ID: 458900
Cookbook: browseurl.jbs
Time: 21:00:45
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report https://pub.lucidpress.com/d2d8f4ec-03d1-433d-9635-8d794acb5292/#_0 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
Contacted URLs 6
URLs from Memory and Binaries 6
Contacted IPs 6
Public 6
Private 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 40
No static file info 40
Network Behavior 40
Code Manipulations 40
Statistics 40
Behavior 40
System Behavior 40
Analysis Process: chrome.exe PID: 5196 Parent PID: 5112 40
General 40
File Activities 41
Registry Activities 41
Analysis Process: chrome.exe PID: 3528 Parent PID: 5196 41
General 41
File Activities 41
Registry Activities 41
Analysis Process: chrome.exe PID: 7324 Parent PID: 5196 41
General 41
Analysis Process: chrome.exe PID: 6968 Parent PID: 5196 41
General 41
File Activities 42
Registry Activities 42
Disassembly 42

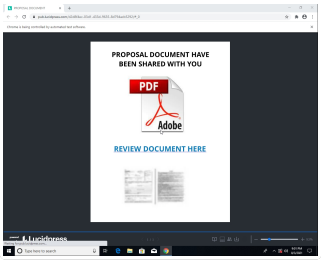
Windows Analysis Report https://pub.lucidpress.com/d…

Overview

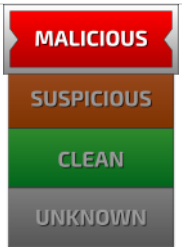
General Information

Sample URL:	http://https://pub.lucidpress.com/d2d8f4ec-03d1-433d-9635-8d794acb5292/#_0
Analysis ID:	458900
Infos:	

Most interesting Screenshot:



Detection



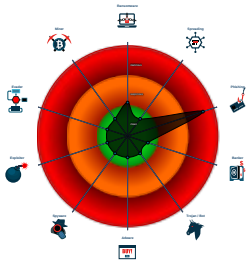
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on sh…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- Form action URLs do not match mai…
- Found iframes
- HTML body contains low number of …
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5196 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://pub.lucidpress.com/d2d8f4ec-03d1-433d-9635-8d794acb5292/#_0' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3528 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1312,3565287986375282334,5985329352411713397,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1760 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7324 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1312,3565287986375282334,5985329352411713397,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6724 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6968 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1312,3565287986375282334,5985329352411713397,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=6568 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Phishing:

Phishing site detected (based on shot template match)

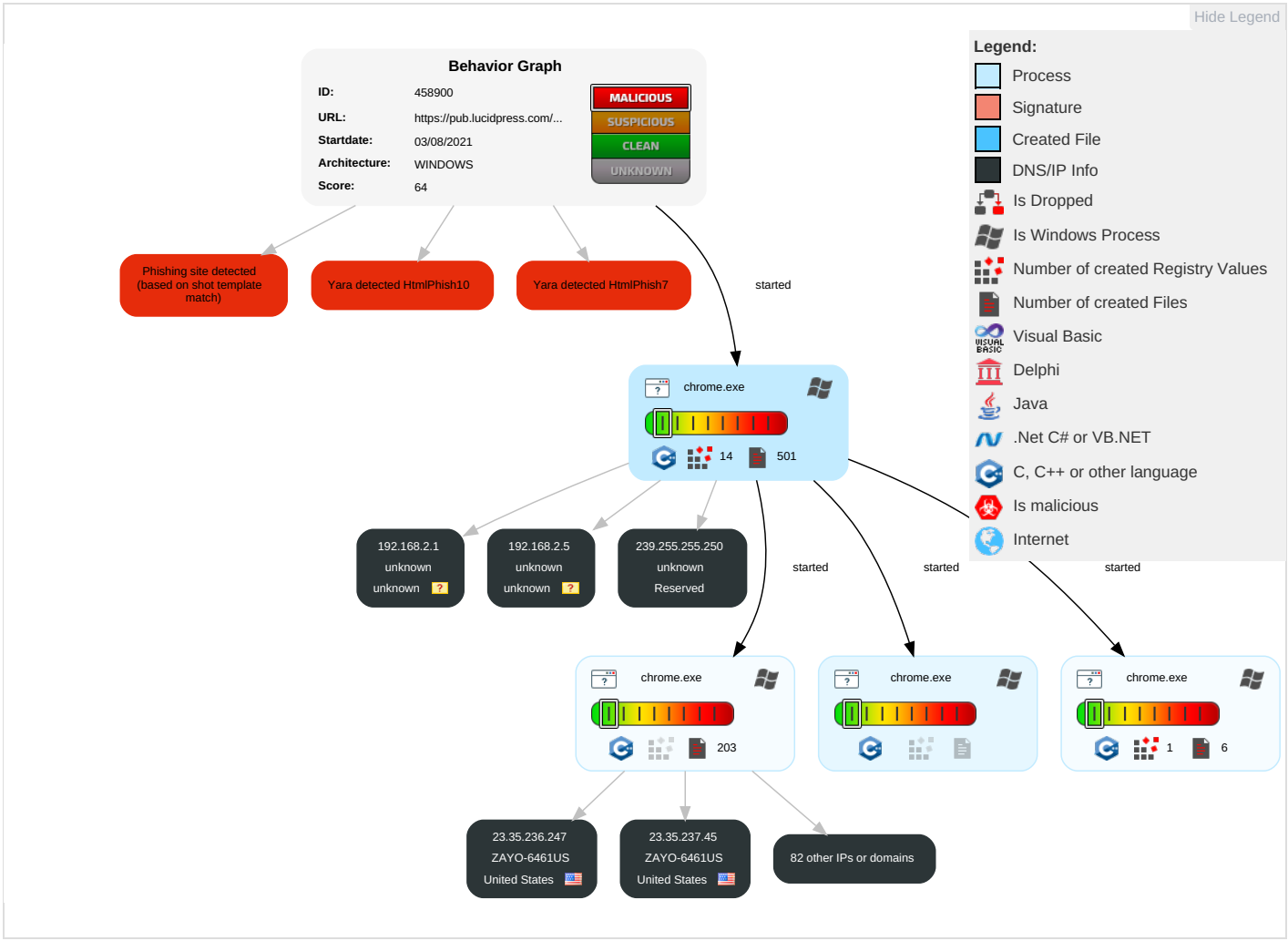
Yara detected HtmlPhish10

Yara detected HtmlPhish7

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	Imp
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mod Sys Part
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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Dev Locl

