mUgVYj018IrAcdQU3MgPHSKml//KFeHJbXP4fbK6t:pgN1tKaP+lX7JuN
MD5:	69BA726E7BC3BB795623E6E1993A5980
SHA1:	3762B6F872F9FEADD158DF0CB4AB60D5103CBBCB
SHA-256:	066C403BBB89C3AE36B5BD0DD06C2585FBD6DABD240A31E94FEF6033F9F93A54
SHA-512:	68D52AB4F5B2A0B56ED5BABD483C8A67D43797D52460CDF741713727FB681C744F5D3F7C6C1DE2103A93A7652DCD8400BC3EE34733F72AB864CB59F4B5A307C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.InlinePlayer.41695835.js .https://twitter.com/i4.a.#/.....A.....2..s..X.....%a..Wu.q ..G.....A..Eo.....Q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1c59a99cbfbec6fa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	362

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1c59a99cbfbec6fa_0	
Entropy (8bit):	5.898575738103566
Encrypted:	false
SSDEEP:	6:mHYj018IrAdGc2xM4d9SeDf7Rrgy/aRK6tMaDmd1RxqfAu7Rrgy/y/:q1tZcwHr7R017ElOD7R0h
MD5:	130C488BBF36AA8EB64B5D638524903C
SHA1:	E8F4E2D4EC6ABF190ED237DE051F6E1FAF71C22B
SHA-256:	7FEB65C340EC5E972DFA347A0A60575C89269E47B2CBDB9AE1CBAA1E23F2276C
SHA-512:	5C21D864133BE9B3E2619DCB1A1A3D85FBC6DF2B42CB76E6CFBA9C2C4B105ACF173B4490DB06C137D183FDFED14832382E51B96866E2A1BFA0F48ACDD745B40
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....._keyhttps://abs.twimg.com/responsive-web/client-web/vendors~main.3bc13d65.js .https://twitter.com/.^.a.#/.....i$.....;...QP.%.1.L.0&..U.!_.;B..4.....A..Eo.....s..z.....A..Eo.....^.a.#/.....31C18C1DC77D3B93B8108BEE26E1B40B56AFE1A0B44B4DE7AD92816ACACE42A6;...QP.%.1.L.0&..U.!_.;B..4.....A..Eo.....$.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1dca5da593a913ed_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.439316614501525
Encrypted:	false
SSDEEP:	3:m+ltEUK8RzYNAgpnRIWaqAKF/uK+6X+9ltlHCoylt8tUoWS6RmVuxpK5kt:mwEwYS6ITqnFd5uHS3ioAVcK6t
MD5:	DC778FD4600D939A34BDE6FAD020A335
SHA1:	17F5304E54614F9DF19FFAA160775F7FF9350C64
SHA-256:	9F7746310735E736B75A752F5F01F5D40B117D1FEFFA5FAB8C1AD2E749E826FD
SHA-512:	85E20027BE3643655F0A01171DAFC303A2CE97E5397D5B3BF90F488384814AB31B0010F148E66B4225D5EC6383A952ACFA191294FD94880F39E16E64D1863E0C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.....]....._keyhttps://ec.europa.eu/info/misc/drupal.js?quhwsu .https://europa.eu/.AV^.#/.....?.D\.7Y. ..o*;..b'.`L,.....6.A..Eo.....t.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f7dde8eb2e4cd3b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8670
Entropy (8bit):	5.886617572907695
Encrypted:	false
SSDEEP:	192:W35tmWlqJ35n7AifgcoJI6Cx3fqkqMTLuA6Tud8E0X6xLW35pJy:G+UJITxybMOYdGOoy
MD5:	86518467A1CD6ABD0BF23F1B50FFF246
SHA1:	E0BCA6FF1C3C3FC6FFB944BEF42A0368BA9D307F
SHA-256:	AE7EE42C4E97FAADDB4BDCCDEB331AF6C4FE7AE5F28F6ABA90D668029037E591
SHA-512:	CCE7B30D9A52B5AAAE9D320564A14542DDB1083BB654B7B0355E5A45B18B8C42072F421FEAC0A14FE3ACBA5E588ABE28B083F93FDB5CD62DB50EA2D89BC0E0ED
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Vg....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~loader.AudioOnlyVideoPlayer~ondemand.InlinePlayer.14e4b0c5.js .https://twitter.com/.D.a.#/.....(.....(.....D6.....>tBs.A..Eo.....q..1.....A..Eo.....'.....O....(.....(S.....`.....9.L`.....QcV..G....window....Q.PJ.f"....webpackJsonp..Qb.....push.....`.....L`.....`.....Ma.....`.....1...a.....Qb6.....+/OBC..Qb..M....+oxZC..Qb.F.....1PcyC..Qb..&.....1t7PC..Qb..).....4D4FC`.-..C..Qb..XN....695JC..Qb.....6OViC..QbR.....7lg/C..Qb^$.u....7x/CC..Qbb*.....HS6iC..Qb>.....HT/6C..QbZ.#.....JDXiC..Qb..g4....JtPfC..Qb.....Qi22C..Qb.....QroTC..QbBl.....TkGIC..Qb.....UmhLC..Qb..#.....W/KdC..Qb..^....XmKVC..QbJ.C.....Xq8BC..QbZc.....aLgoC..Qb../5....aokAC..Qb.....cAROC..Qb.....hBpGC..Qb.A.....hXPaC..Qb..-.....ho0zC..QbNJl.....jHwrC..Qb&..q....jQ/yC..Qb..F.....jwueC..Qb.K.....kH1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\200b9c01d20a8da1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.398203686297011
Encrypted:	false
SSDEEP:	6:mml/lXYS6WbBluKe0eCWzr8FdfpdI9SfeNYH4/9FDK6t:ZjRuKve7MXnYHKF1
MD5:	9013105F4FB9CDA0CE827B0152F87611
SHA1:	C5A29F3CFBC56B7E5E77BBE18F1B5737905D3C91
SHA-256:	134BBECA5540A77563E353A468AF23B618EE6AA492C0EAAE489896C47D7E9C67
SHA-512:	AD36B319E555FA00AB5E472AEFDDA55C42906CB2819AC5A79F6E5AC8F2C3CED87CF0DADF0711AA9200FFC558F4056302CFEB4602FC98AA93E6712679F70A5E56

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\200b9c01d20a8da1_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x..._..u...._keyhttps://ec.europa.eu/info/sites/default/themes/europa/js/libraries/modernizr/modernizr.js?quhwsu .https://europa.eu/.Q`.#/.....:.....?K..dK*..j..B...\Y..d\..X..|.d..A..Eo.....|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2101f9463a2591a1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	263
Entropy (8bit):	5.916848373732872
Encrypted:	false
SSDEEP:	6:mc4YsMb4MJjjdTimDFNrMb4MJbYSRQ95saZhzrrXlZK6t:xhbvJjhTHD3obvJbYCiJh71
MD5:	623DD66C0C3674864959BE7843B97CE2
SHA1:	4021B78F0D88AC09C0FD19DD74EE94195CC320B7
SHA-256:	B23CDA713F466FDFE3E98FB9DBAB4A5AAD16F7A345D2DDCF9AF9BC5FC0ECC704
SHA-512:	F90A2B23D2A007D36C8B1730C7EA292FE4AD99EFA82195EDF4AB5775D61A0E5C3EE22E7981D089F03CA8D27986AE85263AAA8236D1E19F7CB771DB4CFAC5A3A0
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://covid19sertifikats.lv/html5-qrcode.min.js?v=Vv6Q2UD-WGc9DYgKpBD7Tc2_Q3-TOd11T6_WM_Lv6os .https://covid19sertifikats.lv/.].].#/.....Q.....y.....&..=.7..@.A..Eo.....G.2.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\21d3159125f29fa5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.6719902677602025
Encrypted:	false
SSDEEP:	6:mIyYEDLBHEuXhM66il5VhMOZEMt57pJbK6dk0Wd8VEaSz7QayYfXhK6t:PODLbRuWB6KK6dk0WdNaK0ay07
MD5:	E2DDFA8D3F2B6F90A7B16DE611CCC98D
SHA1:	7A7C1053C5AE8492916043943E75018587B07AA9
SHA-256:	355933B53AC6EBAA284F3B04DAAE75B8F431B147E3F27FCC0B5D4C15DE0333E1
SHA-512:	B5D0FE4E47F45F1CB5D6F5941A93FE6E23730A55FCEDD641107AF01657E59884EBFEC4750653ADEC5E75D6BB26D9F5889427B43F71B07EBBAF0C8ED8E81E799
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Zq."...._keyhttps://cdn.syndication.twimg.com/timeline/profile?callback=__twttr.callbacks.tl_i0_profile_Brivibas36_old&dnt=false&domain=covid19.gov.lv&lang=en&screen_name=Brivibas36&suppress_response_codes=true&t=1803843&tweet_limit=1&tz=GMT-0700&with_replies=false .https://covid19.gov.lv/.NWa.#/.....p.....X..-V".#.k.....D.....A..Eo.....Qw/.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\224fb90ee15e7c6f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	190
Entropy (8bit):	5.2847376478034
Encrypted:	false
SSDEEP:	3:m+lzI8RzYXK+MEEkVDSK+KF+/tlHCQn/tGIea+vt8W0JWbH5mX7lXpK5kt:m0xYahEEs/g/SQUIea+F8Wz4XK6t
MD5:	D40B65DAD94429418E2FE9632E6C9F06
SHA1:	B7F7062F6175494CA214866708E04E3C11B0D8D2
SHA-256:	E0A68A881065AFDA068C9D36ABA2875042BACB91BB724D23857384511EE217C5
SHA-512:	1045AFCB050C2E71AB5A8EF02F317924CD0EBC51CEA4BB4E0089392FCD9E1643572CDB4545720F9717C81600027C1E5EE6BAB5A26150492628D4917F03483CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....nFt...._keyhttps://europa.eu/webtools/load.js .https://europa.eu/qA^`.#/.....*.8.p....h...P...lm....U../.A..Eo.....r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22addbc23903a81b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	31000

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22addbc23903a81b_0	
Entropy (8bit):	5.720647422869587
Encrypted:	false
SSDEEP:	768:DG1umAL/ElQeHyX7QaOgZqVsFedWSmiXVglk:Do8LMlfyX7QXQqWGWDMVglk
MD5:	BEB9B4C300C1B2BE768C2459261637A7
SHA1:	9EDB1D42F7C0F9788918FD8325683F2333010451
SHA-256:	B57D92A918775BCA23666D19EA9E0DE5377E4BDD9E7E62BD4E3FD048886AF5B8
SHA-512:	DD5A87112A4D649F7BBF79C447D5A4959A48A147F5A71F25AFE4276FA079EA077CFC49522B43B0C2924AC4A309D5B61E3CF70CA694A3E9C6592C11D9D5A1F4E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....I@...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y9/r/gopL_q52WxU.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/ f;b.#/.....N.....q...xD.;.p.....@.:.....A..Eo.....:W.....A..Eo.....'.o....O....pw...j=.....\.....(S.....`.....L`.....Qbf.:....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`.....M`.....Qcvx.....9hir0TX...Qb.k.d...__d...Qc*..Y....BlueBar...`.....M`.....Qb.$R.....csx...Qb.4.....CSS...Qc>..{....DOMQuery..Qcz$^.....Style.....Qb.D.....ge...(S...`.....LL`"....XRc(.....O...Qb.h.....h.....S...Qb2T.....j.....Qb.|.B....k.....Qb~.....l...e.....I`....Da....P....(S.....Ia....D.....&...%.@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/y9/r/gopL_q52WxU.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`6...D`.....`....&...&... &..a'&.(S...IaN...o.....&...A(d.....&.(S.....Iay.....M

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\23a82d235106f889_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	28288
Entropy (8bit):	5.895502752406235
Encrypted:	false
SSDEEP:	384:qam4aLlnCSrmARxani+A2Cr2JunhPDyE0HFPNx+oab48gum2F72791wUt:qaHaLcSr0YJhPDyJHR+v667+Z
MD5:	60413F7D29DE5E0B4942C9890716025F
SHA1:	9D0EAB02BC4C4D49F49E77339FB921D43A7E6217
SHA-256:	C65CE34379DAA21F6530A33D8DBF47DE3D5640A3DBC4364F67AC4B4C24D100FC
SHA-512:	D9C353FEDA21D442C33C3288B83EF6BA95BBFBDF232C97320B98269A8DB3ED4D9A74EFEFA00E8423CDE01057430DCF2D7144E1D61A8759104AED47214489602
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y5/r/eFb43EGq1Fw.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..<b.#/.....N.....z..m|.N..0. ..Z ..p....1...o....A..Eo.....q.....A..Eo.....'..~....O....l..J4.....(S.1...`.....L`l.....Qbf.:....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`.....M`.....Qc.....KUDPaun...Qb.k.d...__d..$Qg..:.....EventListenerImplForBlue...`.....M`.....Qc.B.#....Event.....Q.P^.(.....TimeSlice.....Q.`..n....emptyFunction....,Qirn.....setImmediateAcrossTransitions....(S.x.`.....HL` ....8Rc.....O.....a.....I`....Da`.....(S.....Ia.....d.....(.....a..@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/y5/r/eFb43EGq1Fw.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`<...D`.....`....&...&....&..A.D&.(S.....Pc.....a.listena.....Qc.....listen.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2639ca97b799905d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.426849574085587
Encrypted:	false
SSDEEP:	6:mfxYS6WbBluKe0k0FVOFd09S5/Cog0eGWCBY1NK6t:IfRuKvNN9gpYGWC0
MD5:	02EE79EC6A8E63C96FA94D214EF42DCC
SHA1:	C611C7BC91C646E6FA6999C237CB244AD6560C39
SHA-256:	B348849F7721E5142548A2B94C722F332C0FE536545C7D9C2EDF02092D888A24
SHA-512:	7F7259B0737F44ABB03E27B5095C9D208BB78019E6ED5A49AEADEA6373838ED6419BAF8A62080DEB2D605A39F390FE3CFC19A51CCD2DF18E5728C7D4B9E912A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...{4#....._keyhttps://ec.europa.eu/info/sites/default/themes/europa/js/libraries/superclamp.min.js?quhwsu .https://europa.eu/i0U`.#/.....k.....Q.'.B.*..a.@....G...9.X..A..Eo.....4ln|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\27895adf9dae3241_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.501091846312497
Encrypted:	false
SSDEEP:	6:mdYSAsJXyNIRKK/S/cLZ+85smnNthK6t:2X+Iv7Lz5smN1
MD5:	8774335C0B570009993AA000F76B6414
SHA1:	7EB8FFE3BAC385C448DE0A1F06AE06B8F9CE8D96