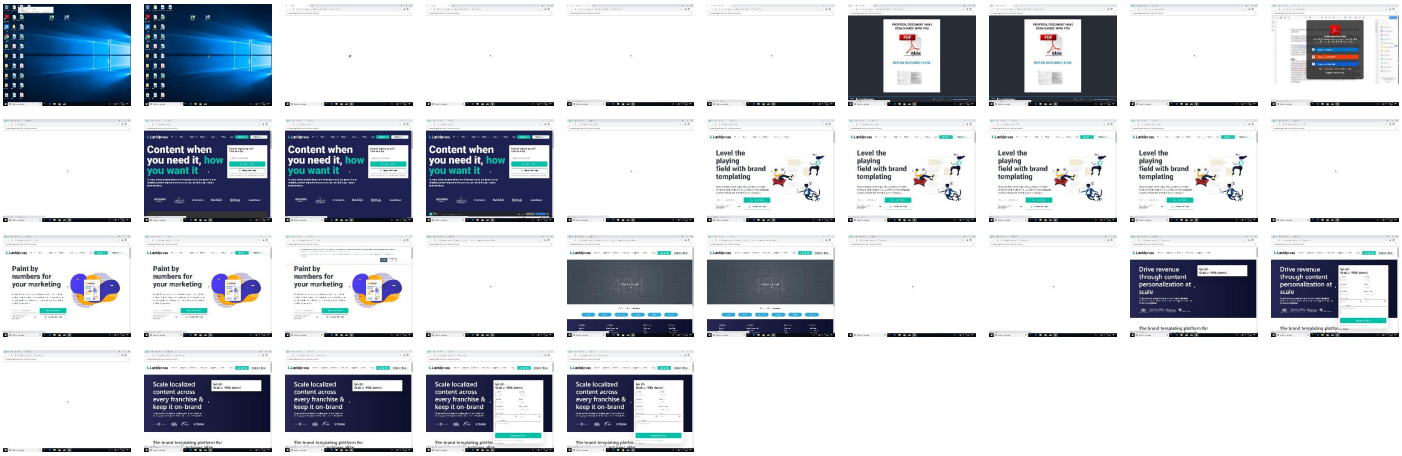
Behavior Graph

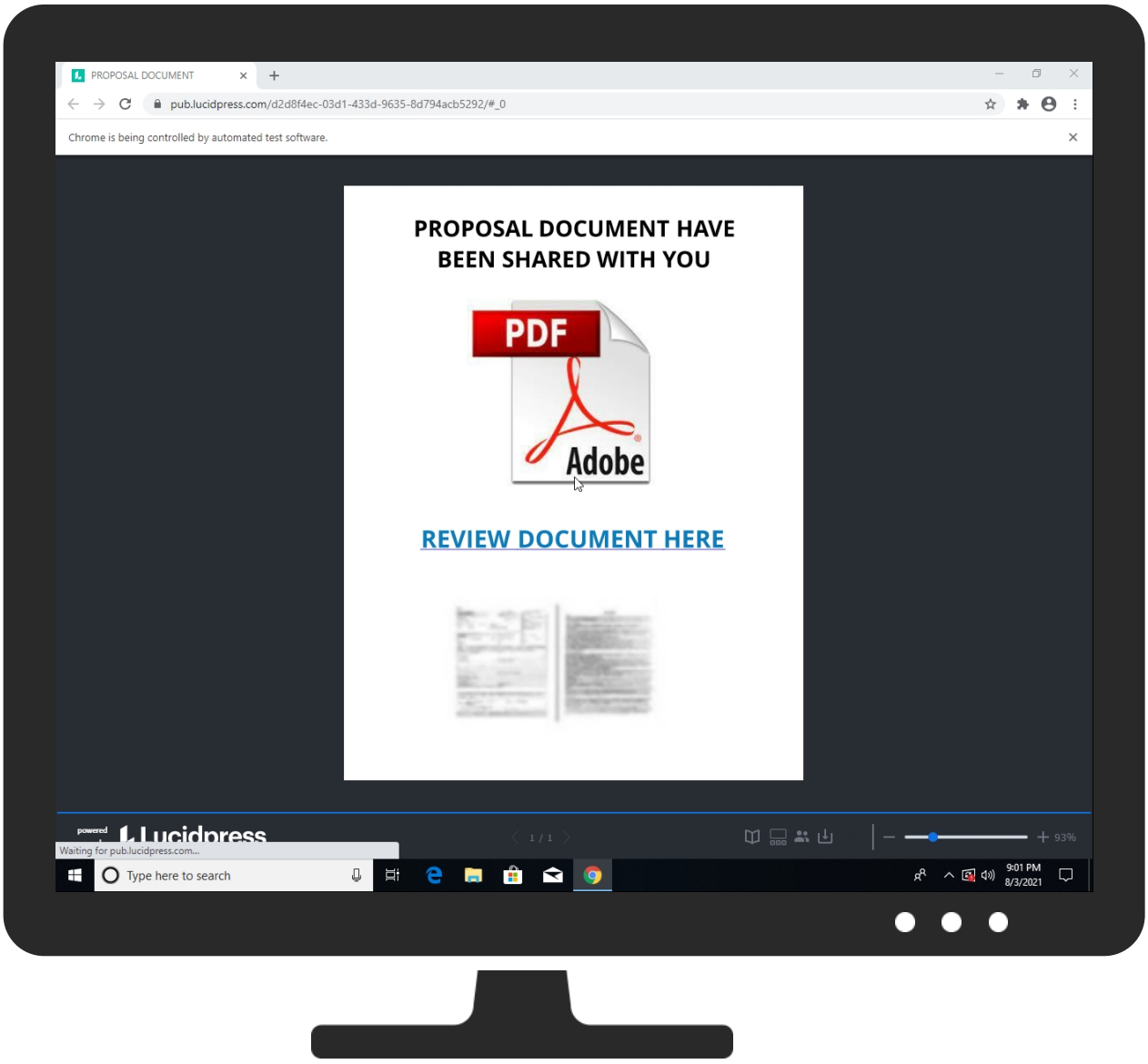


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://pub.lucidpress.com/d2d8f4ec-03d1-433d-9635-8d794acb5292/#_0	0%	Virustotal		Browse
http://https://pub.lucidpress.com/d2d8f4ec-03d1-433d-9635-8d794acb5292/#_0	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://js.hs-banner.com/19908047.js	0%	Avira URL Cloud	safe	
http://https://munchkin.marketo.net/munchkin.jsaD	0%	URL Reputation	safe	
http://https://scientificemployment.co.kr/	0%	Avira URL Cloud	safe	
http://https://scientificemployment.co.kr/files/d	0%	Avira URL Cloud	safe	
http://https://js.hs-analytics.net/analytics/1628017200000/19908047.js	0%	Avira URL Cloud	safe	
http://https://a.omappapi.com/app/js/api.min.js	0%	Avira URL Cloud	safe	
http://https://a.omappapi.com/app/js/webfont/1.5.18/webfont.js	0%	Avira URL Cloud	safe	
http://https://analytics.app.preprodpress.com	0%	Avira URL Cloud	safe	
http://https://app-ab23.marketo.com(_https://app-ab23.marketo.com	0%	Avira URL Cloud	safe	
http://https://scientificemployment.co.kr/#	0%	Avira URL Cloud	safe	
http://https://www.lucidpress.comh	0%	Avira URL Cloud	safe	
http://https://analytics.preprodchart.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.lucidpress.com/pages/tour	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.19.155.83	unknown	United States		13335	CLOUDFLARENETUS	false
216.58.208.162	unknown	United States		15169	GOOGLEUS	false
173.194.76.154	unknown	United States		15169	GOOGLEUS	false
192.28.144.124	unknown	United States		15224	OMNITUREUS	false
204.79.197.200	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.21.81.131	unknown	United States		13335	CLOUDFLARENETUS	false
13.226.247.126	unknown	United States		16509	AMAZON-02US	false
13.226.247.25	unknown	United States		16509	AMAZON-02US	false
54.144.101.159	unknown	United States		14618	AMAZON-AESUS	false
157.240.17.35	unknown	United States		32934	FACEBOOKUS	false
52.204.216.64	unknown	United States		14618	AMAZON-AESUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
216.58.208.129	unknown	United States		15169	GOOGLEUS	false
52.84.148.55	unknown	United States		16509	AMAZON-02US	false
104.18.21.191	unknown	United States		13335	CLOUDFLARENETUS	false
173.222.108.210	unknown	United States		20940	AKAMAI-ASN1EU	false
142.250.180.166	unknown	United States		15169	GOOGLEUS	false
142.250.184.106	unknown	United States		15169	GOOGLEUS	false
108.177.126.157	unknown	United States		15169	GOOGLEUS	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false
185.33.220.244	unknown	Netherlands		29990	ASN-APPNEXUS	false
142.250.180.163	unknown	United States		15169	GOOGLEUS	false
142.250.180.164	unknown	United States		15169	GOOGLEUS	false
209.85.226.8	unknown	United States		15169	GOOGLEUS	false
142.250.184.99	unknown	United States		15169	GOOGLEUS	false
142.250.184.110	unknown	United States		15169	GOOGLEUS	false
13.248.245.213	unknown	United States		16509	AMAZON-02US	false
3.209.16.152	unknown	United States		14618	AMAZON-AESUS	false
216.58.206.40	unknown	United States		15169	GOOGLEUS	false
142.250.180.138	unknown	United States		15169	GOOGLEUS	false
216.58.205.77	unknown	United States		15169	GOOGLEUS	false
216.58.206.42	unknown	United States		15169	GOOGLEUS	false
52.4.147.50	unknown	United States		14618	AMAZON-AESUS	false
216.58.209.35	unknown	United States		15169	GOOGLEUS	false
104.19.148.8	unknown	United States		13335	CLOUDFLARENETUS	false
13.107.42.14	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
18.156.0.31	unknown	United States		16509	AMAZON-02US	false
23.35.237.45	unknown	United States		6461	ZAYO-6461US	false
89.187.165.193	unknown	Czech Republic		60068	CDN77GB	false
52.222.135.75	unknown	United States		16509	AMAZON-02US	false
35.244.174.68	unknown	United States		15169	GOOGLEUS	false
104.18.22.52	unknown	United States		13335	CLOUDFLARENETUS	false
108.174.11.37	unknown	United States		14413	LINKEDINUS	false
54.84.30.144	unknown	United States		14618	AMAZON-AESUS	false
74.125.8.72	unknown	United States		15169	GOOGLEUS	false
142.250.184.66	unknown	United States		15169	GOOGLEUS	false
50.17.238.117	unknown	United States		14618	AMAZON-AESUS	false
104.18.10.207	unknown	United States		13335	CLOUDFLARENETUS	false
80.67.82.65	unknown	European Union		20940	AKAMAI-ASN1EU	false
69.173.144.139	unknown	United States		26667	RUBICONPROJECTUS	false
34.255.138.57	unknown	United States		16509	AMAZON-02US	false
104.17.71.176	unknown	United States		13335	CLOUDFLARENETUS	false
104.17.210.204	unknown	United States		13335	CLOUDFLARENETUS	false
157.240.17.15	unknown	United States		32934	FACEBOOKUS	false
13.226.247.99	unknown	United States		16509	AMAZON-02US	false
185.64.189.110	unknown	United Kingdom		62713	AS-PUBMATICUS	false
13.226.247.51	unknown	United States		16509	AMAZON-02US	false
52.58.229.235	unknown	United States		16509	AMAZON-02US	false
69.16.175.10	unknown	United States		20446	HIGHWINDS3US	false
13.226.247.53	unknown	United States		16509	AMAZON-02US	false
141.226.228.48	unknown	Israel		200478	TABOOLA-ASIL	false
142.250.74.193	unknown	United States		15169	GOOGLEUS	false
172.217.18.99	unknown	United States		15169	GOOGLEUS	false
142.250.184.72	unknown	United States		15169	GOOGLEUS	false
70.42.32.95	unknown	United States		22075	AS-OUTBRAINUS	false
3.120.13.220	unknown	United States		16509	AMAZON-02US	false
194.163.158.153	unknown	Germany		6659	NEXINTO-DE	false
99.81.27.250	unknown	United States		16509	AMAZON-02US	false
104.16.93.80	unknown	United States		13335	CLOUDFLARENETUS	false
216.58.208.174	unknown	United States		15169	GOOGLEUS	false
142.250.184.78	unknown	United States		15169	GOOGLEUS	false
142.250.184.34	unknown	United States		15169	GOOGLEUS	false
142.250.180.118	unknown	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.78.251.22	unknown	United States		16509	AMAZON-02US	false
87.248.118.22	unknown	United Kingdom		203220	YAHOO-DEBDE	false
18.197.253.20	unknown	United States		16509	AMAZON-02US	false
52.84.148.125	unknown	United States		16509	AMAZON-02US	false
54.74.23.153	unknown	United States		16509	AMAZON-02US	false
96.7.53.23	unknown	United States		16625	AKAMAI-ASUS	false
34.98.64.218	unknown	United States		15169	GOOGLEUS	false
52.84.148.3	unknown	United States		16509	AMAZON-02US	false
23.35.236.247	unknown	United States		6461	ZAYO-6461US	false
13.226.247.9	unknown	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458900
Start date:	03.08.2021
Start time:	21:00:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://pub.lucidpress.com/d2d8f4ec-03d1-433d-9635-8d794acb5292/#_0
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@52/364@0/87
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.lucidpress.com/ • Browse: https://www.lucidpress.com/pages/tour • Browse: https://www.lucidpress.com/pages/individuals • Browse: https://www.lucidpress.com/pages/business • Browse: https://www.lucidpress.com/pages/industries/associations • Browse: https://www.lucidpress.com/pages/industries/finance • Browse: https://www.lucidpress.com/pages/industries/franchises
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:01:53	API Interceptor	3x 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 GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	183060
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	3072:0tdeYPiuWAVtlLBGbtdeYPiuWAVtlLBGbtdeYPiuWAVtlLBGm:0rec7VDBGbrec7VDBGbrec7VDBGm
MD5:	7DAFFD77F2D6E43937A4AF91891D572A

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
SHA1:	B00718D20556FAB59D4F815460CE0E657707B125
SHA-256:	D9A5468356659DD4E681FBBEC4EBFECDE08400FC5432BAF92553813A62336A3D
SHA-512:	7E8C0EA36B41D44B914D409F9FD2B1E8BB0F0BD617670E274452E7CF56E61CEC68CC550BA817D9654B6F5C85A0135C45B5ECECC73E61EA0A4D2642D89723198
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$...._Y..Y`&..s.1.....s.{...,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_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):	978
Entropy (8bit):	3.157542238246964
Encrypted:	false
SSDEEP:	12:L5kPlE99SNxAhUe0eN5kPlE99SNxAhUe0ejIe5kPlE99SNxAhUe0et:L5kPcUQUfeN5kPcUQUfe35kPcUQUfet
MD5:	00B10EC825DACB963816592063668FF1
SHA1:	AD81245B6A5461B8A067CBBAD7DA7D62FADBF7A0
SHA-256:	1F8C31813427434659D1C23191D847BAAAEFC32F60B28C0343F5948F2824A43C
SHA-512:	23AE6D0FA765C57358850F7079CF225FFFB739E08457806C1773EE8A78CCAD6843759A4CCB5B20562AE8E25DC3C3C4F39D7E23B9DC968CD30AEF82DA8E4AC03
Malicious:	false
Reputation:	low
Preview:	p..... .....u...(..... .....T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...p..... .....(..... .....T'._.....$.....\...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.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...p..... .....D.....(..... .....T'._.....$.....\...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.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0d39f03c-ed4d-4c3d-aede-f87a0582b81a.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):	174336
Entropy (8bit):	6.07934881535559
Encrypted:	false
SSDEEP:	3072:DqNGaYTJQE+mugy9+QV1T7IRwdfLSNPzFcbXafIB0u1GOJmA3iuRw:GoxaV+QfT7GSmhhaqfIlUOoSiuRw
MD5:	9AEACCD437B18414ECA802C6F49D4B61
SHA1:	1D1603D5B0F5B176E9BEBEAAE38F2B7CCBBBD6D3
SHA-256:	A0D90C504AF817AD43C724B80B4B4D9873328964016D4C827404F4DE18C03078
SHA-512:	A73C448E4975D25BF89F2D6E7642504CACFE6FFEACF812733FC53120F52C381E6DA03BC7F5205EC1343D2C62628E611820616FF230CFAC1FE40DE3E0D2C1B18
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":1.628049702412018e+12,"network":1.628017303e+12,"ticks":6202473572.0,"uncertainty":4556111.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\49629bd8-7b1f-42e8-bc05-ea3d8cf393aa.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7497091420802264
Encrypted:	false
SSDEEP:	384:hX9SSsvpkvMSVHZW1Nqrfvem3Nm0pHk9Gx4rTwCUx94ow7rjimvUTAKm2VOgUmNQ:N6WRhCE19Qevsu0M/z2GKs2Wxw
MD5:	80932DFBC63167699512FA433F1E7563
SHA1:	60E619B29F8C970F0A757225D6A36077B5BD8044
SHA-256:	DD80EC15D52AC1E17F25CA16FAFE55FCEC2516CAC3AAE5CDCE52F594540A89C7
SHA-512:	D07753C3ED82267328205787DEA14E27162CF7ED7003919603A88FF0EE78EAD30B872EB59A8F2C14874F5F782FC2DF27AAC68A7F12C4FC022539C17F808FAFCE

C:\Users\user\AppData\Local\Google\Chrome\User Data\49629bd8-7b1f-42e8-bc05-ea3d8cf393aa.tmp	
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....A8.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\5ffc311d-58cb-48ef-bf73-bb9aee277a15.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):	174337
Entropy (8bit):	6.0793482570117545
Encrypted:	false
SSDEEP:	3072:Dh0GaYTJQE+mugy9+QV1T7IRwdfLSNPzFcbXafIB0u1GOJmA3iuRw:tFxaV+QfT7GSmhhaqfIlUOoSiuRw
MD5:	104AA89442362FE1FD215E1E5D7D7981
SHA1:	831BEA9B2156D0E7E53B8C596B51E60646A24379
SHA-256:	945CA3EF6EB877CD91565E489D3486E0A75404806F60F634F8E43FE50EB55711
SHA-512:	4DFD77CCA3786F3FCCECADF884C4A060FE5F146DC69C38ED38BF71A29E38BB26F0E53BADE8B2832904C5794B312832493E9437E87F3DC092AF40D745D1D29F B
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":1.628049702412018e+12,"network":1.628017303e+12,"ticks":6202473572.0,"uncertainty":4556111.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\66e0bca5-4287-422b-bbdb-c177b39e77d4.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):	174337
Entropy (8bit):	6.079348364395185
Encrypted:	false
SSDEEP:	3072:hcTGaYTJQE+mugy9+QV1T7IRwdfLSNPzFcbXafIB0u1GOJmA3iuRw:CixaV+QfT7GSmhhaqfIlUOoSiuRw
MD5:	C6785873BC952D7C7F2584C524455791
SHA1:	A67510A154C14C63A80C848E5E354E390AA490E5
SHA-256:	7CDD70FB075ECEE8DAF41C6AE3A0EC3859F594DBC7B2C1A0E28AA05C7C1C4CD4
SHA-512:	42F2D4D5575BEE598D1276C4147D4FCFAD4958E8935C20796C3096926D71262CDA1120A9B7446C017625FB64106D770202E18B347D0D6CAB7CC3D3F8310B903F
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":1.628049702412018e+12,"network":1.628017303e+12,"ticks":6202473572.0,"uncertainty":4556111.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016204142"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\75a3d904-3c3d-4273-9e04-556fb5245e0a.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):	174337
Entropy (8bit):	6.0793493222664585
Encrypted:	false
SSDEEP:	3072:hvkGaYTJQE+mugy9+QV1T7IRwdfLSNPzFcbXafIB0u1GOJmA3iuRw:JVxaV+QfT7GSmhhaqfIlUOoSiuRw
MD5:	1905048C889A53574F405F06290CF0F8
SHA1:	43A93899821D381041A304E36E1EEE9048F2E0E3
SHA-256:	A11FDAAFC186551D2B2114C994F34EC902F1FF764FA20FBBEBEA0A7F66953C89
SHA-512:	BAD55C159C34D785961254A46453518C53C13D49724B942EB410A5FA0E3672F1249B891F0C97D74015248F1285F248010E2F48B595D4934EC279CDDE957254BA
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\75a3d904-3c3d-4273-9e04-556fb5245e0a.tmp	
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.628049702412018e+12,"network":1.628017303e+12,"ticks":6202473572.0,"uncertainty":4556111.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016204142"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\80ebe639-ac0a-44c8-898e-401dd859235f.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):	174337
Entropy (8bit):	6.079349148069858
Encrypted:	false
SSDEEP:	3072:D8JGaYTJQE+mugy9+QV1T7IRwdfLSNPzFcbXafIB0u1GOJmA3iuRw:lkxaV+QfT7GSmhhaqfIlUOoSiuRw
MD5:	7543E5FF766110938FBC29FE3FDFD0E3
SHA1:	BACD32E00800E4559A70F2125AE3DAC32BFE02BA
SHA-256:	283062E3FDFDEA9D16D91B9B82E56C200A810C858422B5179391125A8E7C09CD
SHA-512:	81A48BEFA7F30C8528AFE323F0E3CAC39AFD93022FBB8E8E1BE5521BF94641F449D0D54D83768F571AB1D4A3EA8F22AFD8DA3AB1B75EE453DA1F2DBE13EAD5BB
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":1.628049702412018e+12,"network":1.628017303e+12,"ticks":6202473572.0,"uncertainty":4556111.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