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\27895adf9dae3241_0	
SHA-256:	13944B361E063C05B553AA5FFF5DE34AB94B5B92124381F45CAFD610A6FFCB2C
SHA-512:	79470F24A8AB8FB305F3621ACD900AF470F3C19457707996047076A9B4EAB4FE656DD058D46E27FC1B08F8C0EEC979BF13B3BAF93C421771F668C358801192E9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....5....._keyhttps://ec.europa.eu/wel/surveys/wr_survey03/js/main.js?901921 .https://europa.eu/..^`.#/.....f....._.\....OC#&`N.....o.h+....b.A..Eo.....:..M.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\29cd2bd1b35b5ae3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	253
Entropy (8bit):	5.392875932197041
Encrypted:	false
SSDEEP:	6:mGnYS6WbBluKXwxE1M7LEhFde1/SVGc/419prFbK6t:pRuKgtr/mGTp
MD5:	C3173FBED07B42821715CECE2E932107
SHA1:	58713071EC1AD823F3BFE6781C858AE28E9D8022
SHA-256:	8092BDD7ED778BBE0B6CB7310149B0D190FA96A5EF611059B9E45F3A464C244A
SHA-512:	889A96BCBD1C2D4C06F06C602C9A9B0CDE391ADB19CEC05A5CA9C3359152940E9E9F8D2F612F0625107CC258FEE7EA2F371A480A8CDF4AF420DF0659F6B04F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....y....;....._keyhttps://ec.europa.eu/info/sites/default/themes/europa/bootstrap-sass/js/bootstrap/affix.js?quhwsu .https://europa.eu/..3`.#/.....TI.cj {k.&.b..N...EY....T.e..A..Eo.....u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c1fae70c6ffc0a0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4503
Entropy (8bit):	5.697230152617131
Encrypted:	false
SSDEEP:	96:4XUOw/W6xi/T3MQld6ROJLYRfVMlBmZeAqcVor9nktAl/f9Sq:4EOWJkTvb6IJ4/dqcVor9ktgF
MD5:	526085EEAF11846D3063EB1B365D5CAA
SHA1:	2A76C0A6B85D7D256CE3F8F5EB878165E0F9FB3C
SHA-256:	26AE058AF2562343D9EA92EE3207D6EA4467C12DE06463E3B9C0F446C8A3414F
SHA-512:	2D43D7939F4BD60943246F901CD7973F44C574068D109EE0144A4F2F6AB6A4722F818654A08E4C9E784EF54FA634858AAE308F17496DADCA620ED7B8017F7733
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...*.p6...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.WideLayout.57be7e65.js .https://twitter.com/..a.#/.....o).....;lm.U..dt.....n3..b...;.R H.0.?.A..Eo.....z,.....A..Eo.....'..C....O.....k.>.....(.....(S...`....dL`.....QcV..G....window....Q.PJ.f"....webpackJsonp..Qb.....push..... `.....L`.....`.....Mb....>...\...`.....T..a&.....Qb2.....0af8C..Qb.(.....LHcrC..Qb2,.....Xs4YC..Qb.....fyKlC..Qb.R.....hqDbC..QbNJl.....jHwrC..Qbb.z.....lP98C..Qb.5p. ....sAnOC..Qb...E....uo3SC.(S.y..`.....L`B....pRc4.....Qbr.v.....o.....Qb:..Y....n.....Qb.@&.....r.....Qb.....c.....Qb.&.....l.....Qbv.....h.....Qb.f.>....p.....R....Qb.k.@....m...h... .....`.....Pd.....push.0af8...a.....1...Qb.g@.....d....(QhB..y....roundToNearestDevicePixel....(S.(.`.....L`.....1...K`....Dd.....,Rc.....l`. ...Da*...B.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3080ea2e3fae4ee4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	255
Entropy (8bit):	5.46202601228664
Encrypted:	false
SSDEEP:	6:mdnYS6WbBluKe0UoGmAVOFd+Sv+n3nLa9P4+K6t:mRuKvUoGXVltXLi
MD5:	2F57B15AD5DCB5114274E7ADC9D1AEE4
SHA1:	8DC2BDBD562D28416104AFC8A2D5E2FDF121BCC8
SHA-256:	568D3B681EACCD5E61DBF5DA6D2260FE10A3233AAB5ED711EE85019E7245A013
SHA-512:	58E5183253533DC79E0C4EF2B11DAF27FE6456601ABC77B2369A4A7B91F1BBEB9F3356970433F177FD611378EF883629CC99A1A0C54119AB560A0473C675322F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{....._keyhttps://ec.europa.eu/info/sites/default/themes/europa/js/libraries/jquery.tablesorter.min.js?quhwsu .https://europa.eu/GpU`.#/.....w&. O.5....g...!.R.H.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\32ab71042485bf4d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	39779
Entropy (8bit):	5.808176673768389
Encrypted:	false
SSDEEP:	384:tSgMWWM3BclJt1Jt/lHjPyRPSnhmKEzpl0k+iOHc8WznnpakvanDhtrgnmGmVQVj:tSgcMRc3JRpEP1GdYknhtgnmG/VpxdlD
MD5:	BA0C32DBFDB81F003068F47D5951D104
SHA1:	5E64343273CD244CED303BF93B07D26DB1B5DDE0
SHA-256:	0D02D1A37C437A751527C4414857E9EF4FA5357C18AC457E8E554306D2B28C6C
SHA-512:	986200F3E0D98CDC0D223EE697551C2DCD0258AA13B727EE6BFAE4871E83EC48E2F9BA63C33C11E7B8FCCA1F5B58E2E5AC68FD0365B203433D3717243FBDAF DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....B....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iNtm4/ys/l/de_DE/Es7qkeXt043.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/(.<b.#/.....N.....sU^. .Od.?.cz[.....a...n.....A..Eo.....A..Eo.....'.....O.....f.....$.....D.....(S....`.....L`.....Qbf.:....self..Q.`F.! ....CavalryLogger.....Qc.g.c....start_js.....`.....M`.....QcB.....GyUDUir...Qb.k.d...__d..,Qi"... ...DesktopHscrollUnitEventConstants.(S.l.`.....@L`.....,Qi.b.K....DesktopHScr ollUnit/itemInserted..(Qh.....HSCROLL_ITEM_INSERTED_EVENT..(Qh..n.....DesktopHScrollUnit/itemShown.$Qg.....HSCROLL_ITEM_SHOWN_EVENT.4Qk R..n%...DesktopHScrollUnit/HideIndividualItem....$Qg...#....HSCROLL_ITEM_HIDE_EVENT..4QkJlt&'...DesktopHScrollUnit/scrollItemBeforeXout..4Qk...Y%...HS CROLL_ITEM_SCROLL_BEFORE_XOUT_EVENT....4QkR..'...DesktopHScrollUnit/unhideIndividualItem..(Qh.Bt.....HSCROLL_ITEM_UNHIDE_E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\32dcc24461d36fa8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.638023395842707
Encrypted:	false
SSDEEP:	6:mLYMGpAlv1EqgByFGmdv/SC/p/J5EyAd5RK6t:OYJveyFF9fJ5Ey4p
MD5:	4015004B17B4B756D14F55D408A6737D
SHA1:	1A99E38FE50A24F17B606969EAAA26EA9BED54E9
SHA-256:	5507EAC28E792B1948C6BA0F9A8E51FF0635191D16A0DD981177EE025BC6AFC3
SHA-512:	E91BB28C20B145E5192BA3A309D82BB5ADE8E92F642DB242A7FDE7567AF5ED09C1ABB46016E4E2DE759C4139EC36356BD0E6C6B542308C8D3664C049407A1C 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....._keyhttps://manavakcina.lv/vendors~index~sess_head.mv.84b7e3c4c2ad458fafc8.js .https://manavakcina.lv/X..`.#/.....\..b.+...VE..!.3.8..c|J.I O.A..Eo.....W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\33159ea472ac0131_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	263
Entropy (8bit):	5.483826928603313
Encrypted:	false
SSDEEP:	6:mc/KYS6WbBst2nQ4F4J8FdZu9SwlKSJvZZGqzFqT7lZK6t:xl+f4F4JhZlQ6vLFahT
MD5:	BF156BBA8943DD6240E0FC07CCC9FBF4
SHA1:	E38F165A3DEAAD536C78084986EA68DA471748F4
SHA-256:	1A76CB424C86744C659183E9B44273CA69AD8AB61A402F430246085AA07F5B91
SHA-512:	0C9BBAFFCF516E66BFEB1165AC06809727A0611B3AA6C2CE779D5C460C187FF969BBCFB97E0ED901CD31F708F43D25EE534B66706AD6592271051AD2B5F4A0 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K...._keyhttps://ec.europa.eu/info/sites/default/modules/custom/dt_policy_next_step/js/dt_policy_next_step.js?quhwsu .https://europa.eu/_.W^.#/..... .....,..2..w..:...=... ..(..A..Eo.....V..2.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\34ca62021a4336ae_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.524892007719901
Encrypted:	false
SSDEEP:	6:m9eYS6WbBstK7AuHWAJLLPdTcu9SEl7CqqTwnzWuhK6t:i8+KTHhLLPdTJhF2wzf7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\34ca62021a4336ae_0	
MD5:	C2268D37F5A8652376182C4B56654E81
SHA1:	F8F0FB1EBC52C51EF8A4DD694967CF2FEFA6EBDA
SHA-256:	06CEF93A11AFDD53C94E9AFA169EA85C7F21E9C3517677F30E2DD7A1EBEB3306
SHA-512:	A301551523E41C27F29DE713401378F64BE247120FC0CE14004A778A5937BCCC9B647B5202408E9576DCC881715E6206D1A925E409E0848EECC388A8143E7F91
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://ec.europa.eu/info/sites/default/modules/contrib/picture/picturefill2/picturefill.min.js?v=2.3.1 .https://europa.eu/.eX`.#/.....w.....9.'..|..|k.O.W...n.Q....~.@..A..Eo.....sC.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\36fb163aa6cbb4a4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	293
Entropy (8bit):	5.635385525394118
Encrypted:	false
SSDEEP:	6:mSQVYj018IrAMUJABIHy6JABIHLQaxM09Ssn599oMgrttK6t:81thULDLLtZhgV
MD5:	75DB7F308C8DB03A73806F41F20B962A
SHA1:	43072530FE453F93511737592F96C416C901DE53
SHA-256:	D9E891873E02A9510B1F03FB076924F657D93B0DA9399C46E73D3BF9FB889505
SHA-512:	23E775DF5B3146201C6FA25C948083EC36191988EEB216AC7F19B737931086DE0560CA409EC52301A125B5F6113834B1557332C0CD2709A5C309F5C76A5578D3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~loaders.video.VideoPlayerDefaultUI~loaders.video.VideoPlayerEventsUI.5aa20a85.js .https://twitter.com/.6.a.#/.....A.....#.....V.|.DWN?w....@8T...A..Eo.....(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3b94c0b176757e41_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.565936337624388
Encrypted:	false
SSDEEP:	6:mDlllXYMGbNpEqgByFGr/SEv7ZYGnrUAho7DK6t:IlllTvyF45v7ZnwX71
MD5:	B86A9DC4259E02F7EC650F5843BC0B5D
SHA1:	DDB77F1735B9D2BA338FB950275AF541F78E8660
SHA-256:	FF62B38B118223888E682CCACF70DFB383FC0ABEAB2CB6729F6E96369E1E5AC6
SHA-512:	151A24538BF9698593331B1816BB5C45650B085E96AFA58650F50966170D803B97DADCF718E7B309D940683A984FCE3F88B7A41074ED707C144B37186D0458BB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....F....._keyhttps://manavakcina.lv/index.mv.84b7e3c4c2ad458fafc8.js .https://manavakcina.lv/...`.#/.....%.....5.{)...Z.fd..|..a..&@G.p...C....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3d276c1aa48e65e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.43894328220253
Encrypted:	false
SSDEEP:	6:mpXXYSAsJXyNymU2R9Q1/SSl0C4KMG4rC7DK6t:0dX+ymtQ1/z0C4KMG4i1
MD5:	8DE1550DC9403746AB6225AD63A36C99
SHA1:	C3D8A4E4EB34546E339BC2AE606A26C9BD57BC9B
SHA-256:	49AE4518DFA860B42601A48FCB356ACF892DFD508F1DFA0F81E1B8E6DA953F87
SHA-512:	FEAD7CE430E131A05E7601410C6E5261B3927F835E56580AF7857C1BE15419B9A034EC5A5F42DAAFF3D92B0CE9E5A76106CCDE2EF3290082048E52C911ABA67A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i...r.K....._keyhttps://ec.europa.eu/wel/surveys/wr_survey03/data/survey_url_rules.js?901921v0.63 .https://europa.eu/.fq`.#/.....h....1..M....f..!).cS%15s!.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3dcda6d0f84e2227_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3dcda6d0f84e2227_0	
File Type:	data
Category:	dropped
Size (bytes):	265
Entropy (8bit):	5.534088319454843
Encrypted:	false
SSDEEP:	6:mvQvnYS66b7E+7ANcFdloSImpz4JmbK6t:9lhbdE5FmpumN
MD5:	B5284348023AC5322C8613FB108EE829
SHA1:	D4B5F4F59E7BA12F9DA087ED1CF82FC5CE0E189B
SHA-256:	DD2908FB5EFEA5D30D9831211B6FA567C7A19C0625DC393282A88D3B1F9AD738
SHA-512:	9830BA556F2533DB927A3EFD8239C0BA2EC2CD9765639F5B950CF975FF6163AE583AB7E3DA7D769CDDC92303414683B4A76CF76F79A18D386620BA49C564DAD
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://ec.europa.eu/info/profiles/multisite_drupal_standard/modules/contrib/maxlength/js/maxlength.js?quhwsu .https://europa.eu/..&`.#/..... .....3..t6..V-..>z..a..f…6...A..Eo.....9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4013015a0d27ebb0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8758
Entropy (8bit):	6.021517906256377
Encrypted:	false
SSDEEP:	192:m3lsoA/qSU+xP/pkmxsMR1saON3oFiRfU6ac2xor:RCG3xvR6aON3h26Qxw
MD5:	AC3FC63A37998ED39E6A9B33AC4E1197
SHA1:	5B821A7DC18EEDA832505A341C5E0DA9029B9D13
SHA-256:	952391D530D606A95DEA273B69DAEADE7B3874FA5D6E267D7CEAC9600D683B22
SHA-512:	1DB72492A16DDA1BB8CE1224730B4F2F7BB76E2F4F85C145EFCFB51244F7018A921CEA0D9CB85EDE5534D46488E98CCD00E49782C96A39A1FBCE2387FC25DE 96
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n.....s....._keyhttps://abs.twimg.com/responsive-web/client-web/bundle.NetworkInstrument.95d70595.js .https://twitter.com/.a.#/.....X(.....sO.i.t.m.....U...0. '.SK...&....A..Eo.....I.~.....A..Eo.....'.u.....O..... .. gW.....(S.l..`.....$L`.....QcV..G....window....Q.PJ.f"....webpackJsonp..Qb.....pus h.....`.....L`.....`.....Ma....p...`.....a.....Qb..f.....ujfhC.(S....`.....L`L....hRc0.....S...Qb.....s.....M...QbJ+M ...._.....R....Qb.....c.....Qb.k.@....m.....Qb.g@.....d...g. .....`.....Pd.....push.ujfh...a.....5....Qb.@&.....r.....a..(S.(..`.....L`.....K`....Dd.....,Rc.....I`....Da.....Q.....@.-....`P.q.....T...https://ab s.twimg.com/responsive-web/client-web/bundle.NetworkInstrument.95d70595.jsa.....D`....D`,...D`.....`>...&...&..1.&....&.(S....`8....|L`:....8Rc.....a....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4025b4b73fe5b130_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	274056
Entropy (8bit):	6.122283127167956
Encrypted:	false
SSDEEP:	6144:SpcY6ZlRPjm6RwlMEiuboeHnamm/gCrQQI9I3k8Cw1mFBC8:nrRPjm6um1gXHnmoCr3I9V8CwcBC8
MD5:	198FB24B7654CFCFE4C7864D4D6B5532
SHA1:	40411562AB2457A48C45DC1058B9B0CFDBB7F800
SHA-256:	B4122FCC9DC5B809B08C5C264A5EA222621677E860ECDAB43DECF14BAEB9FF8F
SHA-512:	BE91BF2A3B6C2909C95907043155CBC81EA116AC8A447B1DBC5B06E1CD0D9982B00CFA75ED463FB22372B04D8DEEE5E09A980BC1EE35C05773C9C88806FDB FB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....E.....2560088F8E6EAEDA5F7EC125D2EDB3AAD18F09CFE35C0CAB8FF9914852BFD96C.....'.e.....O9....,.....%.....t....-..Do..... .....d.....(S.l..`.....$L`.....QcV..G....window....Q.PJ.f".. ..webpackJsonp..Qb.....push.....`.....L`.....`.....Ma.....`.....a.....Qb.....oFUsC.(S....-..`.Z.....EoL`.7.....Qb.r.....3XMw..Qd...H...._register.....Qb.....en....Qc:.]J....i5 06b71f..Qe."....Smileys & people..Qc.2.^....f457f731..Qe..tm....Animals & nature..Qc.....ce9bf9a3..Qd..J.....Food & drink..Qc.....da1e1fd1..Qc..Q[....Activity..Qc... ....g280553b..Qe.....Travel & places...Qcj..%....b2f95aa6..QcJH.....Objects...Qc&.....ac91750d..Qc.....Symbols...QcN.....j56c4be0..Qc.....Flags.....Qc.9n....ef15e12a. .Qez|.T....Grinning face.....Qc.s

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\431aad649edaa8c5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	108768
Entropy (8bit):	5.795318682452029
Encrypted:	false
SSDEEP:	1536:lsoiKb++CA3VKN6CWdaLV97z5F+7pprAA71RCLwZKwsi/mmyQNNAt6QbU:4KM/6CW4P7+7ppxCLwl/FhNNPQbU