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):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0896bf0c-6ea7-43e9-a1b3-a2128c708dc3.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):	6012
Entropy (8bit):	5.198315969232373
Encrypted:	false
SSDEEP:	96:n2Cfki9ZpnM8XqcKI3ok0JCKL8XvkPZ1jqkqSjgbOTQVuwn:n2C39Z+mqcU4KskPZckN2
MD5:	95394BC21A328BD11211D9528735D113
SHA1:	22142B297EAE245434C4E8F7B10D36680DD9D3E9
SHA-256:	3C53F57F98F375D493FD37287DA1908CDF2F4F3050BC6906C68E145CBA14011B
SHA-512:	5EFB8D1A78EF86E6FC2BBEDD464544FA2A6E8AD3E4B1863B64D80AB13A2121B03202087A52334AC85C56FC4BDFE39D20A34E31B44771BCD0AB3430CA5EB1A47B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0896bf0c-6ea7-43e9-a1b3-a2128c708dc3.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523297186376","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1c673b59-d464-4c6c-9a6a-3254a05644dc.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):	5228
Entropy (8bit):	5.607632400315869
Encrypted:	false
SSDEEP:	96:bUtDUwU7k6UWjUmUrU8SeU1eieUOUUEUNUgU18Ub0UdUrUgIUb0U2UmDKUeqqUMT:bUtDUwU46UWjUmUrU8SeU4UOUUEUNUgb
MD5:	C00624945A9CFCEFA21CA1DDDF5E31D8
SHA1:	283F89FA27D7950EA96CB3E336B08CE48DC1BEF6
SHA-256:	E74FC961E06980C20F049BAFF935364CF1A11613E19A98E7B2D9B2E086E63785
SHA-512:	5FB6C2BE9E937999DBBD226C9E02C60AB79548B86B580BA244309F294CEFACD7F07C81FA2EFCA1B2913283FE789945CE4946F192DF72E52C12F097C422C0505
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659585849.14027,"host":"D3hv38PxEHV/fYjHSqf6awTT1q1h/DzUiyZ/y6cgiQQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049849.140274},{"expiry":1643829833.861795,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049833.861801},{"expiry":1659585849.264944,"host":"F166S2RufctU1mcwgRXSCljJCTsKa6xzpFhpPQImBhQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049849.264951},{"expiry":1659585848.991503,"host":"GRkr4wgfnR5GxQsC3l3RUCOe9GM6JratmY45dCfHG/g=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049848.991508},{"expiry":1643601855.257417,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049855.257423},{"expiry":1659585855.020599,"host":"IjdRz/ABIlneFZw1/zlKojo7PKLoVqcc+q9YP4CDk8k=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ea4cc7c-5318-4232-ad03-8a49de009f05.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):	6038
Entropy (8bit):	5.202125156890443
Encrypted:	false
SSDEEP:	96:n2Cczi9ZpnM8XqcKIzok0JCKL8XvkPZ1jdkO4A65bOTQVuwn:n2CV9Z+mqcQ4KskPZrkO4tZ
MD5:	7B6152C2520F586A540FE347C100BBA5
SHA1:	4840FA55955B0ED0D1A151B22B81B65D2414D07C
SHA-256:	2E87A6F39431EF430C5EB3020282110609849AF960D2DDCFC7E97365F4CABC96
SHA-512:	2527ECD6619D78E9C71B0E148A7F2FC9447612D0BF7F0FBF9DFF699ACBEE877275DECF24A227FBA28CB6F4579A2FCCD9B576191209460E8303D0D2201C0406C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523297186376","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3644b03d-5edb-422f-a87a-23d40977b851.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):	2546
Entropy (8bit):	5.600389144025011
Encrypted:	false
SSDEEP:	48:YjU9YdUneUu6UUhbeU58UeUYeKUWYUdqPeUerReUaUefxL6wUmtsYULkpUenw:mU96UneUzUUEU58UeUbKU5UoPeU8eUaw
MD5:	B753EABD3517723AD02294D18F309D1A
SHA1:	BAF7E1E07AB60969E0EC7FA061E5C101E89B67FA
SHA-256:	629A6B606E091E5B55F88492E4D747FD211F8F3BF47681CE7C52DBF85895FC8B
SHA-512:	04EDF2E0C235E78F80E29B461E06E5DBD7AE6643CA624DAD65A9DD2543E1BEF927375836665EAD8A3A0DFDD6AB726C9223420CEDBE14671B4EEEA97AF7BBE1A6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3644b03d-5edb-422f-a87a-23d40977b851.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1659585707.783698,"host":"F166S2RufctU1mcwgRXSCljJCTsKa6xzpFhpPQImBhQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049707.783706},{"expiry":1659585706.651585,"host":"GRkr4wgfnR5GxQsC3l3RUCOe9GM6JratmY45dCfHG/g=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049706.651592},{"expiry":1638936106.665938,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628049706.665944},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1659585713.054484,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049713.05449},{"expiry":1659585706.947854,"host":"XvNPEzIWAUnPn1qSae0pmIEXIWQxJ7crkzVU1FGq07s=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\524eb97b-cc46-4d43-befb-1833d443708b.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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\59cca78f-08dd-4d57-80b8-2432a40ca9bc.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):	5225
Entropy (8bit):	5.609684160638959
Encrypted:	false
SSDEEP:	96:yUSDUnUj6UwUaUTUneU9MieUNd5UUEUYUwU18Up0UfUpUgIUb0U2UmDKUeHUOgUy:yUSDUnUj6UwUaUTUneU98UNd5UUEUYUf
MD5:	C56AE01D6BC283E194479FF5BC3C08C0
SHA1:	371B024790226D48D7AF16B674F77D1DA8587225
SHA-256:	E53F9FA350D8EED28A6C40728D2095F8ED7C334D8EBC6C39E6C1684A0CCAF1AD
SHA-512:	08C0D435374A7DAE8E77F292CD885C9BB232A6ADA088A2B13B1BBF30C894D26C16E6E8A8DF6A9753598064FA8DA10F70E91BC8AD3B2160EDDC01E146F0B9E5CF
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659585842.785156,"host":"D3hv38PxEHV/fYjHSqf6awTT1q1h/DzUiyZ/y6cgiQQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049842.785163},{"expiry":1643829833.861795,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049833.861801},{"expiry":1659585843.283188,"host":"F166S2RufctU1mcwgRXSCljJCTsKa6xzpFhpPQImBhQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049843.283194},{"expiry":1659585843.166624,"host":"GRkr4wgfnR5GxQsC3l3RUCOe9GM6JratmY45dCfHG/g=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049843.16663},{"expiry":1643601836.922456,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049836.922462},{"expiry":1659585845.322808,"host":"IjdRz/ABIlneFZw1/zlKojo7PKLoVqcc+q9YP4CDk8k=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\65eab0cd-03e8-4527-a16c-ecc0b7194713.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):	5787
Entropy (8bit):	5.1908485233699135
Encrypted:	false
SSDEEP:	96:n2Cfki9ZpnM8XqcKIyok0JCKL8XvkPZ1R7bOTQVuwn:n2C39Z+mqcX4KskPZXv
MD5:	6A70532BFD395EDE0EDA7232788E4A3E
SHA1:	F9ED6335C3AA7ADA25CADF91B3517369E24FAEF5
SHA-256:	1D05E9F1DA873B4393071C23D184F8BC02D2F7B4570A800ADE247B140D104481
SHA-512:	8502E8C9B26A59EDA892E8BC133C37D6C8D07D1901B55FFB33CFD2B553C1CF559EBD6EF82B65380979AD438112B3039C21B10E3D57E0F4EE18236FAAC8AA470
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\65eab0cd-03e8-4527-a16c-ecc0b7194713.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523297186376","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6def4a21-c78d-445a-9272-2d268b1669e6.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):	2546
Entropy (8bit):	5.600154764573282
Encrypted:	false
SSDEEP:	48:YjU9YdUneUu6UUhbeU58UeUYeKUWYUdqPeUerReUaUefxL6wUmLjsYUpxUenw:mU96UneUzUUEU58UeUbKU5UoPeU8eUal
MD5:	40E42B4CC162851901284E6167A14FF0
SHA1:	2E6D4A600BB61279C9DA52C6205DE520131B0203
SHA-256:	E7B82507CBF37E7A72FC75E71E252729001A10C6F6A8078D1B346916E3111A75
SHA-512:	E21073B7A4489D152AC07E3639DBCE48804107069439DC135466BD481683164225CA06D7529524C311D4EC4C88D47AAC89AF47A0129B1CD603B4D855AD09680A
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659585707.783698,"host":"F166S2RufctU1mcwgRXSCljJCTsKa6xzpFhpPQImBhQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049707.783706},{"expiry":1659585706.651585,"host":"GRkr4wgfnR5GxQsC3l3RUCOe9GM6JratmY45dCfHG/g=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049706.651592},{"expiry":1638936106.665938,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628049706.665944},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1659585713.054484,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049713.05449},{"expiry":1659585706.947854,"host":"XvNPEzIWAUnPn1qSae0pmIEXIWQxJ7crkzVU1FGq07s=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\74723681-1cb8-49bc-82af-99b10bfbea5d.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):	2211
Entropy (8bit):	5.600542298710451
Encrypted:	false
SSDEEP:	48:YjU9YdUneUu6UUhm8UeUaseKUeQYUdqPeUerReUaUefxL6wUmkUenw:mU96UneUzUUQ8UeUa3KUgUoPeU8eUaUy
MD5:	92DED708CE0239F9E7A184EBECD861CF
SHA1:	8AE8439DDE96093E26C05778178C722A21C3DA46
SHA-256:	C0B504E33478D1B3275A6DC22521886CE0685249D2087A20D8306557BBCC8E85
SHA-512:	CA0A62950F55D56089714605D73DE4A88EA5D032C64D6A938C1CCDAE5C86B0852157C060094A30AFDF6F16185ACA47439A4C43274B25B2EDDA39D6E308BD43E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659585707.783698,"host":"F166S2RufctU1mcwgRXSCljJCTsKa6xzpFhpPQImBhQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049707.783706},{"expiry":1659585706.651585,"host":"GRkr4wgfnR5GxQsC3l3RUCOe9GM6JratmY45dCfHG/g=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049706.651592},{"expiry":1638936106.665938,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1628049706.665944},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1659585706.947854,"host":"XvNPEzIWAUnPn1qSae0pmIEXIWQxJ7crkzVU1FGq07s=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049706.947861},{"expiry":1638936106.352488,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\77661c9f-5331-4c21-8294-2c7f39db1e96.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):	4893
Entropy (8bit):	5.608082018211957
Encrypted:	false
SSDEEP:	96:qUpUEUX6UcU8UoUpieUwSieUMUUEUyjUa+8U30UY5U3UCIU1U+KULgU6UVFUX7Px:qUpUEUX6UcU8UoU8eUxUMUUEUyjUWU3g
MD5:	D5FB10493A9C20F1037CD9D28A0112AB
SHA1:	F61940EBCB4DE1D1AAADC00A6641D98143AF89B8
SHA-256:	F69D4885F6738A6EC252103784542C517D81CC634F4B074A25D6B2189EDAFA44
SHA-512:	06F93D5AD89F5607BC690BDAAC89503BE8FDC3B74D03B09CC2998AA41ABF2C6EDBB425A1E6868C4BB57C4E2CE92AA1F3CD0CFCF6A0D98A86B9607367B08F69F7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\77661c9f-5331-4c21-8294-2c7f39db1e96.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1659585807.781634,"host":"D3hv38PxEHV/fYjHSqf6awTT1q1h/DzUiyZ/y6cgiQQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049807.781638},{"expiry":1643829773.600495,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049773.600499},{"expiry":1659585808.714104,"host":"F166S2RufctU1mcwgRXSCljJCTsKa6xzpFhpPQImBhQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049808.714111},{"expiry":1659585814.478917,"host":"GRkr4wgfnR5GxQsC3l3RUCOe9GM6JratmY45dCfHG/g=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049814.478921},{"expiry":1643601809.908345,"host":"HS0xQK8RrrSZ/KdSgKIC7bLU+xijlimr9JuWvTPbfkE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1628049809.908349},{"expiry":1659585809.460724,"host":"IjdRz/ABIlneFZw1/zlKojo7PKLoVqcc+q9YP4CDk8k=","mode":"force-https","sts_include_subdomains":false,"st

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\77dc4fb3-8486-4fd5-b357-265bc266a040.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):	8081
Entropy (8bit):	4.848149424764463
Encrypted:	false
SSDEEP:	192:JOXGDHzkRT5E+t9tK5NaZzbBFiIj6QSJ0+CEu96VFB6Mz3tJGZ+8kV1OqS6rxKHq:JOXG7oRT5E+t9tK5NaZzbBFdj6QSJ0+X
MD5:	DD3C657322463EC20686A0F30EC93739
SHA1:	5AF3317B5CC31EA1867A4CCF7D960C7D660975B1
SHA-256:	1FA201E2F8128001FAA0DD2FE4DC3CCBE9F43B4B8AF3D43F864BE58049B78A98
SHA-512:	055383C335848907D6572E01D801AD60624EF364EDF3E59CA5EA1C76954D1A7B216CB099389F00B167BEFBD9FC0D5EAC9146D2F2DF7F2FE743F59B181A65F5F
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.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":"13275115302435936","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275115302471104","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13275115302678932","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13275115302678936","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7bd1043c-c264-47c9-9d92-51c69ff2ad13.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):	5129
Entropy (8bit):	4.982627883306648
Encrypted:	false
SSDEEP:	96:n2CmHX9pcKIjok0JCKL8XvkPZ1R7bOTQVuwn:n2CS9pc84KskPZXv
MD5:	BAB687231B7692574788D0469135DAE3
SHA1:	5E7E00D80BF104C59A3261E027C6EBD658166E71
SHA-256:	8BF69ADF3BFBD3DF12566A140DD8B7E77D5B353C9B6F6502BC49BAEE38BD6B6E
SHA-512:	1EBC16AD7EC6F459F93EA8CAFDBD565CA6A89277C32BD2705457092E8308693F02D9B683AEFE834EC5AE7DA957F3D96E6E275A992AB4148632A05F6F1FA6ADA5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272523297186376","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8ba8b74b-03ec-485d-9441-154b11d38f82.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.536068096233457
Encrypted:	false
SSDEEP:	384:2IftNLl5fXR1kXqKf/pUZNCgVLH2HfD9rUUHGJnT+w5R04i:JLlNR1kXqKf/pUZNCgVLH2HfprUYGJnA
MD5:	9BF92CF41BDF0BB4BE0654A8CBFD2FD4
SHA1:	34B9F85A1CBA3DF012539FA5F56D50E990EA6ACB
SHA-256:	F2ECF64CB2F387753F9FCC934C6DF578B98289A75CE4237F0D964F3C263FECFF
SHA-512:	D403E53B84C881E6910FE29BAA6CE90A88CE028B943BA117E501C5FF992C5FF546B067442C2437F81C54306332B3B57FEC2DE45DC161C2A82C56E880EE798D6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8ba8b74b-03ec-485d-9441-154b11d38f82.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13272523296779336","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\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2243685572240235
Encrypted:	false
SSDEEP:	6:mTEmYN4q2PWXp+N23iKKdK9RXXTZIFUtpa3bJZmwPazDkwOWXp+N23iKKdK9RXXH:qY4va5Kk7XT2FUtpaLJ/PazD5f5Kk7XH
MD5:	5A2E54D2E30DC4508E4258D8E42977E4
SHA1:	F29E8C42123EB0694E0F7B82C1FB12BC00541DD6
SHA-256:	98DD390C2F8DE7D4B4684AA9A5CEC6DAF3192EC2FAF76CDE7CF155BDFA6057D8
SHA-512:	8ADC0C31DB2E78B7035387561CBB245685A4E35496AD03767A3DB864F54C133A8C2A446E269B8A0B0ADE7BCAA49CF000D9D6D71B4A2FD412A34D2C0BB9EB0E26
Malicious:	false
Reputation:	low
Preview:	2021/08/03-21:01:53.988 1724 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-21:01:54.007 1724 Recovering log #3.2021/08/03-21:01:54.010 1724 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.oldNT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2243685572240235
Encrypted:	false
SSDEEP:	6:mTEmYN4q2PWXp+N23iKKdK9RXXTZIFUtpa3bJZmwPazDkwOWXp+N23iKKdK9RXXH:qY4va5Kk7XT2FUtpaLJ/PazD5f5Kk7XH
MD5:	5A2E54D2E30DC4508E4258D8E42977E4
SHA1:	F29E8C42123EB0694E0F7B82C1FB12BC00541DD6
SHA-256:	98DD390C2F8DE7D4B4684AA9A5CEC6DAF3192EC2FAF76CDE7CF155BDFA6057D8
SHA-512:	8ADC0C31DB2E78B7035387561CBB245685A4E35496AD03767A3DB864F54C133A8C2A446E269B8A0B0ADE7BCAA49CF000D9D6D71B4A2FD412A34D2C0BB9EB0E26
Malicious:	false
Reputation:	low
Preview:	2021/08/03-21:01:53.988 1724 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-21:01:54.007 1724 Recovering log #3.2021/08/03-21:01:54.010 1724 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):	318
Entropy (8bit):	5.228499845198612
Encrypted:	false
SSDEEP:	6:mTEq4q2PWXp+N23iKKdKyDZIFUtpaEzHJZmwPaEObDkwOWXp+N23iKKdKyJLJ:qL4va5Kk02FUtpaGJ/PaXbD5f5KkWJ
MD5:	F5DA1D4ABD0FC2BB568F31CA1155327E
SHA1:	D648E2C020BCCD1C962B72F3B65061E9AE263573
SHA-256:	83E28CF4D171E3A791468703847ECD4F55B47024F9F3247F9A1C52768D7D7A48
SHA-512:	CBE8F8A9897D722C0C4F3C3B12489ACDF7654208A07F291B96DC428ED1AC7BFC96FFC59721879623A59A9BA97361F4398E30981F51056CF753102A6CD6F4310E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-21:01:53.923 1724 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-21:01:53.951 1724 Recovering log #3.2021/08/03-21:01:53.952 1724 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old.. (copy)	
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.228499845198612
Encrypted:	false
SSDEEP:	6:mTEq4q2PWXp+N23iKKdKyDZIFUtpaEzHJZmwPaEObDkwOWXp+N23iKKdKyJLJ:qL4va5Kk02FUtpaGJ/PaXbD5f5KkWJ
MD5:	F5DA1D4ABD0FC2BB568F31CA1155327E
SHA1:	D648E2C020BCCD1C962B72F3B65061E9AE263573
SHA-256:	83E28CF4D171E3A791468703847ECD4F55B47024F9F3247F9A1C52768D7D7A48
SHA-512:	CBE8F8A9897D722C0C4F3C3B12489ACDF7654208A07F291B96DC428ED1AC7BFC96FFC59721879623A59A9BA97361F4398E30981F51056CF753102A6CD6F4310E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-21:01:53.923 1724 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-21:01:53.951 1724 Recovering log #3.2021/08/03-21:01:53.952 1724 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\04961dce325769e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	735
Entropy (8bit):	5.468310991899483
Encrypted:	false
SSDEEP:	12:QbhjaSRhd+FsIVUlN+bhjaSRhc+vFsIVo+bhjaSRh3LUIFsIVkX7:chjNvdxIVUlNyhjNvZSIVoyhjNv3LUrn
MD5:	825C2E40ED7474C7FEBC97C26FEF28EE
SHA1:	495F7116AEDC898E05501C6669508E7C49F50F4A
SHA-256:	38A4B18AC3837B1F43384E5179EDD4D706EBCA69EAF448354CFE02C26670A96A
SHA-512:	C10ABE718E70049EF5C1E06A1DE9067ED6AE7E6D275E160B7C2BA4AB31F27093CBC60EECF7A4568B9C5FFB0E8B17B5904B07E6293CE822BFE8F2BD168EC2C925
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q.....J....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/dialog-polyfill.js?qwihau .https://lucidpress.com/...,J'/.....x5.....bx...../..K5....@.....iOPk...c..A..Eo.....Q..&.....A..Eo.....0\r..m.....q.....J....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/dialog-polyfill.js?qwihau .https://lucidpress.com/...-J'/.....iY.....bx...../..K5....@.....iOPk...c..A..Eo.....|%_.....A..Eo.....0\r..m.....q.....J....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/dialog-polyfill.js?qwihau .https://lucidpress.com/y.r-J'/.....q.....bx...../..K5....@.....iOPk...c..A..Eo.....S.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0533db396c0afa88_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	687
Entropy (8bit):	5.614241223131611
Encrypted:	false
SSDEEP:	6:mvYGLZwjD+SVhtGTvYV9lHk+IM5n/K6tWvYGLZwjD+SVhtGQVYYlHk+IM5nLRK6Y:+2lkMLU2hVpkMxrU2l4TkMv
MD5:	3C3E935C9CD83E2EC29739A6218473A1
SHA1:	AEFCE462D7E9358C06BCB9912A616130828646AA
SHA-256:	DDEB646CDE40648304A7D5B765C9E06689FA5F7518C94EC5BF8A311427DBB33D
SHA-512:	E55AB1B8769B901F5AD430544438E4345921A09316A6E1A8DDFC23834E65934195DF6A6FEE070FE75AFA1C9ED96B1DF62AC6ABB432C979736C1CD05763E77AC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....n....._keyhttps://www.lucidpress.com/pages/misc/jquery-extend-3.4.0.js?v=1.4.4 .https://lucidpress.com/.!.,J'/.....)3.....7.....k.e.3.NZ.Ap!.....1....&..A..Eo.....].....A..Eo.....0\r..m.....a.....n....._keyhttps://www.lucidpress.com/pages/misc/jquery-extend-3.4.0.js?v=1.4.4 .https://lucidpress.com/.(.-J'/.....W.....7.....k.e.3.NZ.Ap!.....1....&..A..Eo.....N.....A..Eo.....0\r..m.....a.....n....._keyhttps://www.lucidpress.com/pages/misc/jquery-extend-3.4.0.js?v=1.4.4 .https://lucidpress.com/..m-J'/.....o.....7.....k.e.3.NZ.Ap!.....1....&..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0acaaaadc4c914e9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1458
Entropy (8bit):	5.820536291512428
Encrypted:	false
SSDEEP:	24:olSJqdeS+tJq5efBtJqCe/JqnTewABJqF7eHPJq3:HJqdbEJq56JqCSJqnTTABJqF7IPJq3
MD5:	97350EDA3470D94EF4270764BF4320E9
SHA1:	7B96EFFD86D0B4051F817D13861421B091001C5E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0acaaaadc4c914e9_0	
SHA-256:	46D7EB4DA5375AF9111EE8C57F18F582B2CD65591C1B8301C71BBDD041E4203F
SHA-512:	7E08B200F801081050D0198417336065180E871F5CF84EDF2464703ABE780751D9C28F279C31181E51D706E8D7A51C5239C11D88E0A5EB60BEFBD52D8EFEA1B2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o...e.)...._keyhttps://doug1izaerwt3.cloudfront.net/97d3f650321122216450758367 86b6a2d73cfab0.2.js .https://lucidpress.com/M{.+J'/.....F.}rY."@X.Zr.q ..O.$.....y.A..Eo.....U.....A..Eo.....0\r..m.....o...e.)...._keyhttps://doug1izaerwt3.cloudfront.net/97d3f650321122216450758367 86b6a2d73cfab0.2.js .https://lucidpress.com/n..+J'/.....F.}rY."@X.Zr.q ..O.$.....y.A..Eo.....y..8.....A..Eo.....0\r..m.....o...e.)...._keyhttps://doug1izaerwt3.cloudfront.net/97d3f650321122216450758367 86b6a2d73cfab0.2.js .https://lucidpress.com/H~.,J'/.....F.}rY."@X.Zr.q ..O.$.....y.A..Eo.....[].K.....A..Eo.....0\r..m.....o...e.)...._keyhttps://doug1izaerwt3.cloudfront.net/97d3f650321122216450758367 86b6a2d73cfab0.2.js .https://lucidpress.com/.,J'/.....b6.....F.}rY."@X.Zr.q ..O.$.....y.A..Eo.....}.a+.....A..Eo.....0\r..m.....o...e.)...._key

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1067e0d10546e20b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	380
Entropy (8bit):	5.873617776451227
Encrypted:	false
SSDEEP:	6:mmN/6EYy2MbHYViSDrVzR3zSwluiCnfm+XBKUhTHIRG0M9Y/MjbaSV4jNlZK6t:hAMbvAGsuiCnuwKUFHIRn0VbPYlT
MD5:	1AF466CE300EDB47963FE20E2FA56F09
SHA1:	9D42A865327E4B08A5748AAFA8D2CF48D34998E8
SHA-256:	8CDBD36FE6997119AF35D5172C289A18082DB8381BA00F2DD640AACDE42F385A
SHA-512:	F1B7ADCF106CEE8DDF8849B0EF82A3074570B779E3602419AA3171E0112ED0DBBE4D942FF419F8E6C1457A768DC2AF8A508F2D74973D9F3FDA9C1E52E528BC0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....._keyhttps://app-ab23.marketo.com/index.php/form/getForm?munchkinId=805-PTZ-019&form=1310&url=https%3A%2F%2Fwww.lucidpress.com%2Fpages%2Findustries%2Ffinance&callback=jQuery112409562693395334136_1628049754155&_=1628049754156 .https://lucidpress.com/.85-J'/....._.....D..7.A5q.d.?..E.A..1..Y...1.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\11519cf6722cebd8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16892
Entropy (8bit):	5.964028017161451
Encrypted:	false
SSDEEP:	384:l4t5EUl+nleWJTWGvHCppPL3naN3pLfTbd:Lt5Al1F5H+pPL3od
MD5:	58872361B02D27A3B66472B8989E5B1A
SHA1:	7AAE69F861C15775DD84B0C169AE75AE3550109D
SHA-256:	1D83EE91CBFE85434166B8E3216AF581A7A3C40A6A49852471DFD9FCC2C44FB0
SHA-512:	688FD1696E1F465F0AF0A50E3FAD2C4DD98CB42885FC9804EFB751FC674262CED0E1EBD8463DABD9A363B84E3C993AE93CE4A09298DC3606E116E02A6CB005F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T...b....._keyhttps://a.omappapi.com/app/js/webfont/1.5.18/webfont.js .https://lucidpress.com/M>.+J'/.....S....#.l1.d..)q.....a.Z..l.cY...A..Eo.....F.....A..Eo.....'..@....O....p@....X.....(S.<..`0.....L`.....(S.q..`.....L`.....Rc.....v.....Qc.....document..Qc..".....window....Qb2..$....aa....Qb.v.....ba....Qb...y....k.....Qb.....n.....QbZ..k....q.....Qbj..z....r.....Qb.._....ca....Qb.F.....s.....QbF.....t.....R....Qb.....v.....Qb.qj....w.....Qb2&.....x.....Qb.(.....y.....Qb2.~1....da....Qbv.....z.....Qbj D.....A.....Qb.`.?....B.....Qb6<.....ea....Qb*.(.....C.....Qb.v.....D.....Qb.\.....F.....Qb..p.....E.....Qb2..f....G.....Qb.@-/....H.....Qb..v.....I.....QbF.}.....ga....Qb..N.....ha....Qb2.F.....J.....Qbzg.B....K.....Qb.....ia....Qb.9.,....L.....QbN.T.....M.....Qb.....N.....Qb.Z.....O.....Qbv.....P.....Qb.....R.....Qb.}.M....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\136ed6e9c6c535fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.963532323754451
Encrypted:	false
SSDEEP:	6:mwYMHAJn1cRaGwvYumrbkhnEK6twrRqpv5GejqXokh:hOt9SkRWuRjKk
MD5:	EFF5BD6711710CB937D6AB6AC34EED33
SHA1:	E93160823A742B2D41882F64DCA8A3BC4339DE2C
SHA-256:	64F6B6113BFCB74C51AD701CBC6F7B6AE285EFF17EB58968BB5DE28CACB87691
SHA-512:	BF58E63694FA8B2C65F0A22CF7E461874D830D482553077003473A2D458B581D4B83EF398B69363B6F02AD4D8EBFF9E58D9449F6D104407E04ABF78CE234A483
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\136ed6e9c6c535fe_0	
Preview:	0\r..m.....V.....v...._keyhttps://script.hotjar.com/modules.7cb32ca5fc09d90486d4.js .https://lucidpress.com/#..+J'/.....r..4-.....l.{.".Vq6Y....h...A..Eo..... ..A..Eo.....#..+J'/.....9D3038B02D5A75EA50F3D8CECEB83ADAD561747515091702C4B2F2C4967FFCD4.r..4-.....l.{.".Vq6Y....h...A..Eo.....r..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\16d3920e81d43803_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	382
Entropy (8bit):	5.894957098322714
Encrypted:	false
SSDEEP:	6:mRYQ9LUnEfVhvDoQGCXYCJBGH2J6nTjK6tYldckNQaTKZneqI4qpGH2J6n+:09wE9N0Q3kVkck+YCq
MD5:	A3716F8189581312B8D18AC134D617BB
SHA1:	B5362E286FA73D0A000B95238CCD579684DE6313
SHA-256:	768393C225B42EE224D94BAA6F8D36871A8F2392DA68040405C744B9A33433A7
SHA-512:	F371BC587CFFF8D4D300B33610442EE31E3C341DEB69909D35C3214DDD9D6D4981B69975A7D9FDA7D53984ECBC4AEEDB07FB9C08F206DFBE94CD27BC70D3 71
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...Zi....._keyhttps://d5x2n72glkaxl.cloudfront.net/js/bacon?compiled=1&version=20201116-151730-f8bf3034 .https://lucidpress.com/..,J'/.....m4.....O .rZ...ec.....^. *..V.yv j.t.C&.A..Eo.....^D.....A..Eo.....,J'/.....5DA20CCCCBA94B11E9A94ABD46729C32C1C6AEA3B9BA2C8D96790F1BDB31CAD5O.rZ.. .ec.....^. *..V.yv j.t.C&.A..Eo.....p'3-L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1bf6f0b82f1b9913_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.51600347993366
Encrypted:	false
SSDEEP:	3:m+la9J8a8RzYRtMxANIhpSV+nRQBLqDk5uQArlHColC71FP7wYr/MmIWhllllpK+:mWYlNYpSVkeq45HAkrSC/1/hK6t
MD5:	4CD20EF9E97C778EA597861E7B29D7FB
SHA1:	B3A2AC56A27305BDE195952D96708389640ED345
SHA-256:	C90989F127D389F191AF93A4656E853FE7243834EC97B91AEA7199AC6A7CE303
SHA-512:	11140993F88E6A789BAAE47B0CD75730D1BA839B1BE37A208181C758878060C253114599D17C5A921928DC618EE43889B925040799B61B9D81E6BE01AB5EFA6A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://kit.fontawesome.com/585b051251.js .https://scientificemployment.co.kr/J.X%J'/.....T.sD<..z5..N.....}_...''...=....A..Eo.....^..... .A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1d58900ef9548d95_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.636775667167498
Encrypted:	false
SSDEEP:	6:mj3nY8SNXmZdT3gGuGh3tm784n0lnK4q6K6t:Y3/02vQI3tPqa1
MD5:	AD0F6D2B2572DD8CF74CCC43A93FE96F
SHA1:	D08D10929974870182 35DBF9108F40845CB8BFCB
SHA-256:	13EA9A4D8F31D5DF3517D0D8BACBB50F15FAA2E7BBABB3EBA00C3FFF674A0D01
SHA-512:	F3A905A3783AE33C2A02F5E016258238903FDD81095D924A00CCCA9606ED4383CE4663BB20BD172513EDD2D4DE7BAA6C65630D011550274368B2AB0C4689AB7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...{....._keyhttps://pub.lucidpress.com/292c4e00-83b0-4a5d-84f0-b0f2e3086142/viewer.js .https://lucidpress.com/U..$J'/.....,.....(C.}.z....s.../(.r<..b... ..F.A..Eo.....e.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1dc280024f36cf4a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.707723591499697
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1dc280024f36cf4a_0	
SSDEEP:	6:mUw/XYGLZwjDFAv0MLbRG0XzYIsN3+hDWdfAAaK6t:p8z8MLNv7swhFz
MD5:	5903E166D519BCF6340316C7442077C8
SHA1:	4D94F06C79E4ABB8BE82D25640BFB85EB09A559E
SHA-256:	C418DC767E6BAB23DB804F5B2D0CC68435D8523E9FA675376A61F390BE7D365F
SHA-512:	FEAA5259E3864B6B4E41776B266470E739FA95ABEB621656E0B166E1EAA16CF93B760A147948A194FE146CDF96F40534F8AAE843A8A261D67DDC88D3493C650D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....+....._keyhttps://www.lucidpress.com/pages/reactPlayerFilePlayer-476d010e022eb97978ec.js .https://lucidpress.com/...*J'/.....!.@..#S..cR.. ..:.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f27d52f4685155b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.483483419981897
Encrypted:	false
SSDEEP:	6:mqYET08NaYWbVOqZxq45cAI4vZZigA4vKhK6t:bg8NaY8ZL5Y4vZZigU
MD5:	C40F544989547463CBFAB951E7B88D46
SHA1:	94C4D0EA3480D9D101352B780BFBB3D24EC569BD
SHA-256:	6A9E6F045819E179052966EEFDFE332A4CB1F409EC44E430EB80ED3919A7CC86
SHA-512:	E9A13E98FED2676F5C4ADF4B8C6266E6A1CDE989E1C9B167D6383E3FBED47A97B2FB36186F1E0EFDA3AC0D3DE9B03570664076DF7707FA60A5E75E5B495C52C1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r....G....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://scientificemployment.co.kr/"..(J'/.....;y...G.1b.AJ..4.vP.... qo.x.A..Eo.....I.>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1fdd9223c59d29c5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1102
Entropy (8bit):	5.7630003528779135
Encrypted:	false
SSDEEP:	24:9UCHqcOA+Rk+k6xUny1Pt+UCHqWMPHCHqH1rm7/YM8oxGb7:2A+Rk+tGnbMPY/dob7
MD5:	B9664421E0DD38D77F0C0BD26C21E57C
SHA1:	02EFF96C6159506DB2F9660A1047BBF28D5C6F03
SHA-256:	6D3164F92C98FA176FF9BC80941BA6BA672E7D4AC8854473E363E79DF33A6F0C
SHA-512:	0421EE11CDAB4B27259A7A6F91809D53A28F05CA2E8598E329CFBA741FE3A2451174412536263 4B325F51DCAA8A38290BC3116AABB8FFC846C23A151CBAE97AC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^....._keyhttps://www.lucidpress.com/pages/3bf9cc50-048e3c591f22f27bea65.js .https://lucidpress.com/...*J'/.....{.....W.fi=...T..1.....x....W..d3u...A. .Eo.....N.G.....A..Eo.....*J'/.(.....'.....O.....t.....(S.x..`..... L`.....Qb:2.....self.$Q...8.....webpackChunkpress_gatsby..Qb^B.....push... ..`.....L`.....`.....Ma.....0..`.....b.....U..C`.....(S.....Pd.....push.10969..ak..... ..e.....)..@.....<.l*.....@.....@...!..@...(..!P..... .....d.....@. .....Qcd.. .....10969...E.@.-....PP.1.....A...https://www.lucidpress.com/pages/3bf9cc50-048e3c591f22f27bea65.js...a.....D`....D`8...D`.....D...`....&...&..A..D`....D.0Qjf%./$...3bf9cc50-048e3c591f22f27bea65.js.map]d.....@.....K`....DxH.....&....&.(.....|.&.-...(...&.z...&...'..&.}...&....*&....&.'..a....%.1...Y....&.....$Rc.....`.....Ib.....).....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\232e7b39f04b917b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	5.745698892450685
Encrypted:	false
SSDEEP:	48:/IClu/NrhvEUfWAmeM4H9beUsmFOSljtp4DKUVA6NErCNLoIjs28MVJ:/IC4NREUrm+9b3smF/jtp4OKzK2Nf8OJ
MD5:	B8A4A16E177A85EF7D00DEFEC0FFAC28
SHA1:	46216A928147A64D0558D5F58F0C4CAA921E058A
SHA-256:	5EF4265947EAE1E809BCB179315226615DB40E65AF5141E63FECEC222049B104
SHA-512:	C9441CABD990CB875C32B95C2AD70F46893CEDAFF2798FAD1394F29AE50A29A43277CC33641A901F43B8869C2B64350CE2DD659FF061BEDEB916E5C1E3BD76F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\232e7b39f04b917b_0	
Preview:	0\r..m.....p..."9.~...._keyhttps://d2slcw3kip6qmk.cloudfront.net/lib/external/retina/retina-1.3.0-lucid.min.js .https://lucidpress.com/.3.,J'/.....4.....Q\.P.....96 .C2@3.y.p..o.!Km.A..Eo.....+.....A..Eo.....3.,J'/.....'.....O.....Y.w.....@.....(S.D..`D.....L`.....(S..`.....pL`4....XRc(.....Qb.....l.....Qb2.. .....e.....Qb..7O....k.....Qb.O.y....d.....Qb..Z.....f.....Qb.l.....m...e.....I`....Da.....(S.....Ia.....QbRp~.....h.....1..@.-....`P.q.....S...https://d2slcw3kip6qmk.clou dfront.net/lib/external/retina/retina-1.3.0-lucid.min.js.a.....D`....D`h...D`.....H...` ...&...&....&....&.(S...Ia....*.....1.d.....&.(S.....Ia4.....1..d.....&.(S.. ...Ia....:.....d.....d.....D&.(S.p..`.....L`.....QeJ.....hasOwnProperty....K`....DvP.....%.q..~&.%..Aw.....&.....2.....$&.&.(...&.Y....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2368f14ec8465d59_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.608962943926368
Encrypted:	false
SSDEEP:	6:mgPVY8SNXmZdT3WDGCBAv0q2Pu0TGYPlbK6t:t02vGDNBSRAu0iAN
MD5:	F08F90D348D8927EEBBC6F2BBF024106
SHA1:	8A0D226742F3BF34552D238A1A16D5ED81BA8C8B
SHA-256:	C6D72351956AD5CAB5A7767A63282C99B3B4493758D228C31AC1E2BED91BB267
SHA-512:	90953E6D16AC3D4820A043A89BAFA97B864575FF3A2014933D8E785934DCFD0B44F1628BBEA5AE397296B11663E8C81701E448FA65F0E76E939BE57C6C92E153
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...m.. ...._keyhttps://pub.lucidpress.com/292c4e00-83b0-4a5d-84f0-b0f2e3086142/viewerDeps.js .https://lucidpress.com/...$J'/.....h.....q^....c_Zq..a.Z..... W.i.7.....A..Eo.....q.}$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\245ef57e8f449a35_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	81368
Entropy (8bit):	6.071184309318428
Encrypted:	false
SSDEEP:	1536:BAfIgDEe8RIzLb82dfWjS5cj6bNDY8hmXMIkh5e4jF9dzCn:6fI8gIz82dWu5cj6Bs84nkh5BjF9a
MD5:	772D7DD60ABC9EAFBB0622F17B637421
SHA1:	CE3D364BF668B3D56B53E6FAD707BF8E11C3B4D2
SHA-256:	1181501E9F607EF0BA8A09ECA577BBDC643914B4C60707BCB61739F8DB9F71DF
SHA-512:	87234953D8F15CFE22BC936D7E3F9CA8431C7A050EE79FFFAEA07F28A4A0BCF448ED183360E3507D08B14DBDE4EC0E554D3357E35CE0B2752C52513E2DBE86 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...F..;....12706BCF772CF053659463579E79629C95B5BDA9B68DEE904A71485A12F6E9EB.....'.....O.....<.....8.....`.....D..... .....\.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.u5.....n.....Qb*..A....q.....Qb.....r.....Qb*k.....t.....QbBs.....v.....Qb.....x. ....Qb.....y.....Qb.....z.....Qbf.....A.....Qb...0....B.....Qb.G;.....C.....Qbf,.....F.....Qb.*.h....E.....Qb.....D.....Qb.&.....G.....Qbz.hX....H.....Qb.e7.....J.....Qbn.e!....I.....Qb..... .K.....Qb6..S....aa....Qb.@.s....L.....Qb.....N.....Qb...\....O.....Qb.|.....P.....Qb6..<....M.....Qb..7i....da....Qb:.....ea....Qb.....Q.....Qbzu.....S.....QbJ.....R.....QbzA0..... ia....Qb.Z.....U.....Qbb(V.....ha....Qb...)....T.....Qb.....V.....Qb.R.|....W.....Qb.....Z.....Qb::s.....Y.....QbJ.{.....X.....Qb>.....ba....Qb.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\26496c37008854d9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1182
Entropy (8bit):	5.518702372586184
Encrypted:	false
SSDEEP:	12:PDK+ybzvVDdnbzapVDIKbzvVDvKbzX0VD20pbz0lNVDe7DDbzTn:bKrnR5ipR7HRvK/0RDp8TRuDD7n
MD5:	FE67EC372835307A585BC35624A7B3A0
SHA1:	303AA0702D6C1A5D8CB5EB5DA8F46B5FA1623302
SHA-256:	FF5B5EE4BC105BC0B671326C66E3A2CF76AF5A90A6AD0FB43ABAD90E38AD44C6
SHA-512:	6020EEAAA1283E378CD324C363DF5B140C2D27D4A2B59DB3F5A0B20E26795240AF6AEE1ED0159274C6D7D7D1CA2C55E9775FF7AF34C1446D2C3652EEBD68C7 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A...g.a....._keyhttps://js.hs-banner.com/19908047.js .https://lucidpress.com/..+J'/.....7.....v..^4.....8....f./f.vZ....A..Eo.....u3>j.....A..Eo.....0\r..m.. ....A...g.a....._keyhttps://js.hs-banner.com/19908047.js .https://lucidpress.com/.c.+J'/.....v..^4.....8....f./f.vZ....A..Eo.....B.....A..Eo.....0\r..m.....A... g.a....._keyhttps://js.hs-banner.com/19908047.js .https://lucidpress.com/C..,J'/.....v..^4.....8....f./f.vZ....A..Eo.....s.....A..Eo.....0\r..m.....A...g.a.... ._keyhttps://js.hs-banner.com/19908047.js .https://lucidpress.com/a..,J'/.....=.....v..^4.....8....f./f.vZ....A..Eo.....dz.....A..Eo.....0\r..m.....A...g.a....._keyht tps://js.hs-banner.com/19908047.js .https://lucidpress.com/.U4-J'/.....^_.....v..^4.....8....f./f.vZ....A..Eo.....A..Eo.....0\r..m.....A..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2b048cc042e03fe8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1428
Entropy (8bit):	5.711321602922889
Encrypted:	false
SSDEEP:	24:bYoDONYoD7s+NYoDwANYoDhONYoDDosNYoD/8y:Sy+6A+976y
MD5:	11584ED5BBE070C0991BD53D24272470
SHA1:	C1EA7295D4C80A6150350CB461F0747F921C11BE
SHA-256:	98C1AEF185F975D439630F965FC1C44768BB4ED1993ABEB3644CF08EF54DEABA
SHA-512:	BB775996F7874B8CD3AE57D959CDDBA0E7743971F3D35E0DF960D9B96714794287946EAC716CAEE43CEA8FA063D537F5639BC8F9DAB0A2ABA3FE490377CDD739
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...:.`.....\_keyhttps://connect.facebook.net/signals/config/388265628034613?v=2.9.44&r=stable .https://lucidpress.com/...+J'/.....n.d.r,s?..q.AH.Z;.....x.u....A..Eo.....5.Z9.....A..Eo.....0\r..m.....j...:.`....._keyhttps://connect.facebook.net/signals/config/388265628034613?v=2.9.44&r=stable .https://lucidpress.com/l.+J'/.....n.d.r,s?..q.AH.Z;....x.u....A..Eo.....:.....A..Eo.....0\r..m.....j...:.`.....\_keyhttps://connect.facebook.net/signals/config/388265628034613?v=2.9.44&r=stable .https://lucidpress.com/..1,J'/.....n.d.r,s?..q.AH.Z;....x.u....A..Eo.....A..Eo.....0\r..m.....j...:.`....._keyhttps://connect.facebook.net/signals/config/388265628034613?v=2.9.44&r=stable .https://lucidpress.com/O:.,J'/.....?.....n.d.r,s?..q.AH.Z;....x.u....A..Eo.....\ .....A..Eo.....0\r..m.....j...:.`....._keyhttps://connect.face