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\431aad649edaa8c5_0	
MD5:	D8225F097C62FEE213D709459064B8C5
SHA1:	CD2F969FE2AAE5041FEBB20000E901D1074566E2
SHA-256:	50ABE84B4FE9B41995F8D22B736F8FF1F3BFC7EB766F713F5FD498992CEFDE97
SHA-512:	1A00C22F0025C47D8B9509CB64DEB8EF8CFAD3237A416356CBA588D96EC3D3C6D9405B430928281EFB6319840E916D0CCF4E4DA5211B5EFAFD10585D46F5EA0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....|....AB8D546F4FC8E49AC752D97F853CE49F4EFF16B329BCC1017C3877EE083EC38D.....'..r....O%...x....#Zf.....T...$%.....p.....(S.<..`4.....L`.....L`.....Qb.....site.(S....`.....L`.....XRc(.....Qbv(.C....e.....QbF.D.....n.....Qb.....r.....S...Qb...7....o.....M.e.....I`....Da"...6.....Qc.....window.....Qb.....self.(S.P.`\.....L`.....4Rc.....Qb"t.h....t...`$...I`....Da....b.....(S.P.`Z.....L`.....4Rc.....Q.`....I`....Da.....Qc...]....document.(S.....Pd.....t.exports...a....s...I..1..@.-....hP.....Y...https://covid19sertifikats.lv/bundle.min.js?v=RBChujdmhIDI2ZMrjLlOGNm9q6GEDofzToHYAUIP14U...a.....D`....D`....D`.....-....`....&...&..Q.&....&....&..Q.&.(S...%%..`.J.....L`.....Rcf.....*.....Q.....S.....M...Qb.;sL...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4811123599279275_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	198
Entropy (8bit):	5.399083042544323
Encrypted:	false
SSDEEP:	6:mSr9Y6LvMmmJC/SxoYzmAX7XVyAJthK6t:3HMGObt7
MD5:	0C85171585E534BD2365383C009C5FD7
SHA1:	4D10C02DAB1D311C8B35C0E7C9CC579A16C82C3E
SHA-256:	63FDD32F1DAAC4F5C604A10CEA25C95FD3919D858235C67A3BA46147ED13049A
SHA-512:	46F7165EBC8E200FB6A783A04EF47C4EEE7A326A0CE42A0FAF4B8571C4518A07CCF6DAD9E214C9AB8A5868139691457203D6CA3CAC61FB6B12360D5F9BB3E1F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B....._keyhttps://webanalytics.ec.europa.eu/piwik.js .https://europa.eu/^.l`.#/.....k....L>o.N.FV.,.W>.a.Z.Ho.....A..Eo.....b.G.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\49c1c240256d653f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	108768
Entropy (8bit):	5.795160646864887
Encrypted:	false
SSDEEP:	1536:2ueyWM+FlXDSP8+cOWxpnxFAo4vyCrOPdgqVHDsbA9O/mmyQNNAt6x6:lWfKcOWrLb4vyCy3BQA0/FhNNPx6
MD5:	E3A193E49F0937366298F98674D0C087
SHA1:	96269CCF0A2727E240C2734287DC44FA2F3B1294
SHA-256:	A847F48DB707548367F9428BC01E6777EB892690CE7D60667516CC0724EAC8EC
SHA-512:	F0E92DC99BD6E2BAB92E484D4F6C649D16D08AD21ABDE4D052308F23A4CE83B38CA63E76F182928417AB37DD2877E7F6B3F4C20A23102F08449FA21C96C42D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....Q....C7F3051FFD45A5512CAA052796A852DCF8D7BDEA5E220E7C498CD8A223278622.....'..r....O%...x...<2.x.....T...$%.....p.....(S.<..`4.....L`.....L`.....Qb..#&....site.(S....`.....L`.....XRc(.....Qb...>....e.....Qb*..@....n.....Qb&i.....r.....S...Qb.....o.....M.e.....I`....Da"...6.....QcF(W.....window.....Qb..5.....self.(S.P.`\.....L`.....4Rc.....QbJM.....t...`$...I`....Da....b.....(S.P.`Z.....L`.....4Rc.....Q.`....I`....Da.....Qc.QU.....document.(S.....Pd.....t.exports...a....s...I..1..@.-....hP.....Y...https://covid19sertifikats.lv/bundle.min.js?v=RBChujdmhIDI2ZMrjLlOGNm9q6GEDofzToHYAUIP14U...a.....D`....D`....D`.....-....`....&...&..Q.&....&....&..Q.&.(S...%%..`.J.....L`.....Rcf.....*.....Q.....S.....M...Qb..jT...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4b1836cb98b878d6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.494400561452344
Encrypted:	false
SSDEEP:	6:mTXYS6IdU7lFI6/SollwskyZxwfa/hK6t:yNj27Z/xleaxqa/7
MD5:	89F27FD1C47D5B50EF7AF0F10C53B525
SHA1:	E103117C0A63DFEB656DB1294A4D722F5BF804AC
SHA-256:	A75A23EE76071D4EC1C9A6969B62C7EFE2F5B347F0DBEC107D98446DDBEE4460
SHA-512:	99EF736A22C60B2EED23B53180455FA10097224B66BEBAF9496CAEAC9C7B616FE4E7079D8A13164736A9D497F5408634497F74C12E7E4775B80718DF81CA3CDA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4b1836cb98b878d6_0	
Preview:	0\r..m.....K....MG....._keyhttps://ec.europa.eu/info/misc/jquery.once.js?v=1.2 .https://europa.eu/.P^.#/.....J.s.tm.....m..&.....\.....A..Eo.....VH.....A..Eo.. .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4bd0fc397a7eeacb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2744
Entropy (8bit):	5.479617805050698
Encrypted:	false
SSDEEP:	48:KLclgrq2dLnf+cE6Xvzf608Uu/5k3Y/fb6fvGWcnxGPZU2hE7:KLcO9nf+l6Xvzf608Uyk3Y/fb6fvkxKU
MD5:	26AED84C32A847FF69055B2E4D291981
SHA1:	670B00435D75845E7621B2FCE7EA949D92794CE5
SHA-256:	03FE4BA4B0C8B43496CABCC6325C64187C8AC404B9986123EA2918D930CE60AB
SHA-512:	5055F600B26DF86DD04B695F01C97D85880F71D747ABBA375EBC01F6FBC957BA06BA0CCCDFAF8F30E7738F6215A1C16422FA1CDD70F59B4CBB01D7A0E57A0F DC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....R...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y6/r/zECeJUINBB_.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..<b.#/.....mN.....&wnO.W....k..P.....$ I...Z.A..Eo.....T.....A..Eo.....<b.#/.....'.....O....H...r.%.....(S....`.....`L`,.....Qbf.:.....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`... ...M`.....Qc.L.....o1FBg2a...Qb.k.d...__d...Qe. .....isKeyActivation....`.....M`.....Qb..%.....Keys.(S.<.`.....L`.....0Rc.....O.`...I`....Da....>....(S.....Ia.....M.....@.- ....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/y6/r/zECeJUINBB_.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`H...D`.....@...`....&...&....&....&.(S.<..`.....L`.....0Rc..... ..O.`....I`....Da.....(S.....Ia....}.....M.....q.d.....@.....Qc...W....exports...K`....Di....8.....%.....&.%.-.....b.....d.....@..@.....&....&.(S.@.`6..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4dc3e20f821a6ca1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	5.439720650272659
Encrypted:	false
SSDEEP:	6:m6XYS6WbBluKXwxE1M7LEWFdh9SHI1Upkengm4HnK6t:1RuKgt9b6kenVe
MD5:	8E38D078D075466CD673B9A1FF2FF240
SHA1:	16CA54BCDC31C241E33CE3F5F735026A9108B2A0
SHA-256:	FC1361B22FF9D3A3237171185985C7F596850EB5B860284D5B4F2E449C65CBC4
SHA-512:	C98CA1E97402EA71F0CFD93C83BB831A31714A10EC955199241E9B31B90C7AD11658E707D2CDC97C851F04D378C17A5CAA90EC1CCE6B8B955F455D02EC8EC A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|....._keyhttps://ec.europa.eu/info/sites/default/themes/europa/bootstrap-sass/js/bootstrap/collapse.js?quhwsu .https://europa.eu/..O`.#/.....s.... .H....=>n.....]..;..d.....A..Eo.....6!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\573fbbcbd3c96c27_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.48447398490023
Encrypted:	false
SSDEEP:	6:msbWXYMGBU1EqgByFGmF4GaS8knP4cK6t:7bGqUeyFZF49vkx
MD5:	48D3F3F8CE178A43B7CD4613687AAD5E
SHA1:	1D2D13726703112C4D3E131C36C6E1F09560EBFC
SHA-256:	0674B61761E664F82AA66F06902B2E4103CD3A4C3F17FEFA76E91288E4C1A8CF
SHA-512:	9DBAD0514325588A5FCDEB2A1E0929309D3404EF8B425239CCB5E49F1EC7D8E368A1E003842D05316EAC51ACFEF03C281ACCD0C6547B4CB12533D7F8EC4BF EB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X...S..`...._keyhttps://manavakcina.lv/sess_head.mv.84b7e3c4c2ad458fafc8.js .https://manavakcina.lv/.{.`.#/.....:..aq..=..GG7\4b...cb.AR^...|...A..Eo... ...>5C.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\59b65e249a69bfa7_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\59b65e249a69bfa7_0	
Size (bytes):	244
Entropy (8bit):	5.6706694287618555
Encrypted:	false
SSDEEP:	3:m+lflDBlll08RzYl4J133ugIeF1GpLJ1AvNRMkTVKHtlHCxmt/zJvDp2/xOfUh68:mYld/PYK3uKG1WrpaSg/RZfUh/tnK6t
MD5:	11CB61CDC614A9BF85EA7D8E70B86E26
SHA1:	F5B0227763C6B9BE1056E2D9FD4DBE0A6AFBE5DB
SHA-256:	3374BC30989069F906F407A82920A87C85A0662DA9452301F4072F16889F31FF
SHA-512:	3D2B6567916C56E6637399889D40DB163CFB636037B112B1628A0E6C093D1FA3EF1C673EA62CA6101ECA3A0365E739D1D861D894E93BA0A73B1FB3480678D38E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....._keyhttps://platform.twitter.com/js/moment~timeline.bcb1cafa923482f4826e32741fe16a98.js .https://covid19.gov.lv/.CJa.#/.....y.M.....LuF'. ..a..P...]w....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5b8087e76d85696c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.591239599256016
Encrypted:	false
SSDEEP:	6:mCGYK/rT8isHaOnryf9Slk/k8wMSLZCYZ/ZK6t:L08isH52lWhMwZF/T
MD5:	0CB310C55466F4566978564B5D084A6C
SHA1:	F8F87C02D2D5E226E13793E9888BE4481498F51F
SHA-256:	0AAF8B5B7D82D119F747AFABA55E5182824CB6B405B44D84383DA360303AAB74
SHA-512:	0FC6B3DC191331C62A63BD82AFF55A5B733724EB12488F63D8C111463B6CA3C13FAEDC7B1380EDEFAABE689614263AB7293F157A87D26DDAF6263131A233499
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i.....@...._keyhttps://platform.twitter.com/js/timeline.28ecda9667eeb8e1b18898b99fee6c31.js .https://covid19.gov.lv/^.Ja.#/.....G.j.PH.....5k... khx_..V.A..Eo.....#/V.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5bf871745fcb6314_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	5.674701677607013
Encrypted:	false
SSDEEP:	3:m+llT8RzYPkTRNB8fYM5KcRTVHwgPiRtTKqIK+MkT1KHtlHCwUsVyft9kP5mrOD:milwYsDBYRCgPsHSwTmt9k4rithK6t
MD5:	331C02E0B8C8D8E0D267269F11AC0D05
SHA1:	8ABF5738401F80171949EEE6F3B44E143A280B9E
SHA-256:	BBF108FD49690B2EFFF0A12DA808EEA102A3C2943B09FB94BE5F7A05EA835C80
SHA-512:	D05B6DA098325CF97C800C1B9821A03014D258583A2BCA1AE1108A427C0FE962519C8703E06054A89C7A745FBC4CA90F8C3582569B94B880C291F5F6D607B5D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|....@R....._keyhttps://covid19.gov.lv/sites/default/files/js/js__Ta5swb09yQErhhz1adSh6m2iHvFEkgJlSZ-FbHozh0.js .https://covid19.gov.lv/.l5a.#/..... .....Fu+..nPM<8.%<er.W.sOZW..i.9.r.p..A..Eo.....s.j.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d703e79b940756d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	251
Entropy (8bit):	5.348515350710677
Encrypted:	false
SSDEEP:	6:mgqtVYS6WbBluKXwxE1M7LEdynFdIGaSMll55CZaa4g/rK6t:Nqt7RuKgtLaNWaa4gl
MD5:	F30E0642B3CBBF09E4D79045CA300D3C
SHA1:	E0849E55365FC4C2E20150CECBE4580ECC324843
SHA-256:	97867A9EC0CCDF184761CDDF7564B24F65E583CA6D93ABC4D4666D6E1BB3ECC7
SHA-512:	8E50D49232EF2491FCB1023B7D3809BDCAC27E200166F7E6700D398FB2AA383BBCE0EC7CE385B109C2565D6CCE0FD5F71B50779A04E95A7AC0663799A771531D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d703e79b940756d_0	
Preview:	0\r..m.....w....>....._keyhttps://ec.europa.eu/info/sites/default/themes/europa/bootstrap-sass/js/bootstrap/tab.js?quhwsu .https://europa.eu/.#Q`.#/.....c.....h..r.... ...RK.J.....)a....A..Eo.....rJxv.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\608ecaa1c32d20c3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24968
Entropy (8bit):	6.08501774873981
Encrypted:	false
SSDEEP:	384:CcuaDwH+S9HGesSr8aypvHP5iNqbpzsfhiN+np14m4rpcBkQDRr8asrqOTusUpD7:Cc7DwHF9HUphLcIOBkWm3uv3/0TZV7C
MD5:	76FDFE54EDBCBDC05112B3FA3BC632F1
SHA1:	A64F551140803B840C0637289F37ED2C07346FBD
SHA-256:	1BDBE0AD2EEB5C49DE1982BCC7CC487796FAA9CE1A8D11E4F0545D2B9D272D14
SHA-512:	8FD366C67525B36DA9742B24C4F7ACB3BF65973D2BE3C3C32F5D55256A0BF0784FD5FA551B192FEA72AF8BFF2CD4DCBBC5C1DDD974B857F13C3779A19A79FI 97
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....(.)...._keyhttps://abs.twimg.com/responsive-web/client-web/bundle.UserProfile.c227d965.js .https://twitter.com//..a.#/.....(..... ..Z.^..CD...(..q..;^..kn,..A ..Eo.....I.....A..Eo.....'.....O...._....u.....t.....4.....(S.l..`.....$L`.....QcV..G....window....Q.PJ.f"....webpackJsonp..Qb.....pu sh.....`.....L`.....`.....Ma.....`.....a.....Qb...W....ll/QC.(S.....`.%.....L`<.....Rc.....b.....Qb.@&.....r.....M...Qb.....s.....S...Qbv.....h.....Qb.f.>....p.....Qb.C.,....f... ..QbJ+M ...._.....Qb&G7.....w.....QbJ.....S.....Qb.....P.....Qbv5+%....C.....Qb.....x.....Qbf`.....v.....QbV.q\....T.....Qb^.j.....k.....QbNO.....F.....Qb.....N.....Qb.....O.... .Qb...~....B.....Qb.0."....L.....Qb..E.....U.....Qb.....R.....QbVrx.....A.....Qb.b.;....M.....QbZ.z.....D.....Qb..V.....W.....Qb..y.....j.....QbvS-4....H.....Qb.Y)7....V.....Qb.)