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2bf196ed578d39d4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.831728495216313
Encrypted:	false
SSDEEP:	6:mrj9Y4rgdsj//Ncttj4oRGA0Y2v5g8I8iZnK6t:8x7jXNe4oRwvv+8LS
MD5:	93060B2015DE831AF427A0F657B1F865
SHA1:	3F0F6E881E16C6758871D7474F27789584C1A6B2
SHA-256:	7A5424785C7D4B86F0E2BFC973A3E695A6D84492D495C1D74F73C74B5BA650CE
SHA-512:	056AA5501B079DD56B1D499BF45029DF30D6CD5A28E26E905FC3AC52621E374DA4E403E957628B6308722C5EB04D858B2E9DEB779F6A3D50C2A5EEB0DFA90EC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C....._keyhttps://s.adroll.com/pixel/DPYX46NNDVH3LEFFJGQU52/2DEQJ47H2BCHDFEEMMMO52/E7HOZDB27BAXZBW2AVAA7Y.js .https://lucidpress.com/.q@-J'/.....b.....4_{.U/.t#....>....x..M....'..q.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3144cfa7b74c9c14_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1176
Entropy (8bit):	5.530772101638451
Encrypted:	false
SSDEEP:	24:ewRQkwwRCTTwwRJlrwwR0LwwRuI0wwRq7n:1eThdAmHiL
MD5:	14AEA34CE586C75DD57A168EE8C7FC9D
SHA1:	B9ABC412B99D31C3BCCA575C8BFD9A268723F5CF
SHA-256:	B8144080A54FCFAA0EF53509E10260030CAB683F1A3DD1F6F72BAE4032CFA302
SHA-512:	E14F6B6AD731078AFCAA6AA5298C8595E81812EC17CE6755A2B56C4F81E6BBF40C3BB3FE43D9DD87EBED83A2533CF381ADBE86B4F9AAE86C78166C98C28D29E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...[....._keyhttps://s.adroll.com/j/roundtrip.js .https://lucidpress.com/...*J'/.....:.....).....#$.*..;..W.7..(C..G....A..Eo.....D.....A..Eo.....0\r..m.....@...[.....\_keyhttps://s.adroll.com/j/roundtrip.js .https://lucidpress.com/.ky+J'/.....g.....).....#$.*..;..W.7..(C..G....A..Eo.....J.....A..Eo.....0\r..m.....@...[....._keyhttps://s.adroll.com/j/roundtrip.js .https://lucidpress.com//...J'/.....%.....).....#$.*..;..W.7..(C..G....A..Eo.....).....A..Eo.....0\r..m.....@...[.....\_keyhttps://s.adroll.com/j/roundtrip.js .https://lucidpress.com/...,J'/.....#5.....).....#$.*..;..W.7..(C..G....A..Eo.....H.....A..Eo.....0\r..m.....@...[....._keyhttps://s.adroll.com/j/roundtrip.js .https://lucidpress.com/.(-J'/.....K\.....).....#$.*..;..W.7..(C..G....A..Eo.....Z.6.....A..Eo.....0\r..m.....@...[...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\335e69ddec2b9ac6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.338015296387499

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\335e69ddec2b9ac6_0	
Encrypted:	false
SSDEEP:	6:m9XYGLKd0Kc5noguGd8pvY28odQSQCw5r3WlbK6t:9WPoguGapwooqT
MD5:	B2A853C8F4953FA7E5E93439B31C9356
SHA1:	9DA65BCD9B34B0516A76867BA10CB0EF08C71195
SHA-256:	F9672032A16DC63CAC6527637ABA95B7EEE04344314E54598CC4F2AADC196DB3
SHA-512:	65BB293E92D3D459E15ACFB99A01FCB89DC964681A1FAB0A8B479092FCF10F5ED317E556AC6185204906B7D33A38C8380D5F9B924CFE221985B8CA00B338462
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...E@S...._keyhttps://www.gstatic.com/cv/js/sender/v1/cast_sender.js .https://youtube.com/o.D,J'/..... .....1@dbM..w./.61...wt...R..u.AU...A..Eo.....A..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\36b6fba4af0d29f0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.901355751777288
Encrypted:	false
SSDEEP:	6:mBqj/PY4rgdsj//NcttjE+B2C0DGt9YtD/SoK/EP4LK6t:tj/37jXNeEhDq+7iEPu
MD5:	6FA3AFB4265A958EF7D77E16CAA2F56C
SHA1:	5A67A780D889DFADFDD50A5B2945D6EC0298A9EA
SHA-256:	80C4A5E7094CC9CBEE8BC252CD7FAC1227E9C5CBBF05E8488116E7102F787331
SHA-512:	ECED898504E83E96BAF7EBACEAB9D14DC2F168136093D798F026F9F4DA70B3B65411C2E1E1BB058885AB05E13B52B076315FAD84CAFC31E6C879374550076098
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\...._keyhttps://s.adroll.com/pixel/DPYX46NNDVH3LEFFJGQU52/2DEQJ47H2BCHDFEEMMMO52/5L5WDS6OHZHVFITHFLZBSA.js .https://lucidpress.com/...,J'/.....>.....g...D.t.....&.c.....A..Eo.....~.FM.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3926d97490ec7585_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1477
Entropy (8bit):	5.857593300299945
Encrypted:	false
SSDEEP:	24:5Bev9b5xh8Ru+kdFArBwcxQxbxKF/BEa9m7/YM7WCQ9J:5aFzuRu+dFQ9xKF/K/vWCQj
MD5:	83E8AEC1BCE78F3C39001E73569C2D41
SHA1:	42D5230C7AC54D9D066911758B98042BB40C3B85
SHA-256:	F7F65BE2C0138BA22EC4AC748F723E6FB2EDF9F15467A517C7011D7D2C6AE4E9
SHA-512:	2682888492FE85669B2EB3277DB6B15AEB306272BDCE5CD5067625ABC4FD90807C139B2A4348B09E199B57823523B5EAAEE020EBB49F2916B0EB89C9A01D89C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Ss...._keyhttps://www.lucidpress.com/pages/component---src-templates-nineteen-nineteen-tsx-1ecc3d0f8bd3b1194491.js .https://lucidpress.com/0.U+J'/..... .....A.....CH.i.....'...>\mz.%...!Y.(...A..Eo.....#..K.....A..Eo.....0.U+J'/.x.....'..(....O....8.....k.....(.....(S....`.....$L`.....Qb6.b.....self.$Q.."yr.....webpackChunkpress_gatsby..Qbz.k.....push.....`.....L`.....`.....Ma.....`..... ..b....."...C`L...C`.....(S.....Pd.....push.17937..aj.....d.....@..... .f.....@.....QcD .....17937...E.@.-....tP.....h...https://www.lucidpress.com/pages/component---src-templates-nineteen-nineteen-tsx-1ecc3d0f8bd3b1194491.jsa.....D`....D` ...D`..... ...`B...&...&.....D&.(S.....Pd.....push.35494..a.....(...P.p;.....@...-..@...8..@.8.;..@.;.B..@.B.I..@.J.Q..@.....\.uN.....@.....@.....@.....@.....@..."..@.%.(. .@.*.*..@.+.,..@.,.-..@.....(