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\622cae38b93c9bad_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	263
Entropy (8bit):	5.464565006278566
Encrypted:	false
SSDEEP:	6:mc//6EYS6WbBst2YqIALKWfQ8FdT+/SdWU3Q7MnuK6t:xqC+fWvuKWU3nQ
MD5:	72CDBD1C878A27AA824F113779514D7D
SHA1:	E44814377E2FC58233CEDD1830B2F2820E8C831A
SHA-256:	E430133D22A5961DB5FFCFE37D4D6AB64F41713ABE4CEDBB05AC63009EFACD1A
SHA-512:	029C780266E26C34006B5BA30C0D67106D2850CF48CFE49CF385EDB7A6AE1B0D07C9A4BD2422DEA50EB8DA27972025C7BF1F91B5005A1FAAA6755A18DC1728 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\.%...._keyhttps://ec.europa.eu/info/sites/default/modules/custom/nexteuropa_feedback/js/nexteuropa_feedback.js?quhwsu .https://europa.eu/.D0`.#/..... .....y%k.p...2....,...^p6A.;.Xi).A..Eo.....C.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6386862eb4b2bb21_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9072
Entropy (8bit):	5.718150723509423
Encrypted:	false
SSDEEP:	192:71iQWpjHPAttd3lFTX1iasYPYo8jYpzlbx1WXWr:7/W5HYlFbMaHFp9x1X
MD5:	92367D2FCB0385E42B3AE1F492222F90
SHA1:	EF44A29BB3F8849E06C6BFE87C519220D3C02F27
SHA-256:	E1C59C7BB7917609D0401019E7507C6007D4936990EB5DB0AB30667EB1A87267
SHA-512:	F8D07C77467711DD8DBDC04B1D7A8B7DA7D49974EEBB3B020B45119206742F42425E90545E497453AF5EE65A365211CC5E91C211E272E04C0A32E33954727E2C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y_/r/JopZtdti8dq.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.,<b.#/.....N.....;...L.tUq9..,F....x..H. ....).A..Eo.....:.0.....A..Eo.....'.h.....O....!....0.....(S.d..`.....(L`.....Qbf.:....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`.....M `.....Qc...u....FEt5GzN...Qb.k.d...__d.. QfB.....CavalryLoggerImpl.....`.....@M`.....Q.@f.....Arbiter...Q.P..R.....Bootloader....Qb.....ISB.. Qf.u.....ImageTimingHelper ....$QgN.....KillabyteProfilerConfig..$Qg.a.....NavigationTimingHelper....Q.P:u.....PageEvents... Qf.....PageletEventConstsJS. Qf.r.....PageletEventsHelper...Qd...+ ....PerfXLogger..,QiVZ.....ResourceTimingBootloaderHelper....Qd.$.....ScriptPath....QdZCo.....performance..$Qg.....performanceAbsoluteNow...(S.l..`L.....L`j....`Rc,. .....O.....Qb.h.....h.....S...Qb2T.....j.....Qb.|.B...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\66041b6b090d03c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\66041b6b090d03c6_0	
File Type:	data
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.358841043066811
Encrypted:	false
SSDEEP:	6:mO2ilXYS6WbBluKXwxE1M7LEGfPFdLdHST1tlmdhzZt4tuubK6t:z7RuKgttndH0orK
MD5:	73923BD0D73EA8B9AAB1E67C44C5356C
SHA1:	CDA38556E2F5274D53BFB417284776797398E9CC
SHA-256:	1E53A1CE55853A212B30E33028340D1563E7146FF8C5ADBD6F7BA87B92B611E3
SHA-512:	570FD814F49B0F37867A00A6136E8808097DC51DE48431FAFA9766813E2FE31EA9DBCCCA78EA9B80A5BC60697F88C395053DC911A7963F810DE81C75A3E851E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}...TH.C...._keyhttps://ec.europa.eu/info/sites/default/themes/europa/bootstrap-sass/js/bootstrap/scrollspy.js?quhwsu .https://europa.eu/./P`.#/.....6.....c. .n..)X@c.{...tex.r...;.....A..Eo.....R..w.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\66baa5a4eaccbd8f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.55623660715575
Encrypted:	false
SSDEEP:	6:m/lYS6IdSVhaFlVNx+/SEllxzba8gr+nK6t:KjFu/NlrCxy
MD5:	847638CA35463E026A7AA66E9F9A8C2F
SHA1:	EC03696076E3F0A1BAB41C4ABE1078A6D29357D7
SHA-256:	0AC9515D537A911E62F5ED21F309C5ABB8A02FA55686E4885F0EBAD0A057D318
SHA-512:	2EE795C66A2C4F19D5C1987E30EFC413AC6DE0849BB79BB737C98BE0AB66DDDCB2AE13D74EBAFFB92A56FCF5864BA93B61417B9B953E91AA6A64784F881B4 E2A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://ec.europa.eu/info/misc/jquery-extend-3.4.0.js?v=1.10.2 .https://europa.eu/..P^.#/.....%.....G....p..b.....r\V\y...|.A..Eo.....@..... .A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\67dd0a4fe5b80501_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	68688
Entropy (8bit):	5.87031756708214
Encrypted:	false
SSDEEP:	1536:ljcclWNoICAYZU2HwUvUvAm5NwEBfNLOz9:lYclH9hPs7BfNLU
MD5:	3E22123EBA3FAB5014C566DCCC2BF3BB
SHA1:	3C10BDA5AF9779105645A2E5EB80D13478B3B725
SHA-256:	5AB945B015C983CB8A490B01403ABD019F299FE434BD432653283AA7342445D1
SHA-512:	4DC0FE0C733FCCE5E2E3E71ABD79AFF93555DBCFCF615CA364C157102E97D4FFE05B2D6579AEC2E5EC658FCDF5CCBCAD772E22E774D1F79443F3FE2F9FC8 444
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.../.]@....C41EB8FFCF6BB6746A4244522405A72D27D103EB67C070CAD0CFB5C2CA246323.....'.w'....O.....JN.....,..|...@..... .....|.....|.....(S.M..`R.....L`@.....Qbf.:.....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`.....M`.....Qc.....KufrNF/...Qb.k.d...__d..$Qg"..... .ReactFiberErrorDialog.....`.....M`..... Qf.-.....ErrorNormalizeUtils...QdF.c.....ErrorPubSub...QdNhe.....LogHistory....Q.P...@....getErrorSafe.(S.H.`F.....L`.....8Rc..... .....O.....a.....I`....DaT.....(S.....Ia.....M.....@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yO/r/RC4Bv8Ta_qo.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`>...D `.....)...`....&...&....&....&.(S.<..`.....L`.....8Rc.....O.....a.....I`....Da(.....(S.....IaK...b.....M....5....d.....@.....Qc...W....exports...K`....Di....8.....%.....&.%.- .....b.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\690304ca1c5c856d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.638254297781799
Encrypted:	false
SSDEEP:	6:mLfVYGLSmXZCV4/RRb9uSQp1UAYFOXPYb/CDK6t:mE4ZRhuhp1ZLQu
MD5:	0217B5AD5D7C0C413F44B6E2E01F5930
SHA1:	843812D9D3118E802EC32CDD8348959FBDBB83A9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\690304ca1c5c856d_0	
SHA-256:	128FD7B406D76B7534D6B4BF2A4329BC5BB5E2DBE52AA744003E4D6A92D47B78
SHA-512:	094AA7B4A9D17A10D70061DB8943419A0EA4BD441ED6EAB616C67940E28B69F8D3543013187558B50A1489AE7AF576802F62E22BB777F3FD36D035C22420B7D7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....."....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-161827578-1 .https://covid19.gov.lv/.l4a.#/.....t.....F.#T..x.#.1....+..."Z?.A..Eo.... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6e6886435ca913a3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	379
Entropy (8bit):	6.076904397481065
Encrypted:	false
SSDEEP:	6:mzzIEYk+f2pomWr2Kcaj7W5hmJ2wQKv/SA1us6+5bkDERNzbK6ty3BcflpkNqHq/:kB++amycgykJnv/Ruy5bkcHI3Bw8wqu1
MD5:	8B2EBAEE24E89F1205875D5E559D7426
SHA1:	D3E4825D68A8BC0184A7E9F5C7FD2C3282F52C04
SHA-256:	F62D898B23500760C1E41D808EA8168C75F6325DC3F7B4F7997D704B86DE98C7
SHA-512:	71E0929C4F199A5FAC878FD5940A3260EACFE51162F8B3AC2A9A705CEAD4E70ACE0453784D82B492E830AE82A6C56FC00CFB4A4A10810AD5FE36706228161AC 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....-D...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iN_84/yl/l/de_DE/qOr5EawgOvU.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..4b.#/.....M.....~. .%.....qF!..N.8...8.@..f....A..Eo.....4b.#/.....ECB8D669F3F015A889721CBACCEF453137609FF89F32456BDDEDB35492B43D19..~..%... ..qF!..N.8...8.@..f....A..Eo.....H.@L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\70b129a1476da8cc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.575492341192252
Encrypted:	false
SSDEEP:	6:mzRqEYS6Idz7HSfFlrXK/ScTXoW4NzbK6t:EPj1S956/FcWwN
MD5:	C645ED70C4D4488631A5515E296A7147
SHA1:	C6B7CC9DFD6F61C63CAE329F6C5EAA520F8B7508
SHA-256:	3DE99313CD7CB5C7C99A8FF399570F3D4535249D9B059F04FCB36DE8C16F0A4F
SHA-512:	7B278CD26DADB6E4268C241F3EB59E4E5EECC0A1D534680F5B66C3C713D55945709B9AEF780AAEAA92175E11DC6117369CC8A35746EC8DF829245CE7EBBF50 47
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....^<v...._keyhttps://ec.europa.eu/info/misc/jquery-html-prefilter-3.5.0-backport.js?v=1.10.2 .https://europa.eu/s.P^.#/.....um..e...,.s....{.....^.....A..Eo.. ....}..}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76927bdcdf216e46_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.339297275776407
Encrypted:	false
SSDEEP:	3:m+ltJlA8RzYXK+Mzxk4SF7SK+E59tlHCxy1w1KbDMTCjx/z4m3e1lpK5kt:mmYah1SrVHSxyC1KbDMmjxLr3eRK6t
MD5:	115B27FD335267FEF0B20AAA4D4072AF
SHA1:	494228B41B762015E472CF197DF55ABC0D146FFC
SHA-256:	FF3057B691A222BD6C3FE960E12327407716D54DF271AA415B1BA3B6036EB04A
SHA-512:	63F4CA76786E5D2645A815094EF56EECCC7426769F2E35DAF358B8B971F4E695055D8288614EF1F20274CDBD91A4E8D7B2CE16AA3A287DE351BA2C8C6FEE6E5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E....v8Z...._keyhttps://europa.eu/webtools/webtools.globan.js .https://europa.eu/:Vm`.#/.....n>....0,.>..)..`.9.VG.i. .\#..A..Eo.....R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76ba21a7a0c3dfff_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\76ba21a7a0c3dfff_0	
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.850884762225976
Encrypted:	false
SSDEEP:	6:mOXnYTWigAH2dtHs60zyWVCHSN16DAzwGz4zZK6t:fZigAUsRzq66ZdT
MD5:	14576D3623BF475D339DBBBDF6A5BA63
SHA1:	F5F596BE4ED04621D7B2B4B3BB14E939929F40C5
SHA-256:	CA21C479BF143DFEC22F1FAE9B70FD7CF85BDBCFB3CF7772A8E9DFADBAB32265
SHA-512:	AF2991957FC048AA7B7B65ACBA7E9BED61FD077F177228C1AE733BF553005891DD01F4B4C73A85D525804B938CC9D587F8EEEF739F479EF69FAF6E11FE34CC2 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}.....`8...._keyhttps://vpm2.viss.gov.lv/STS/VPM2/bundles/WebFormsJs?v=vlaiI0HgepEnk_u1HZndmi_-Lu6wAJsf7dFsyM7r_2k1 .https://viss.gov.lv/}..].#/.....\ .....W0..>;...I.~N.W....b4%..*..#3g..A..Eo.....I.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\788d15787b71e5e8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215816
Entropy (8bit):	5.8968226087988
Encrypted:	false
SSDEEP:	3072:NnEoDXll55HBm94j4n2/RMkMrWrWD8/xNu/8XJHB:7lX194n2oMWY/68XJHB
MD5:	6A62974F9E3D968875859C5659B64C61
SHA1:	24194DC49401DF3C41A53F7A2BC31FE8117DA02D
SHA-256:	4BCD11A64BD837B64D1008E903A18F15FE1177A00966361B69C8FEF4E2B81930
SHA-512:	2DBEA5AF4C33A24E823DBAEB3097354E1388E35FB343365265ACD7A7DB2280701DF7F4F2CF49F9D803E8E080F4A14AF1BAAA7436735B7B27FBE341400A6AD35 F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....;?!....E12F3832A09CCA45A579A8054619BC2DBB1A8480D287A480A33720E571362352.....'.....OC...(I..WI.....(....'.....`"..... .....\..... .....(S...'..`*O.....q.L`.....Qbf.:....self. .Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`.....M`.....Qcv.h....pgovsL/..(S..`.....,L`.....8Rc.....M....O.a.....I`....Da.....Qb...e....flat.(S.....Ia..../.....d..... .....2.@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/ya/r/nKQgTVgFAG8.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D`....D`.....a"...`,...&...&..q/&...3D&...(S.....Pd. .....Array.flat..aM.....I...15d.....&.(S.....O.a.....2.d.....&.(S.....5.a.....Pc.....flatMapa.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78b9b6df18d2eae2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7160
Entropy (8bit):	5.867764545186969
Encrypted:	false
SSDEEP:	192:8ieO0yoC0mhk8IhPGGkp6bIbcu1YV+Txg:8/UoC0gYXbIbcC/W
MD5:	A25874094927C3B8CD7EE3141EC29E54
SHA1:	E26E5B447F2504D71283250342AD973931739C49
SHA-256:	8431002B043FBE92B9CAE8AF53AE3E87238A991611FD4898D09BD410ECB2165E
SHA-512:	42E928AABDFD32FA1536EE92BB1415D3F8B2AC35191B987C3C5D6CBDCB0DB0DF1B8DD1BF6B65F8239494EF9C8B12ED58DE4678D2A3E7141FBF5CEC47FAE5/ 11C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...iS~....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yG/r/jf43jL33vGK.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/..<b.#/.....N.....w...9.....K.%...nX.r. ..^]Q..A..Eo.....A..Eo.....'..*....O....h.....n.....(.....(S.M...`N.....L`>.....Qbf.:.....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`..... M`.....Qc&KN.....NVC4WD0...Qb.k.d...__d.. Qf.....InlineBlock.react.....`.....M`.....Qb.4.....cx....Qd.b.....joinClasses...Qd^..1....prop-types....Qc..i.....react....(S..`D....PL`$... .@Rc.....O....S...Qb2T.....j...b.....I`....Da....l.....,..a.....Qc..1....baselineF..Qc..2f....bottom....Qb.....6d...Qc..S.....middle....Qb~....._6b...Qb.$*.....top. ..Qb..l...._6e..(S.....Ia..... ..f.....@.....@. ....I..!..@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yG/r/jf43jL33vGK.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D` R...D`....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d4315639ae7120e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.592704701588842
Encrypted:	false
SSDEEP:	6:mfXYMGpAIEpEqgByFGKS/kke6oxzkvP4fZK6t:KTYJXyFpAPwT