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3abce8e1224b2b4a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	365
Entropy (8bit):	5.514790947373435
Encrypted:	false
SSDEEP:	6:myKtXYyyoVDRhGYYYLj40lnnEDnK6tGGvY4XJ40lnn8M9Yt640lnng7:KVRvD31lqpZ7X/l80Allg
MD5:	DC408126429C0FEFE6029D7A161FFC6C
SHA1:	7D4006B07D925BA22354593547A2A416B95B791A
SHA-256:	68709BD1076B13462BAD08B02FDD4A760ABADF0F60DEB48858EA06F574162318
SHA-512:	8AAA15E194CAAD1A0F6F6DC78FA0F1DB06EE1145FD10F80EC31BEE754AC32B0D719236202FB04454F1ADEAFB93E8CFE2127293C3A582B90F5F0B5E43282176E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3abce8e1224b2b4a_0	
Preview:	0\r..m.....A...1^i3...._keyhttps://app.lucidpress.com/js/config .https://lucidpress.com/.u.,J'/.....i5....."..qw%@.....:..'....lg.b'.A..Eo.....|.#f.....A..Eo.....C$.-J'/.....^Y....."..qw%@.....:..'....lg.b'.A..Eo.....jw-J'/.....q....."..qw%@.....:..'....lg.b'.A..Eo.....H.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3b8a3819ae183954_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	741
Entropy (8bit):	5.488451892007554
Encrypted:	false
SSDEEP:	12:0bhjajHRhXv5clOZKbhjajHRhG/clOqTKbhjajHRhv/XclO671:ohjuHvXv5clu2hjuHvG/clB2hjuHvvfc
MD5:	B56849B3644AF0944D1706E8D25D94A3
SHA1:	739DE571D82D6BAE1388BF644FC062944DEDA22E
SHA-256:	A13D1D3905FC0F6C5FAE62F9477B624F18414C1F21721BA4B1D0848EAD33A9CB
SHA-512:	7512C76F6CB17C8B19E4B7E0C1E8C9CA1BA8DB49DB2A7871E1A09D08BF4A4013F52CBD8797118AD1E02A0BC96D832CD5AC6BC63D40AB4B6F62D1746588CEC 472
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...uRB....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/lucid-modal-video.js?qwihau .https://lucidpress.com/..,J'/.....x5.....J..i.....[{y.=.$.p_..._u.....A..Eo.....J.f.....A..Eo.....0\r..m.....s...uRB....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/lucid-modal-video.js?qwihau .https://lucidpress.com/6..-J'/.....jY.....J..i.....[{y.=.$.p_..._u.....A..Eo.....X.q.....A..Eo.....0\r..m.....s...uRB....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/lucid-modal-video.js?qwihau .https://lucidpress.com/.r-J'/.....q.....J..i.....[{y.=.$.p_..._u.....A..Eo.....%.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ca51d4fc58c490f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.55167004692455
Encrypted:	false
SSDEEP:	6:mmJR9YGLUxGBztT2buGguGzjhlY6Qviq4athK6t:KGBt6buGguGah71
MD5:	B577B47268A504CBDEB44C3F704479B0
SHA1:	670A595A2AFC1BC6B4F1E53CBFB2ACFF3593ECFA
SHA-256:	7F42FEF91DB1A28590EA0A61E380FE2A096D80163235FA1AEC65A3609D0FEFD3
SHA-512:	B8219BCA105354AA3DF71475A07F0A47C2C136F6A9B62345FE697B77203ECED960A2B16474C56627333C76DFBD7DDD0B6817ED92D9DC716C68CAE6B7CCF38A B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e....._keyhttps://www.youtube.com/s/player/2840754e/player_ias.vflset/en_US/remote.js .https://youtube.com/O.@,J'/..... .....c.....X..X.....Z.!....J ..A..Eo.....TQ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\40dc66a8c7c1909a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221832
Entropy (8bit):	5.959299031176904
Encrypted:	false
SSDEEP:	3072:msV82rqZowx92uWjWVSFN4ljCneMe+V4TS+jg9A4Q:mZxZown2rtSmifg9S
MD5:	6528B90A5C57A2F6B505F3B2DBABEC8D
SHA1:	BDD7F9093500F1FB0E6B3DED37FC300D6438A969
SHA-256:	AB177E40E5C534A222E14EAD5DF2810A641AE1A95335BE05FD2AAE2ECFAA077E
SHA-512:	8C46EB8186EC68AF01821A40D7D6A427C3BBAC49B9034310BCAE4351A987AFB5FE7ED1237629DB03F587291BB95A068DCBEDE76EB00D33B1888C35B3721A00 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....*....4844315676EE1FA7D858D37316A865DAF0080F64FBD9E82A11CD70D5CDD6C14F.....'..1....OD....`.....T...l..... .....0....&.....h.....@.....x.....(S....`.....L`.....(S.x.`.. ....L`.....PRc$.....Qb..c.....d.....Qb.`.....c.....O...Qb.}yz....e.....QbB."....f...d$.....$.....M.`....Da.....(S....`.....4L`.....4Rc.....`$.....q&`....Da....8..... .$..Q.@.....require..... Qfr.....Cannot find module '..Qb.....'.....Qe.\.m....MODULE_NOT_FOUND.9.....a.....Q.@.....exports....a.....Qbv5.....call..q/.(S.T..`d...]..K`.. ..Do.....&...*..&...*..&.%.*..&.....&.%...%...%.&.].....,Rc.....l`....Da.....,....c..... .....@.-....DP.....7...https://app-ab23.m

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\428618177cf744c1_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\428618177cf744c1_0	
Category:	dropped
Size (bytes):	6847
Entropy (8bit):	6.233746771441635
Encrypted:	false
SSDEEP:	192:wJgNvtnYV7vKiYlBMF1k3k2o6xbku+CObDNF6bwQkUU:lsKiYI1k3k2Pau+COlF6bw3
MD5:	90C61CEAD581D7A3A6042993DBB909FC
SHA1:	2BE8E8CBBA582F7483A14D86E76D79883E465335
SHA-256:	4CECF420707EA448A13FDD4C8119361548AC882A107C15BC262B7474F0688D9C
SHA-512:	826003A58FCBCC52010EDE4D3CD0A22CC5A734E2576C50EA41126A11849CCE36F4F0C6B19ABB1D978D9260D51E1D4EFFD0E2E70EC51A50C74B62C62B6053C 9F
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...U$...._keyhttps://www.lucidpress.com/pages/framework-8f6597af57c976af6db6.js .https://lucidpress.com/...*J'/.....JS....o....e..s.D.9p...m.....A..E o.....e.....A..Eo.....'.....O....8...../.....D.....(S....`.....@L`.....Qb:2.....self.$Q...8.....webpackChunkpress_gatsby..Qb^B.....push.....`. .....L`.....`.....Ma....\L..`.....X..b(.....(...C`~...C`....C`rT..C`l...C`~D..C`....C`.....C`....(S.....Pd.....push.58772..a....;...(..g.....@.....@.....@.... .f.....@.....@. .....QcP.....58772...E.@.-....PP.1.....B...https://www.lucidpress.com/pages/framework-8f6597af57c976af6db6.js..a.....D`....D`....D`.....`N...&...&.....D&.(S.....Pd. .....push.23615..aJ...g.....Qc.p.....23615...E....d.....&.(S.....Pd.....push.90331..av.....Qcl.....90331...E.d.....@.....&.(S.....Pd.....push.43577..a....u..... ....!3.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4801acb45b7933b3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213080
Entropy (8bit):	5.784540794635424
Encrypted:	false
SSDEEP:	3072:gj3NGJeWLSqC5tWMjwA2JUNVzGg+PjBmZynuEZ0VJ3O0LHs5ytLX:oNPvtWoGJUNYb0Zys
MD5:	C5E9EE458DB52DB618014D6FC3620B04
SHA1:	2A938BB57C5D561C004FBCFC4E6AD20776289DFD
SHA-256:	7A7081BCBCE2836F4560E168D0EB33260E144FA0C7B568EEAB5A10474986520C
SHA-512:	1C257CBED8435601C92D5955014252A6E632A19D97832E381BE88FB89ACBCEE0DFD5597C516179CEBF2FF76265E6EAFB87549A9741EE1481E111995A7F629F2E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...:B.|....50815253C6ED5B7DB002B6B697A47731342E1DA7EC84C7BAA81DB56BB0F81A31.....'.mq....OE...p>...<h.....(....".....D..... .....p.....X.....t.....\.....(S.q...`....pL`4....(S.p.`.....L`.....0Rc.....Qb>.|n....t..`....I`....Da.....Q.@.....module....Qc.4.u....exports...Qczp.D....document.(S.....5.a.....a.....a.....A....a.....a. .....Pc.....exportsar.....I.....@.-.....P.....https://d2slcw3kip6qmk.cloudfront.net/lib/bundles/js/jquery-2.1.1_jquery-ui-1.9.2_jquery-cookie-pre-1.0_jquery-fancybox- 1.3.4_jquery-lucidtab-1.0.min.jsa.....D`....D`"...D`.....`....&...&..!.&....&...(S...."..`.C.....Q.L`.....q.Rc4.....M...Qbr.....s.....Qb.....x.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\484516fa709d9ae0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.4908191107057
Encrypted:	false
SSDEEP:	6:mX/PYGLUxGBzP8j4PY0c71j4GguGFzY/jV/64IX7LK4HK6t:yYGBP8sPjcRsGguGq64IX7R
MD5:	07B91A44208604C73F3163165700E742
SHA1:	CF71DBDD88F1122FEF7DB784BAA663C7CC0E703C
SHA-256:	A00D2F2E5A0A6B5971BF1F3EB1DD648804E07BFD605811A5A7C7B8FF6036D641
SHA-512:	2ED2FD5A137A55734D1EC4ACC911F80D93D7331AC5E7A73FC45F11D163541ADF249276323AED438CF2F7E9569B919FD0416CE78A35C8D280296064B8A831766
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o...VN....._keyhttps://www.youtube.com/s/player/2840754e/www-embed-player.vflset/www-embed-player.js .https://youtube.com/..7,J'/.....o.q.w-. ;}.i.`.pZ_.)..].e..ol..^.A..Eo.....$.~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4e43ecd1850e312e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	199960
Entropy (8bit):	5.895847127057814
Encrypted:	false
SSDEEP:	3072:p1wk+GFkruTzscN14fXSQUh13GGXvB77Ppheo:kk+Skru3scTpBRhf
MD5:	70242A6BC6A1D918E9F43825E9567CAB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4e43ecd1850e312e_0	
SHA1:	E93B356C0D674412A19601846B27C5B94C076A46
SHA-256:	8095D939D7CF8D3D40AF3F7D1619BDE3751D8ADC14734EC81E74EA3B6F6FEFB3
SHA-512:	1E149DBDCA00FC4F08904FBA6E5A52C3755B278CDC83460E2EE3AEF14675F1F38FF959DAC6D3BD3D7E2D17D33AB37A45E6B92FC982B637E842A44CA74BE787 2C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....j.....73DE1A7A20FFB8C017EB1AE21A3A797F7165FE8819F33FE7C22573E0B518AE55.....'..1....O>...P.....+.....T...l..... .....|.....&.....p.....l.....`.....(S....`.....L`.....(S.x.`.....L`.....PRc$..... .....Qb.O.y....d.....Qb.k.....c.....O...Qb2.....e.....Qb..Z.....f...d$.....$.....M.`....Da.....(S...`....4L`.....4Rc.....`$.....q&`....Da....8.....$..Q.@:H .....require..... Qf.....Cannot find module '..Qb.M:y....'.....Qe.....MODULE_NOT_FOUND.9.....a.....Q.@..:e....exports....a.....Qb.5.....call..q/.(S.T..`d...]..K`....Do.....&.. .*..&...*..&.%.*..&.....&.%...%...%.&.]....,Rc.....I`....Da.....,....c..... .....@.-....DP.....7...https://app-ab23.marketo.com/js/forms2/js/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ffe4d312864231e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1560
Entropy (8bit):	5.875489200113882
Encrypted:	false
SSDEEP:	24:YVQOSFpeVQaRSeVQ5FjeVQaeVQVrEliFfVQEXppkS:AZSf25S20j292ErEliF9NX
MD5:	63CE4211B6539F63D1838FBB00E07A60
SHA1:	CE0D60BC74429DEF62A0F9CB9B83779D69ABAB85
SHA-256:	8A6A41DF85351B6A6BE7D2A9796629463FAD1B534CB8BA09DFDBFD301701E890
SHA-512:	B334D121F30B73E2A8BBD3F67F9F8732F39D540264F12F618E095A516B77A43E7BF7895EEA33CBDF10C419C6BF420AEA49E9315A7122E30144F8285E793EB14E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....!....._keyhttps://app-ab23.marketo.com/js/forms2/js/forms2.min.js .https://lucidpress.com/l..*J'/.....7.....n..L....S.H....&....(.....A..Eo.....uh.....A ..Eo.....0\r..m.....T....!....._keyhttps://app-ab23.marketo.com/js/forms2/js/forms2.min.js .https://lucidpress.com/..y+J'/.....n..L....S.H....&....(.....A..Eo.....n. .....A..Eo.....0\r..m.....T....!....._keyhttps://app-ab23.marketo.com/js/forms2/js/forms2.min.js .https://lucidpress.com/%..,J'/.....n..L....S.H....&....(.....A. .Eo.....Y..F.....A..Eo.....0\r..m.....T....!....._keyhttps://app-ab23.marketo.com/js/forms2/js/forms2.min.js .https://lucidpress.com/.<.,J'/.....8.....n..L.. ..S.H....&....(.....A..Eo.....&=9.....A..Eo.....0\r..m.....T....!....._keyhttps://app-ab23.marketo.com/js/forms2/js/forms2.min.js .https://lucidpress.com/.<.-J'/..... .....6Z.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5455f51911b7f1ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	382
Entropy (8bit):	5.9561181037290085
Encrypted:	false
SSDEEP:	6:m45YQ9LUnEfVSXF4p8cGeTlY15ca7YQ/7ZK6tiRxG6OhTRV2gc2XcVKjnn/ca7Yz:l9wE9SXBcXe5l7YUTexG6U382Xkmn97Y
MD5:	3A014A1067B28E8676FD36AFAF741909
SHA1:	16F7E5F404F39D589BE91E0E3BAF55E2845B1AB3
SHA-256:	7397D4E7F21F73A05B9386762E497119C13569C7C58D0542E3AE54B2DADDD648
SHA-512:	C647F42725B312D13EC204FC49A5592575DBC89497CF522C143E11EB3F7C37749795C28C116BE943337BBE25B44375AC056C2F5D9444E687223BE4B97AB77DC3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v.....6....._keyhttps://d5x2n72glkaxl.cloudfront.net/js/bacon?compiled=1&version=20210422-142202-054eb930 .https://lucidpress.com/...*J'/..... \..n.7.D.G..\..j?-.Y.hJx..;Z(..A..Eo.....P>@>.....A..Eo.....*J'/.`...7CCDEDC602480CE9333CB637D243A860790E0341DE655FE79060FB5F85DC004C.\..n. 7.D.G..\..j?-.Y.hJx..;Z(..A..Eo.....Y.)L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\54676502d7e53de2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3187
Entropy (8bit):	5.44819216754661
Encrypted:	false
SSDEEP:	48:xXGdpvc5d/8asd1t3XdbGdpJHESWvItIYYKgt9gP/dRSSOtRQCSRTP46l:8K/Id1RNmJHdpZY3t9gnOu
MD5:	8828C606B8019E19105044AA48016020
SHA1:	25EF8B9A7B20D79000A2F27F94CDE9867612187E
SHA-256:	B0E28BFADA1A5B7BC05809113F2D112DF53499CE5DF8647430FA14A863B2DEEB
SHA-512:	D15FFA9C4B7A3E9E681816F7D4B280FA95A4DC16C325D14F60E96E7DE93D4D62F02BAC8474AAFB23DD3EE08CC55CA96092ED3D5A464E3572B18EBB13365F16 F6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\54676502d7e53de2_0	
Preview:	0\r..m.....}&V...._keyhttps://nexus.ensighten.com/choozle/13609/code/7e3bcccbe9be6061a65a6eb142929580.js?conditionId0=421905 .https://lucidpress.com/A}.+J '/.....F..."....%....._..~...\.!...x..A..Eo.....-.....A..Eo.....A}.+J'/.(.....'.F.....O.....ec.w.....|.....(S....`.....,L`.....Q.Pj`4.....Bootstrap per..Qe"> .....bindImmediate....(S.`.`x....(L`.....0Rc.....`....I`....DaF.....Qc.."....window.....Qe:.....ensightenOptions..Qb.m.w....on....Q.P.Pzw....mousedown.... QfZ .0.....#newsletterSubmit....(S.....Ia.....I..1..@.-....tP.....f...https://nexus.ensighten.com/choozle/13609/code/7e3bcccbe9be6061a65a6eb142929580.js?conditionId0=421 905..a.....D`....D`....D`.....D...`....&...&..q.&....&.(S.`..`x....(L`.....0Rc.....`....I`....DaT.....A.....Q.@..P.....click.....Qe..cJ.....primary-action..(S.....Ia.....I..Q.... .d.....K`....Dr@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\55e80d4e28e5225e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	283
Entropy (8bit):	5.51476290825385
Encrypted:	false
SSDEEP:	6:mlHlXYGLZwjDvMW37dzuNRGAFYTXwmGn9nK6t:C5GBcDbcw19p
MD5:	ECC75CC53D6517755800E4A075E1094C
SHA1:	224199FB32382FE1B72C2B0017597A0725CBE1B8
SHA-256:	4DF8C23E6096728A7B27CAB5C3522118AE31265E15944DE4CC8D9CE6A367FD4A
SHA-512:	7126D7C991B14A5754B564EFAA730942F1FD1EA38C33611B0610F95ADB6ED884F3591E91071788CB8EC1D1F59BAC7E1CC1888846980269E6F672671FB6E53EEE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e....._keyhttps://www.lucidpress.com/pages/component---src-templates-nineteen-homepage-nineteen-homepage-tsx-db945e10e1403cd78f91.js .https:// lucidpress.com/.t.*J'/.....q.....p.q....Ex..F..,.....i1.Sm.V..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5a67bb9a97ce4a10_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1290
Entropy (8bit):	5.686427398147941
Encrypted:	false
SSDEEP:	24:B9MTHNL9WlITYTL9mTJrL94T47L963/6T3L9S+wyTe:BqNLc9L4Lf7Ls3/gLk+wt
MD5:	58249AE565E1ECE04A2BFFEF1D5918C9
SHA1:	9CD3E82D005AE344084B8C47A8C0BEBAAB682FB5
SHA-256:	B0F2C49139D3A1ED8092F84D8E7C71150FF9B214B8DBADF3F5CA4D545C779B3E
SHA-512:	6DD3087232926606148 56A579A8A0316820F6A66C06ABBBAB01B572DBCF1F6149374901B050E918ED0C000896A44001D870BB38687BB7944F64F6F788220407B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5NTB7NT .https://lucidpress.com/.3.*J'/.....{.r....wdo.....e.q.... ...6#.A..Eo.....X =.....A..Eo.....0\r..m.....S....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5NTB7NT .https://lucidpress.com/G._+J'/.....t.....{.r....wd o.....e.q.... ...6#.A..Eo.....A..Eo.....0\r..m.....S....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5NTB7NT .https://lucidpress.com/.Q..J'/..... .....M.....{.r....wdo.....e.q.... ...6#.A..Eo.....X.....A..Eo.....0\r..m.....S....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5NTB7NT .https://lucidp ress.com/c.,J'/.....4.....{.r....wdo.....e.q.... ...6#.A..Eo.....G.....A..Eo.....0\r..m.....S....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5 NTB7NT .https://lucidpress.com/.L!-J'/.....Z.....{.r