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d4315639ae7120e_0	
MD5:	AC4C6CA10405866CC96E5574409541E0
SHA1:	83809BB570ACD7A775FA67F2513C04021D85C472
SHA-256:	DD79317DA693563E40103E42106ABF2B97568D8915E75F2141BA0BA487744DEA
SHA-512:	882A1A49A20AE470DA06A3E688738A94F054F59B7BF6ED3C4564807BD2D59B54EBBBABBBE395B8966350077DDF6097C3291DAEB50E23378F82BB9D295C88395
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\....Go....._keyhttps://manavakcina.lv/vendors~index.mv.84b7e3c4c2ad458fafc8.js .https://manavakcina.lv/b..`.#/.....:r.oOO..._..&.x....'...G9..?..A..Eo.. .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\805c16eafbc3c530_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	289
Entropy (8bit):	5.536466952554954
Encrypted:	false
SSDEEP:	6:mdYS66b7E+7s24XNVu9TwFlu41/SAlloFQ/JhK6t:+hbda+TY11/kA7
MD5:	1D92409D0F66653F666687859C833D63
SHA1:	3ACFC217DCE733E8CD385F33FEB8FB05A09D7CB4
SHA-256:	06F5F926B8C7C65839681A5D4E6A5B32093BCC449BF676A8E2B79032FCC8A051
SHA-512:	05280FD1F57FEF7381258D27EA28FAE20F0869109F89103A9C0675A616C17F7E9BBB086EC7624A93E9C4762A2E659E85A99B511A0DB4D541C0FBAD2C32003AF7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....7!....._keyhttps://ec.europa.eu/info/profiles/multisite_drupal_standard/modules/contrib/jquery_update/replace/jquery/1.10/jquery.min.js?v=1.10.2 .https:/ /europa.eu/PmP^.#/.....#.....X...e..&.H.S....U0.t...;..1.O.A..Eo.....a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\805e0b59b714f9af_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	51683
Entropy (8bit):	5.919545568037941
Encrypted:	false
SSDEEP:	768:5EwjI5PIG59Rzz/2UXWOXUBo/HDvhmoPCDBnu4euL/Sp51zL7:5EwjyNNOUmOXoaH1moPqButuL/sDv
MD5:	7FCDBB3361A6374A42E124820B843B95
SHA1:	8ABB8294C4F43EC69936F09F58A083D29AD032AC
SHA-256:	16468EAD2F930918DF68BE80260060473A06429DC43D3856B6CFAA36BC0FFD53
SHA-512:	488F9D8F996141C210DF0ED39C5EF947EA4C4F280504C7556EC82D6DE7EF661BD5F3FE8406DDAD1B5A311F22B215DF518FA6928BA34877948C7D2204A37BD8A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...jH ....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i2UN4/y3/l/de_DE/3i7v8hvbQ9J.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.,<b.#/.....N.....J,.6..w/.... 6..)zy....M....(H..A..Eo.....u{.#.....A..Eo.....'.....O.....(.....(S.U...`^.....L`.....Qbf.:....self..Q.`F.! ....CavalryLogger.....Qc.g.c....start_js.....`.....M`.....Qc..]....7tOe5qb...Qb.k.d...__d.. Qf.....isAdsExcelAddinURI...(S.T.`^....$L`.....8Rc.....Qb.h.....h...a.....I`....D a.....(S.....Ia....W.....M...Q#.@.-....dP.....X...https://static.xx.fbcdn.net/rsrc.php/v3i2UN4/y3/l/de_DE/3i7v8hvbQ9J.js?_nc_x=Ij3Wp8lg5Kza.....D`....D`@...D`.....`. ...&...&... &..q$&.(S...T..`^....$L`.....8Rc.....1$a.....I`....Da....N....(S.....Ia.....M.....Q%d.....Qc...W....exports.....PQr.{..A...((^|\.)instagram\.com$)

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\83703561b8ee400f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	379
Entropy (8bit):	5.937646454553674
Encrypted:	false
SSDEEP:	6:mbyYk+f2pomWucC6zhmJ239SvtsleW84OhQK6tEL+r3ZCRuPfQRjQaeW84Oh7R:Mu++amncRkJmJleW8MS+OuPfQRjQaeW8
MD5:	A6D76AC2669903DB1ABEECD61A179E9F
SHA1:	574B2AC166020B69B0F4B595E965BF8AFC24358B
SHA-256:	5488EB847C1C9C7D2E6B5EEB03F1548C9F09AADB81509CAC95D26CFA2AC36921
SHA-512:	DE8B4C180FC5D1A9BA1BBEF28330389B3680587122F0F11038753A47B889A071DB328C86DF1086E45F3A05B5327991B4E39CC87450C52FDB44E56838873867BC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...? ....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ibo64/yv/l/de_DE/9DL_vTkVYwy.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.f;b.#/.....N.....A...3P|B .Ezz....".?....V..A..Eo.....A..Eo.....f;b.#/.0...9842F66479067907DBF09F7BCF312BC02D00E7C64A3568752961EF4B7AC48108.....A...3P|B.Ezz....".?....V. .A..Eo.....v>L.....

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):	5.384572799605149
Encrypted:	false
SSDEEP:	3:m+lrlaK8RzYiMRLyM6IpMREp4dHtlHCsltrXrvj8IcNup5+/z4m4BhltpK5kt:mEanYiMs8pM9SsXj8IcNupgLrMnK6t
MD5:	E65B7E90BFACEBEA1E2F9CBF4053CC66
SHA1:	FA4EF15F907B340CAD8FDE5C0E92A69715B6872E
SHA-256:	4C6B3215B86271DE554A0E42FB3DE0432ED50054271888D5D861C179A1AB4A5C
SHA-512:	DB30AC2F9B664C77235FF2FBF8FB303FE92CB35C4807BA93D4E1DFB55307592C8C4672C07040F6492550B277BE22A71FEEBBB6D0711528F8B8B5EAB0F624834
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....._keyhttps://twitter.com/i/js_inst?c_name=ui_metrics .https://twitter.com/.u.a.#/.....Y).....D...L...9..g.....-...m...oN.B.A..Eo.....R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\84a2c65baeedd7c9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3192
Entropy (8bit):	5.749552935058922
Encrypted:	false
SSDEEP:	48:9zlXaTPAtZffTljiqtuUVNX/Na66QsU8+AVR81NLDC1RLY6pWanxsoiHH7uTL6s6:9zBGmTXu566VBsR+1REaFxL2ua
MD5:	85CB79A77EC65AE8CF8918D79C4C0958
SHA1:	74AA79962885BBE8CA3F4CDE6F5DCACFB22FFED5
SHA-256:	6693812B82447A6E7D46DBE0A7999DD7C46CA2F4A810DDEA4E27B4791219BAEA
SHA-512:	8008F9CF1462178BB61B923F00299D5F6BB4C6BB861C5FC39E483DECFD977C5171CD76E02D1A1D2DAF6E1E1EBDE84BD2459BB7BF24206742A92B99206EBEC8B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....S...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yB/r/j06NZgGeWmg.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/--<b.#/.....N.....-.....&.z...Y\.V...@n.....A..Eo.....`x.....A..Eo.....--<b.#/.H.....'.....O.....:W.....|.....(S....`.....<L`.....Qbf.:....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`...M`.....Qc.....hWhIggq...Qb.k.d...__d..,Qi.*I? ...EventListenerImplForCacheStorage...`.....M`.....Qd".. ....cr:1351741...(S.0.`.....L`.....Qc...W....exports...K`....Df....8.....&.]...-.....(Rc.....I`....Da....l.....b.....,...@.-....\P.a.....M...https://static.xx.fbcdn.net/rsrc.php/v3/yB/r/j06NZgGeWmg.js?_nc_x=Ij3Wp8lg5Kz...a.....D`....D `Z...D`.....`r...&...&..a.&.(S..`f....`L`,....xRc8.....QbZ.yv....e.....O.....Qb.h.....h.....S...Qb2T.....j.....Qb.|.B....k.....Qb~.....l.....Qb._N.....m.....Qb..1j....n...i$.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86b899db8793e745_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	115376
Entropy (8bit):	5.896116268367674
Encrypted:	false
SSDEEP:	1536:29vva7smQUuMMU+KObk/QyKodMiiaaxwD/bOfj8rZJF0LD14FiXgjmn0uZjk+cXK:Ga75QUUU+D9a/nsVG+cXbGyalDd
MD5:	5C00E2AE616227A45D3DABD0EA14A143
SHA1:	CD4FBB2059813F4D98F04D5C8BE1F0EA9CE9F0F0
SHA-256:	FFD7A298F759DF4E6ED035CF1CD3C59D46AC37D8360C463FEE3C4D44BFBFFD6B
SHA-512:	1DE1BC2B6479DA3C38B0A23B992FE8F487F07C4FCED0CCE147CEBE2250F28E90D67EEA9F688BF2A40F2BDAE6B93C9D0BEF264B3677A2E4DBD7D881CD72E4C382
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...+.....ECB8D669F3F015A889721CBACCEF453137609FF89F32456BDDEDB35492B43D19.....'.....O(...@....g.....(.....L.....H.....p.....(S.....`.%.....L`.....Qbf.:....self..Q.`F.!....CavalryLogger.....Qc.g.c....start_js.....`.....M`.....Qc..'.....7cWmW3B...Qb.k.d....__d...Qdn.....GenderConst..(S.,.`.....L`.....I..a2.....Qd.Q.....NOT_A_PERSON`.....Qe.:%.....FEMALE_SINGULAR.`.....Qerr.....MALE_SINGULAR...`.....$Qgz..#....FEMALE_SINGULAR_GUESS...`..... Qfz,.`....MALE_SINGULAR_GUESS.`.....Qe"S.J....MIXED_UNKNOWN...`.....QeR.....NEUTER_SINGULAR.`.....Qe...`....UNKNOWN_SINGULAR`.....Qe..3....FEMALE_PLURAL...`.....Qd2;.....MALE_PLURAL.`.....Qe.....NEUTER_PLURAL...`.....Qe:..9....UNKNOWN_PLURAL..`.....Qc...W....exports...K`....De....8.....}..)-.....(Rc.....I`....Da.....b.....S....@.-