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5b25dd016621059c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	55921
Entropy (8bit):	5.900860923276079
Encrypted:	false
SSDEEP:	768:jRtETQe1nHodDS+4sM1t41glJJgv7rh+OkS6jJXnr3akXHhtBRCZ:jSQKn+OmmSqlJJgTrhwS6jlOkXHhq
MD5:	26711A07541BC47237F7D5C51B207099
SHA1:	7520E84AA971070895205332AE89DF32FE0B8859
SHA-256:	DAF24B91C3C261F053EAE94BF8D2F5AAE055DAB38964D5062063D253AB01739F
SHA-512:	C2C3CB1ACFD279820ABEDFDBD5477ECD408D61CE1D96DFE4FC3FDF98C870AFC2A0F27537BE7A40A8E0E7734EA9310FBBAB35092F42ABAD4644D033E5587A F23
Malicious:	false
Reputation:	low
Preview:	0\r..m.....y....._keyhttps://d5x2n72glkaxl.cloudfront.net/js/cookieSyncClient?compiled=1&version=20201116-151730-f8bf3034 .https://lucidpress.com/.../J'/..... ...@4.....O.:k7y..3.... .Z.'u.....&..-k...A..Eo.....^.....A..Eo.....'.-.....O.....`.....(...x.....8.....D.....(S...y...`.2 .....e.L`.....L`.....Qc..(....Reflect..(S.....Ia.G...H.....d.....,...QbZ/T ....cscaE.@.-....pP.....d...https://d5x2n72glkaxl.cloudfront.net/js/cookieSyncClient?compiled=1& version=20201116-151730-f8bf3034a.....D`....D`v...D`.....`V...&...&.(S.\.`p....8L`.....Qcf.A]....assign...(S.....Pd.....t.__assign..aZ.....IE...#d.....Q.@. .I.... __assign.(S.=...`2....$L`.....HRc .....QbB2w.....n.....Qb...O....r.....Qb2.....e.....Qb.f.....t...c....d.....d...I`.....Pd.....t.__decoratea....n....M.....!..Qc.....decorate.e...K`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d87a95d8e77ca56_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2456
Entropy (8bit):	5.865890237030985
Encrypted:	false
SSDEEP:	48:YsLl6eEb2p2sLiFdbA2eqpsLgcboIasLxJbjpt/8fsLWLb42sLFNbP2sLRqb5r2e:YsLYb/sLiFdHeqpsLgeHasLHgfsLWP1t
MD5:	1D9234A590BC1F4DFB73EC61BA107D86
SHA1:	D1580F9E74C5874BC396628A37548BD6A47A9883
SHA-256:	EF3B18E2C63D8965C787C190623348D0FA77C6E95FC7251496F3F2B82126B090
SHA-512:	C2670ECB559E7E80115943F1EFDFF7C84343DE5A62603A524F0C39FDEBEABF2BEA8B82C632ECB22D32F1C95ABFDFEE237923E4D4483584594F228F1388DC43 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J....._keyhttps://www.google-analytics.com/analytics.js .https://lucidpress.com/H..$J'/.....f.e....`..C.. .....<..1.6.W.d.A..Eo.....-.....A..Eo..... ...0\r..m.....J....._keyhttps://www.google-analytics.com/analytics.js .https://lucidpress.com/`..*J'/.....f.e....`..C.. .....<..1.6.W.d.A..Eo.....s.....A..Eo..... .....`..*J'/..>..203D78ACD8AB0D56F391448A021C3998A3280C23B6B8665926E563E653ADB0B4.f.e....`..C.. .....<..1.6.W.d.A..Eo.....Qc.$L.....0\r..m.....J....._ keyhttps://www.google-analytics.com/analytics.js .https://lucidpress.com/..o+J'/.....f.e....`..C.. .....<..1.6.W.d.A..Eo.....XT+.....A..Eo.....o+J'/.`<. .B95C478DA5630A1B1CA32F428436518A98511E18FEDFCE0FCB735D56E573231E.f.e....`..C.. .....<..1.6.W.d.A..Eo.....L.....0\r..m.....J....._keyhttps://www.g oogle-analytics.com/analytics.js .https://lucidpress.com/...,J'/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5faeb509b5edb73a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	193672
Entropy (8bit):	5.885804649015457
Encrypted:	false
SSDEEP:	3072:1LGu7lc3A9CrNsdG3oUXdruq5YYNrfiuWNF4yjc:NGklc3kCradW5RrfGCyQ
MD5:	8929D85E309776B784A2B60DCABBE3D0
SHA1:	DC09C9FA9FA96D0A877E478B98DABBB849FF80A3
SHA-256:	47DFBFDB4F383238E1E85973CA8E51714A86689104F242C8541438C22D726ABA
SHA-512:	57D1CD8F75B5FC446A9AA179C8824AF9DF0F58E33BEF64B468B0DC515F046CE7429A81F70354DA302666FB4C9B6EEC19E93D84A58E410C8088B39960A9C11C4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.... D.....3D323E77B2F97C73CD950496178B98901B1FC130991ADD0C6A70F0DA7B9D354A.....'..1....O=.....s.T.....T...l..... .....|.....&.....(S.....`.....L`.....(S.x.`.....L`.....PRc$..... .....Qb.^.....d.....Qbb.x.....c.....O...Qb..W.....e.....QbFQ.....f...d$.....$.....M.`....Da.....(S....`.....4L`.....4Rc.....`$.....q&`....Da....8.....$..Q.@..^.....require..... Qf.k.(....Cannot find module '..Qbjc;.....'.....QeRu>.....MODULE_NOT_FOUND.9.....a.....Qc.....exports....a.....Qbf..p....call..q/.(S.T..`d...]..K`....Do.....&... *..&...*..&.%.*..&.....&.%...%...%.&.].....,Rc.....l`....Da.....,....c..... .....@.-....DP.....7...https://app-ab23.marketo.com/js/forms2/js/f

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6310199623e4f717_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	474
Entropy (8bit):	5.722095150214414
Encrypted:	false
SSDEEP:	6:mdYy2YURK9Y84Lfo09hnzK6tWdYy2YURKh5WnUlFDx1hLfo09hndwZK6t:N9RE0Lf5lr9Ry5LlFDFLf5dwT
MD5:	17E27C701B746CBFE44CDE4893DF3129
SHA1:	13F31AC37C8B3EC5066E3C279671AC6F48BAF2A9
SHA-256:	4138C1CF3CFB75CD73490298CB70A68C3C5D04EE95B810843F35333A03D9E171
SHA-512:	4C7C0265A930CC0653B3D15A26EC40EF873946129A6A188EACA17CB89EA96E3E3B2DC7524536477807E26FA4B0230D4C12AE1F61BD558CCCE4263EFE0A21C4 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....E....._keyhttps://app-ab23.marketo.com/js/forms2/js/forms2.min.js .https://marketo.com/[%_-J'/.....T.....J(.cp..~.[>...,4..l..&..z.[...A..Eo.....;.;.....A.. Eo.....0\r..m.....Q....E....._keyhttps://app-ab23.marketo.com/js/forms2/js/forms2.min.js .https://marketo.com/[%_-J'/.....3D323E77B2F97C73CD950496178B98901B 1FC130991ADD0C6A70F0DA7B9D354A.J(.cp..~.[>...,4..l..&..z.[...A..Eo.....L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\63d2ef5776c2dff9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1290
Entropy (8bit):	5.619154895617545

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\63d2ef5776c2dff9_0	
Encrypted:	false
SSDEEP:	24:BEGdu6+OkiktTLEGdu6Z/SkiklLEGdu6lakikC1LEGdu6v/kikBLEGdu67ukiktg:BEGdBkiITLEGdL/SkikLEGdWki91LEGR
MD5:	806935BF1F854B0634CAC83CC1D63A2C
SHA1:	5044E7A5A97B550CDD5118E418F465C73039116C
SHA-256:	6F22A1A362E714E50D95D22BE7A313A45D0DF32ECB2A79D14C5B43F5DA93473B
SHA-512:	E847E321AD532A875245237ACC0642DA66E0AA2F396614EBC405859EACCFA065B8FCB47BF070EE8D20D60721F340264D4ABC25227B118632FCB8E7A54C66982
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....._keyhttps://nexus.ensighten.com/choozle/13609/Bootstrap.js .https://lucidpress.com/.~.*J'/.....G.....[."..g.....v7.B.\....T.!15.!Z..A..Eo..... .A..Eo.....0\r..m.....S....._keyhttps://nexus.ensighten.com/choozle/13609/Bootstrap.js .https://lucidpress.com/..y+J'/.....[."..g.....v7.B.\....T.!15.!Z. .A..Eo.....o[.....A..Eo.....0\r..m.....S....._keyhttps://nexus.ensighten.com/choozle/13609/Bootstrap.js .https://lucidpress.com/...,J'/.....[."..g.....v7.B.\. ....T.!15.!Z..A..Eo.....?.....A..Eo.....0\r..m.....S....._keyhttps://nexus.ensighten.com/choozle/13609/Bootstrap.js .https://lucidpress.com/a8..,J'/.....9..... [."..g.....v7.B.\....T.!15.!Z..A..Eo.....#.....A..Eo.....0\r..m.....S....._keyhttps://nexus.ensighten.com/choozle/13609/Bootstrap.js .https://lucidpress.com/.;*-J'/... .....].....[.".