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8cbb0e39b96bd90d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2830
Entropy (8bit):	5.746868092681523
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8cbb0e39b96bd90d_0	
SSDEEP:	48:Qm6bgH92pdg9dx5TuQm0Llm6bW+8wpC8F+bpxjsjv+m6bXhhCTck/sEl5xtQ9U:bHkI5W+8wk8F+lxjkOha/fWS
MD5:	15FCEE2A66C2B9DEC5D5B9845E1C1883
SHA1:	CF7AF1733825708E860CF5FA96F200C294BA8A44
SHA-256:	4F14E60FDBEAB20C4735DA295D9D8B8393079ED2DBE74BDFAC65106A256BAAC9
SHA-512:	654CF3D7BBC58F2DEF23A3BB28054E160DED08122AEF1FEE74FF26617209BE3D652A3CE65DEB2693CB312ACA3F41645CFF4B45612C456D17F0B9D71C018BF6F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....~.....|....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~loader.Typeahead~bundle.UserLists.35567b05.js .https://twitter.com/.W.a.#/..... .,.....?..8.#F...)9.F.....7..%.;....A..Eo.....kM[.....A..Eo.....W.a.#/.....'..}....O.....]0.....(S...`.....tL`6.....QcV..G....window....Q.PJ.f "....webpackJsonp..Qb.....push.....`.....L`.....`.....Ma...."...`.....d..a.....QbB9.S....3EFPC..Qb.<.....4e/KC..Qb6.:.....AQOcC..QbF.I.....LbZ7C..Qb.....OEYwC..Qbf*; n....OhSZC..Qb...N....V5QiC..Qb.....ZcYNC..Qb.....aA19C..Qb.....o52zC..Qb..F.....p9G8C.(S.....Pd.....push.3EFP...aI...o.....E.@.-....pP.....d...https://abs.twimg.com/responsive-web/client-web/shared~loader.Typeahead~bundle.UserLists.35567b05.jsa.....D`....D`2...D`.....i....`....&...&..q..D&.(S.....Pd.....push.4e/K...a....> ...T..sF.. .....5..@.5.6..@.6.6..@.6.7..@.7.7..@.8.8..@.8.9..@..*.**.....@.....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 17:55:20.110131979 CEST	192.168.2.6	8.8.8.8	0x6d6a	Standard query (0)	covid19sertifikats.lv	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:22.290606976 CEST	192.168.2.6	8.8.8.8	0xdf9f	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:23.140742064 CEST	192.168.2.6	8.8.8.8	0x723b	Standard query (0)	covid19sertifikats.lv	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:37.793452978 CEST	192.168.2.6	8.8.8.8	0xa9f1	Standard query (0)	vpm2.viss.gov.lv	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:41.956187010 CEST	192.168.2.6	8.8.8.8	0x9ae2	Standard query (0)	vpm2.viss.gov.lv	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:44.529675007 CEST	192.168.2.6	8.8.8.8	0x5e54	Standard query (0)	ec.europa.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:52.414959908 CEST	192.168.2.6	8.8.8.8	0xc395	Standard query (0)	europa.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:53.496339083 CEST	192.168.2.6	8.8.8.8	0x8e2f	Standard query (0)	webanalytics.ec.europa.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:54.621160984 CEST	192.168.2.6	8.8.8.8	0x754a	Standard query (0)	ec.europa.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:01.891988993 CEST	192.168.2.6	8.8.8.8	0x199f	Standard query (0)	manavakcina.lv	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:03.836460114 CEST	192.168.2.6	8.8.8.8	0x4083	Standard query (0)	manavakcina.lv	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:05.962855101 CEST	192.168.2.6	8.8.8.8	0x92b8	Standard query (0)	covid19.gov.lv	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:06.845259905 CEST	192.168.2.6	8.8.8.8	0x73a4	Standard query (0)	cdn.matomo.cloud	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:06.847031116 CEST	192.168.2.6	8.8.8.8	0x8b63	Standard query (0)	static.addtoany.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:07.182024956 CEST	192.168.2.6	8.8.8.8	0x1695	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:07.878289938 CEST	192.168.2.6	8.8.8.8	0x17cb	Standard query (0)	syndication.twitter.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 17:56:08.439694881 CEST	192.168.2.6	8.8.8.8	0xd26	Standard query (0)	cdn.syndication.twimg.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:08.951051950 CEST	192.168.2.6	8.8.8.8	0xecf1	Standard query (0)	covid19.gov.lv	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:09.234971046 CEST	192.168.2.6	8.8.8.8	0x3c3a	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:09.314997911 CEST	192.168.2.6	8.8.8.8	0x92ba	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:12.619971037 CEST	192.168.2.6	8.8.8.8	0xdf3a	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.142940044 CEST	192.168.2.6	8.8.8.8	0x3b35	Standard query (0)	api.twitter.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.146575928 CEST	192.168.2.6	8.8.8.8	0xa030	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.199711084 CEST	192.168.2.6	8.8.8.8	0x1d96	Standard query (0)	video.twimg.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:17.362037897 CEST	192.168.2.6	8.8.8.8	0x4eeb	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:17.575958967 CEST	192.168.2.6	8.8.8.8	0x8a49	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:17.995964050 CEST	192.168.2.6	8.8.8.8	0xa411	Standard query (0)	abs-0.twimg.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:22.321613073 CEST	192.168.2.6	8.8.8.8	0x8642	Standard query (0)	abs-0.twimg.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:22.709907055 CEST	192.168.2.6	8.8.8.8	0x2410	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:23.260128975 CEST	192.168.2.6	8.8.8.8	0xea43	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:23.626977921 CEST	192.168.2.6	8.8.8.8	0xacac	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:25.229579926 CEST	192.168.2.6	8.8.8.8	0xb28f	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:25.334043026 CEST	192.168.2.6	8.8.8.8	0x8f49	Standard query (0)	cs.atdmt.com	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:25.338574886 CEST	192.168.2.6	8.8.8.8	0xe6eb	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 17:55:20.190234900 CEST	8.8.8.8	192.168.2.6	0x6d6a	No error (0)	covid19sertifikats.lv		104.21.8.55	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:20.190234900 CEST	8.8.8.8	192.168.2.6	0x6d6a	No error (0)	covid19sertifikats.lv		172.67.156.224	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:22.359747887 CEST	8.8.8.8	192.168.2.6	0xdf9f	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:55:22.359747887 CEST	8.8.8.8	192.168.2.6	0xdf9f	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:23.201307058 CEST	8.8.8.8	192.168.2.6	0x723b	No error (0)	covid19sertifikats.lv		104.21.8.55	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:23.201307058 CEST	8.8.8.8	192.168.2.6	0x723b	No error (0)	covid19sertifikats.lv		172.67.156.224	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:37.890227079 CEST	8.8.8.8	192.168.2.6	0xa9f1	No error (0)	vpm2.viss.gov.lv		195.244.156.188	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:42.015836954 CEST	8.8.8.8	192.168.2.6	0x9ae2	No error (0)	vpm2.viss.gov.lv		195.244.156.188	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:44.589374065 CEST	8.8.8.8	192.168.2.6	0x5e54	No error (0)	ec.europa.eu		147.67.34.30	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:44.589374065 CEST	8.8.8.8	192.168.2.6	0x5e54	No error (0)	ec.europa.eu		147.67.210.30	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:52.478743076 CEST	8.8.8.8	192.168.2.6	0xc395	No error (0)	europa.eu		147.67.210.45	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 17:55:52.478743076 CEST	8.8.8.8	192.168.2.6	0xc395	No error (0)	europa.eu		147.67.34.45	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:53.556003094 CEST	8.8.8.8	192.168.2.6	0x8e2f	No error (0)	webanalytics.ec.europa.eu	webanalytics-ec-prd.fpfis.tech.ec.europa.eu		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:55:53.556003094 CEST	8.8.8.8	192.168.2.6	0x8e2f	No error (0)	webanalytics-ec-prd.fpfis.tech.ec.europa.eu	lb-webanalytics-ec-europa-eu-768915372.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:55:53.556003094 CEST	8.8.8.8	192.168.2.6	0x8e2f	No error (0)	lb-webanalytics-ec-europa-eu-768915372.eu-central-1.elb.amazonaws.com		3.67.90.247	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:53.556003094 CEST	8.8.8.8	192.168.2.6	0x8e2f	No error (0)	lb-webanalytics-ec-europa-eu-768915372.eu-central-1.elb.amazonaws.com		18.156.187.205	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:54.675700903 CEST	8.8.8.8	192.168.2.6	0x754a	No error (0)	ec.europa.eu		147.67.34.30	A (IP address)	IN (0x0001)
Jun 11, 2021 17:55:54.675700903 CEST	8.8.8.8	192.168.2.6	0x754a	No error (0)	ec.europa.eu		147.67.210.30	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:01.955188036 CEST	8.8.8.8	192.168.2.6	0x199f	No error (0)	manavakcina.lv		104.21.35.245	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:01.955188036 CEST	8.8.8.8	192.168.2.6	0x199f	No error (0)	manavakcina.lv		172.67.181.126	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:03.911135912 CEST	8.8.8.8	192.168.2.6	0x4083	No error (0)	manavakcina.lv		172.67.181.126	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:03.911135912 CEST	8.8.8.8	192.168.2.6	0x4083	No error (0)	manavakcina.lv		104.21.35.245	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:06.082137108 CEST	8.8.8.8	192.168.2.6	0x92b8	No error (0)	covid19.gov.lv		212.70.163.204	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:06.909512997 CEST	8.8.8.8	192.168.2.6	0x8b63	No error (0)	static.addtoany.com		104.22.70.197	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:06.909512997 CEST	8.8.8.8	192.168.2.6	0x8b63	No error (0)	static.addtoany.com		104.22.71.197	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:06.909512997 CEST	8.8.8.8	192.168.2.6	0x8b63	No error (0)	static.addtoany.com		172.67.39.148	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:06.920161009 CEST	8.8.8.8	192.168.2.6	0x73a4	No error (0)	cdn.matomo.cloud		13.32.25.103	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:06.920161009 CEST	8.8.8.8	192.168.2.6	0x73a4	No error (0)	cdn.matomo.cloud		13.32.25.48	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:06.920161009 CEST	8.8.8.8	192.168.2.6	0x73a4	No error (0)	cdn.matomo.cloud		13.32.25.96	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:06.920161009 CEST	8.8.8.8	192.168.2.6	0x73a4	No error (0)	cdn.matomo.cloud		13.32.25.32	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:07.245475054 CEST	8.8.8.8	192.168.2.6	0x1695	No error (0)	platform.twitter.com	cs472.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:07.245475054 CEST	8.8.8.8	192.168.2.6	0x1695	No error (0)	cs472.wac.edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:07.245475054 CEST	8.8.8.8	192.168.2.6	0x1695	No error (0)	cs1-apr-8315.wac.edgecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:07.245475054 CEST	8.8.8.8	192.168.2.6	0x1695	No error (0)	cs1-lb-eu.8315.ecdns.net	cs41.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:07.245475054 CEST	8.8.8.8	192.168.2.6	0x1695	No error (0)	cs41.wac.edgecastcdn.net		93.184.220.66	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 17:56:07.934026957 CEST	8.8.8.8	192.168.2.6	0x17cb	No error (0)	syndicatio n.twitter.com		104.244.42.136	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:07.934026957 CEST	8.8.8.8	192.168.2.6	0x17cb	No error (0)	syndicatio n.twitter.com		104.244.42.72	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:07.934026957 CEST	8.8.8.8	192.168.2.6	0x17cb	No error (0)	syndicatio n.twitter.com		104.244.42.200	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:07.934026957 CEST	8.8.8.8	192.168.2.6	0x17cb	No error (0)	syndicatio n.twitter.com		104.244.42.8	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:08.498786926 CEST	8.8.8.8	192.168.2.6	0xd26	No error (0)	cdn.syndic ation.twimg.com	cs196.wac.edgecastcdn.n et		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:08.498786926 CEST	8.8.8.8	192.168.2.6	0xd26	No error (0)	cs196.wac. edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:08.498786926 CEST	8.8.8.8	192.168.2.6	0xd26	No error (0)	cs2-wac-eu .8315.ecdns.net	cs45.wac.edgecastcdn.ne t		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:08.498786926 CEST	8.8.8.8	192.168.2.6	0xd26	No error (0)	cs45.wac.e dgecastcdn.net		93.184.220.70	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:09.012708902 CEST	8.8.8.8	192.168.2.6	0xecf1	No error (0)	covid19.gov.lv		212.70.163.204	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:09.305468082 CEST	8.8.8.8	192.168.2.6	0x3c3a	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.n et		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:09.305468082 CEST	8.8.8.8	192.168.2.6	0x3c3a	No error (0)	cs510.wpc. edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:09.367759943 CEST	8.8.8.8	192.168.2.6	0x92ba	No error (0)	pbs.twimg.com	twimg.twitter.map.fastly.n et		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:09.367759943 CEST	8.8.8.8	192.168.2.6	0x92ba	No error (0)	twimg.twit ter.map.fa stly.net		199.232.136.159	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:12.675252914 CEST	8.8.8.8	192.168.2.6	0xdf3a	No error (0)	twitter.com		104.244.42.129	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:12.675252914 CEST	8.8.8.8	192.168.2.6	0xdf3a	No error (0)	twitter.com		104.244.42.1	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.195252895 CEST	8.8.8.8	192.168.2.6	0x3b35	No error (0)	api.twitter.com	tpop-api.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:13.195252895 CEST	8.8.8.8	192.168.2.6	0x3b35	No error (0)	tpop-api.t witter.com		104.244.42.2	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.195252895 CEST	8.8.8.8	192.168.2.6	0x3b35	No error (0)	tpop-api.t witter.com		104.244.42.66	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.195252895 CEST	8.8.8.8	192.168.2.6	0x3b35	No error (0)	tpop-api.t witter.com		104.244.42.194	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.195252895 CEST	8.8.8.8	192.168.2.6	0x3b35	No error (0)	tpop-api.t witter.com		104.244.42.130	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.198415995 CEST	8.8.8.8	192.168.2.6	0xa030	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.198415995 CEST	8.8.8.8	192.168.2.6	0xa030	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.198415995 CEST	8.8.8.8	192.168.2.6	0xa030	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.198415995 CEST	8.8.8.8	192.168.2.6	0xa030	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:13.260382891 CEST	8.8.8.8	192.168.2.6	0x1d96	No error (0)	video.twimg.com	cs296.wpc.edgecastcdn.n et		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:13.260382891 CEST	8.8.8.8	192.168.2.6	0x1d96	No error (0)	cs296.wpc. edgecastcdn.net	cs2-wpc.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 17:56:13.260382891 CEST	8.8.8.8	192.168.2.6	0x1d96	No error (0)	cs2-wpc-eu.8315.ecdns.net	cs531.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:13.260382891 CEST	8.8.8.8	192.168.2.6	0x1d96	No error (0)	cs531.wpc.edgecastcdn.net		192.229.220.133	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:17.422621012 CEST	8.8.8.8	192.168.2.6	0x4eeb	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:17.422621012 CEST	8.8.8.8	192.168.2.6	0x4eeb	No error (0)	cs510.wpc.edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:17.625938892 CEST	8.8.8.8	192.168.2.6	0x8a49	No error (0)	pbs.twimg.com	twimg.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:17.625938892 CEST	8.8.8.8	192.168.2.6	0x8a49	No error (0)	twimg.twitter.map.fastly.net		199.232.136.159	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:18.045970917 CEST	8.8.8.8	192.168.2.6	0xa411	No error (0)	abs-0.twimg.com	abs-zero.twimg.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:18.045970917 CEST	8.8.8.8	192.168.2.6	0xa411	No error (0)	abs-zero.twimg.com		104.244.43.131	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:22.371725082 CEST	8.8.8.8	192.168.2.6	0x8642	No error (0)	abs-0.twimg.com	abs-zero.twimg.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:22.371725082 CEST	8.8.8.8	192.168.2.6	0x8642	No error (0)	abs-zero.twimg.com		104.244.43.131	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:22.769025087 CEST	8.8.8.8	192.168.2.6	0x2410	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:22.769025087 CEST	8.8.8.8	192.168.2.6	0x2410	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:23.310122013 CEST	8.8.8.8	192.168.2.6	0xea43	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:23.310122013 CEST	8.8.8.8	192.168.2.6	0xea43	No error (0)	scontent.xx.fbcdn.net		157.240.27.27	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:23.687908888 CEST	8.8.8.8	192.168.2.6	0xacac	No error (0)	facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:25.293257952 CEST	8.8.8.8	192.168.2.6	0xb28f	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:25.293257952 CEST	8.8.8.8	192.168.2.6	0xb28f	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:25.397030115 CEST	8.8.8.8	192.168.2.6	0xe6eb	No error (0)	facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Jun 11, 2021 17:56:25.399461985 CEST	8.8.8.8	192.168.2.6	0x8f49	No error (0)	cs.atdmt.com	star.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 17:56:25.399461985 CEST	8.8.8.8	192.168.2.6	0x8f49	No error (0)	star.c10r.facebook.com		31.13.92.10	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- covid19sertifikats.lv

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6020 Parent PID: 3284

General

Start time:	17:55:17
Start date:	11/06/2021
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 'http://covid19sertifikats.lv'
Imagebase:	0x7ff7c15e0000
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: 5720 Parent PID: 6020

General

Start time:	17:55:18
Start date:	11/06/2021
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=1580,8389171160626933808,14452260508819524 82,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1712 /prefetch:8
Imagebase:	0x7ff7c15e0000
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

Disassembly