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6471a25cf09b93a9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2905
Entropy (8bit):	6.1660700375016715
Encrypted:	false
SSDEEP:	48:gGdvo3Qivba6P1tlv0BJTyuRjhTywTLef/zvZiSNHNqwGdvo37vvPfyh4+HIOGnb:+7zP1heoRTClR97vvPfyitb
MD5:	5220AAB181D95B3FAF6F427E6246402C
SHA1:	AF75FE68E6E319E99263F72D108C4E1996CBCC6D
SHA-256:	1A766D72B4C499A5BDEDB02BA87568B35D143B998792A0F7FB08E1B7F0184151
SHA-512:	03D10C0F35736EF1778C20E33CD7506963CFD553A9AA4AD47FE2CF6AE2C8D81E19DC3EF30B3341785FC0BF91AA87BF66ADE41B884F434032857B0F71947D1A1
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://nexus.ensighten.com/choozle/13609/code/6270411c3792dbc63b7e880e949ffac3.js?conditionId0=4899739&conditionId1=4899741 .https: //lucidpress.com/.{.+J'/.....4.....O..`.....Th....Dx....)....A..Eo.....O.....A..Eo.....{.+J'/.....'.....O.....$2.....(S.|..`.....L`.....Q.Pj`4... ..Bootstrapper..Qe"> .....bindImmediate....(S....`.....xL`8.....Qc.."....window.....Qe:.....ensightenOptions..Qc.]E.....parent....Qc.....document..Qcn.....referrer..Qc.U .!....location..Qb.#7.....Math..Qc2hE.....floor.....Xa... _..B..Qc.=.....random....Qe.O.....createElement.....Qb..<.....img...Qc~~.F....hostname. Qf.p].....encodeURIComponent.... Qc^DB.....match....0Qj...U"...^https?:\/\/([^\/?#]+)(?:[\/?#]|$)....Qd>.`m....setAttribute..Qb..s.....src..,QiBh.. ...//cs.choozle.com/dp/chz/22443?d=..Qb>,.....&cb=.q...Q.`..<.... .display: none;... Qf.!i.....getElementsByTagName..Qb...%....body..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\649647fdaa2ac7fa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.576585771718164
Encrypted:	false
SSDEEP:	12:lp87DD+hYVf9s/p87DY2GYVf9y5/p87DW0OlGYVf9j:EHD+h6syHY2G6cyHW0KG6j
MD5:	9F36B13EB751953A1B7B87AE88AD2B6D
SHA1:	5F9878471DB2725B84A6F9135F32DF90EACBDC25
SHA-256:	57F219405E02E10ABCF32A82DBA299EA9A580F1D18F43C37D72DF7AEB811C258
SHA-512:	21C29972A11DC17FBFC01005017361E6423CB16BCABF30F55BDE33A8CB5331EE1BE790007BE0167F0BF15D576CD43EB934DC70BF9F1E4DAD042E21597F4E938 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...6....._keyhttps://www.lucidpress.com/pages/misc/jquery.once.js?v=1.2 .https://lucidpress.com/*..,J'/.....53.....~.[K)B.....Y..MK./.?.8.:c\.X...A..Eo.... ....9.....A..Eo.....0\r..m.....W...6....._keyhttps://www.lucidpress.com/pages/misc/jquery.once.js?v=1.2 .https://lucidpress.com/.+.-J'/.....W.....~.[K)B.....Y ..MK./.?.8.:c\.X...A..Eo.....A..Eo.....0\r..m.....W...6....._keyhttps://www.lucidpress.com/pages/misc/jquery.once.js?v=1.2 .https://lucidpress.com/..q-J'/..... .....o.....~.[K)B.....Y..MK./.?.8.:c\.X...A..Eo.....E.*.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\653512280d5ec3f7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1188
Entropy (8bit):	5.546844324192514
Encrypted:	false
SSDEEP:	24:ARvDKMfcuRvD7dfbuRvDPf1uRvDF3fjiNuRvD4+Nf17uRvDakfb:AReHuR/ZuRJuRR8uRs+b7uRmU
MD5:	C494FB5D9A2315BE3F147BEB741387CF
SHA1:	1B46B78AA0E3FAAC01F63B207ACD29AEB63EFB35

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\653512280d5ec3f7_0	
SHA-256:	A8670B6881AC0406E1C6FEC3238589BEB59163D2BF42156798C906B64868A16B
SHA-512:	718551E2CBE6683CC774A6A9B1EB94ADC770171220016B04FFE0FA6E65D2FFE5E144CCD5F58569CF5AD880AD8C45EA915E4758C7E45A1F3FC6E62B902168AE 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B...-....._keyhttps://s.adroll.com/j/sendrolling.js .https://lucidpress.com/we.+J'/.....YG.....8E...W5....r!.+'.(.^3...A..Eo.....c.....A..Eo.....0\r. .m.....B...-....._keyhttps://s.adroll.com/j/sendrolling.js .https://lucidpress.com/\$.+J'/.....a.....YG.....8E...W5....r!.+'.(.^3...A..Eo.....E.=.....A..Eo.....0\r..m .....B...-....._keyhttps://s.adroll.com/j/sendrolling.js .https://lucidpress.com/..1,J'/.....YG.....8E...W5....r!.+'.(.^3...A..Eo.....WP.D.....A..Eo.....0\r..m.. ....B...-....._keyhttps://s.adroll.com/j/sendrolling.js .https://lucidpress.com/...J'/.....>.....YG.....8E...W5....r!.+'.(.^3...A..Eo.....A..Eo.....0\r..m.....B...-.... ..._keyhttps://s.adroll.com/j/sendrolling.js .https://lucidpress.com/..D-J'/.....Sh.....YG.....8E...W5....r!.+'.(.^3...A..Eo.....`.8.....A..Eo.....0\r..m....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\665496601399c43a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	723
Entropy (8bit):	5.387978249244749
Encrypted:	false
SSDEEP:	12:KIbhjahIvqrrdgzyNIIbhjahI87rdgzArIIbhjahITvMrdgzM:Rhj1v8dg2NXhj18vdgwXhj1jqdgQ
MD5:	B216D869DD40F6DBCB44FBDE3B3E2C21
SHA1:	275DDA5D0F18BF21E7A9F396C88D4A8E7B358FA2
SHA-256:	E5A0AD3F4E0566E5171C1496BEEB2E048FF829CEEBDE1D2AC83A3D85586B9E60
SHA-512:	3D19A97AA68483832E9D72EB04661619B466BC2866935AE07765A76A151667B6879267FDDB35CB6F08A3FE0A4DDB28E9DE07629E792F703CD3E596981DA0FC1F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m...g#o....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/marketo/load-forms.js .https://lucidpress.com/..|,J'/...../.....9..i.....^..}V:.x|s..... e...A..Eo.....9.....A..Eo.....0\r..m.....m...g#o....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/marketo/load-forms.js .https://lucidpress. com/.M.,J'/.....L.....9..i.....^..}V:.x|s.....e...A..Eo.....Xx.....A..Eo.....0\r..m.....m...g#o....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/ma rketo/load-forms.js .https://lucidpress.com/..i-J'/.....l.....9..i.....^..}V:.x|s.....e...A..Eo.....>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\669cabd97da730ba_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	168800
Entropy (8bit):	5.967898534959525
Encrypted:	false
SSDEEP:	3072:i8N/IaRGh5LyXhWs7gub3SZ0Yl8hl/GDzF38CUc:iajGh5uXks7gISZk//yUc
MD5:	79A0C8CDA0726297A95ABCD3796749CC
SHA1:	EA15D91D0463F0BDB495EBCCCC104F56CC720C46
SHA-256:	48C9C3712D001250E24DE24C089F6EC0DF4195BE6D0960ED8253A88340E6709F
SHA-512:	F850965DE7F6F84009BB48EB8111F38C6F8F7231373F6ACF82FDEDA940CF04B66744442769D5AD95FAF2DB960CB68F7CC6C2A55309C75E1B2C2032F8D97FA94
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...s..Z....2AA8C8329D3B8368279A0F0604B23FF521801A9454F62DC7E2D1FA03CC58CEB3.....'..U....O2.....(....S..|...|...$..... .....&.....D.....(S....S..`.....}.L`.....L`D.....Qb.E.....mcl..(S.....la....h.....c.....1g.....,..Qc. <.?....mclaa...E.@.-....8P.....*...https://app.lucidpress.com/js/metriclogger..a.....D`....D`*...D`.....%....`....&...&...*D&...(S.....Qc.....mclba...a.....lE...,d.....&. (S....`.....,L`.....`.....Le.....Qc..".....window....Qb:2.....self....M...Qb.#7.....Math....(Qh.."....Cannot find global object.....K`....D... .....z..%&..&....s.....1.. ...&.%.1.....&....s.....1.....&....s.....1.....&....s.....1..'...&.(...i...%%.*..&...(...&....g....%..%.L.&..)....&...&.]. .....(Rc.....Qc&..~....mcl

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68382e91bd491a4a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	714
Entropy (8bit):	5.496497398659804
Encrypted:	false
SSDEEP:	12:dtbhjaHRhADvnvNftbhjaHRhe5vnvqftbhjaHRhHx8DvnvI:dJhjWvAXNfJhjWve5XqfJhjWvHxcXI
MD5:	1136F832FD3696C72AED50654E56F6F5
SHA1:	1058C7F5023794943630FE56AEFB6A078C2CB24A
SHA-256:	0E51E212E992B91E1B519D6D444AD8B4BCC1170267B75F390E4A1A3C2434E7DA
SHA-512:	A32484A18636C0F809BE1C5F241086744541BAD8D51F6DFA7E60AFC9B726DED893A86857350D45910E880D8BC1EA4E6162B9DA75BEC5F95F5C235C8BA453D5D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68382e91bd491a4a_0	
Preview:	0\r..m.....j....5.|...._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/nav/core.js?qwihau .https://lucidpress.com/...,J'/.....=3.....F+.....J.H..pH....rF..,_U..<...A..Eo.....wH.....A..Eo.....0\r..m.....j....5.|...._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/nav/core.js?qwihau .https://lucidpress.com/=..-J'/.....W.....F+.....J.H..pH....rF..,_U..<...A..Eo.....A..Eo.....0\r..m.....j....5.|...._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/js/nav/core.js?qwihau .https://lucidpress.com/..q-J'/.....o.....F+.....J.H..pH....rF..,_U..<...A..Eo.....8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\69c52365d1e07cb3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1818
Entropy (8bit):	5.75733214853486
Encrypted:	false
SSDEEP:	48:xkZJ/7+5hRTF4TTOp4bXBxqqdN/dpoA/YrACZ+:WU51SSp4bSWqA/ri+
MD5:	9B7102C697677C55B54C6661D46AE055
SHA1:	9318300B47C71E2B6FA72567234001014DE9C425
SHA-256:	D1A7028CDF259692323A6D722E12D1AE03E3AC4C3C938E0D2D07465C1E895A84
SHA-512:	ADB8D746BD3D1408A16B6D538C566EE0622DF6C10E24110AF07BD1A2D9DE347CBF34AB69771336656CE8849A8F2D4C742E95491C627490D5AC44341B03780D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z.....=....._keyhttps://www.lucidpress.com/pages/1571-3de1b972d9fe07c0c6db.js .https://lucidpress.com/K..*J'/.....W...2.q...6ow.,..fp.....]J.{.|.A..Eo.....).cS.....A..Eo.....K..*J'/.....'.....O.....oD.....(S.x..`..... L`.....Qb:2.....self.$Q...8.....webpackChunkpress_gatsby..Qb^B.....push.....`.....L`.....`.....Ma....F...`.....b.....C`.....(S...`.....(L`.....PRc$.....Qb..X.....o.....Qb.....n.....M....S...QbR8.+....c...d.....QcL.....31571...`.....Pd.....push.31571..a.....(S.....lar.....e.....@.....@.-....LP.!.....=...https://www.lucidpress.com/pages/1571-3de1b972d9fe07c0c6db.js...a.....D`....D`....D`.....`....&...&..A.&.(S.....5.a.....QbF.....t.....a.....a.....Qbb..{....d.....Pd.....lazyHydratea.....Qd.9.....lazyHydrate.....d.....@.....&....D`....D.,Qi.C.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6cf670600583e2ad_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10199
Entropy (8bit):	5.664551762678881
Encrypted:	false
SSDEEP:	192:bi+aRFm1AXuiB+LgBvg49kNp44NlQyC/ihm+:p2FeYBI49wvEyCKm+
MD5:	9551251796CC4C0338DAB03BBCE7D974
SHA1:	043ABC6E1822D03216054FFC08AA7A8BF21AF912
SHA-256:	FEA857F0C9BAF4E06372EB8CF4C5F4FF881E00DFA122C88D0D95D2275EC87E00
SHA-512:	3D9A13507FC377095FF746556C1FEE9D5AAB31090195EC70423EF7584A334070E8954AE85E2EFD5168AD6070E769BDEDD87B191821BA78060D3443E4312AA9A1
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....$...._keyhttps://d2slcw3kip6qmk.cloudfront.net/common/js/tsDeps-20171101.js .https://lucidpress.com/.*.*J'/.....=.....M.ER..2...7....7...z.....A..Eo.....Y{E.....A..Eo.....'.3:....O....P&.....[.....(S....` ....<L`.....L`.....Qcn.....Reflect..(S....`x.....L`l.....Rcl.....QbF.....t.....Qb.F.....s.....Qb*.....p.....Qb2G.....l.....Qb.(.....y.....Qb.....v.....Qbb..{....d.....Qb.qj....w.....Qb.w-K...._.....Qb..p.....E.....O...Qb...b....T.....Qb...y....k.....Qb.Z.....O.....Qb..$.....m.....Qb.8.+....j.....QbN.T.....M.....Qb.....R.....Qb..z.....W.....Qbv.....z.....Qb*.(.....C.....Qb.\.....F...v$.....I`....Dah....4...(S...IaO.....QbvE".....e.....@.-....PP.1.....B...https://d2slcw3kip6qmk.cloudfront.net/common/js/tsDeps-20171101.js..a.....D`....D`"...D`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6d222a8160032f40_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	741
Entropy (8bit):	5.408613664270246
Encrypted:	false
SSDEEP:	12:Nbhj8BsevHpnbhj8Bw0MvKnbhj8BtL9UvI7:phjcsmbhjclzbhjczN
MD5:	8D9F66F7515024B3EFD1227F323E67AA
SHA1:	47180BD3DFA23DE0BD155DBF88A90C847BD667A0
SHA-256:	CD0B7575675616518A6FC3208A14B79CCA435E6252F49D1B30751756C0B8D5BA
SHA-512:	822BBF685D1AD7DABF73B568C147268E26044EACCC3D7524EAC842BEC1ED4C661D8F4B8360BDFF8BFB229A23F451C049A489AB30EFF668A75FE9F0D2B3380C B9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....h....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/templates/nav/nav-ad/nav-ad.js .https://lucidpress.com/...,J'/.....x3.....Y.....h..}.tDd.....<.(@.B...3.A..Eo....._.....A..Eo.....0\r..m.....s.....h....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/templates/nav/nav-ad/nav-ad.js .https://lucidpress.com/.g.-J'/.....6W.....Y.....h..}.tDd.....<.(@.B...3.A..Eo...../&.....A..Eo.....0\r..m.....s.....h....._keyhttps://www.lucidpress.com/pages/sites/all/themes/lucid/templates/nav/nav-ad/nav-ad.js .https://lucidpress.com/..q-J'/.....p.....Y.....h..}.tDd.....<.(@.B...3.A..Eo.....i.<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6ee33651a10082bc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.662232116535982
Encrypted:	false
SSDEEP:	3:m+lWD8RzY8GjXdXm2O5dTUMu7wvGimtNjlPDYVAbAzERcoG2Gom5maBpK5kt:mgY8SNXmZdTkQGdB5hRcoh+4wK6t
MD5:	B89CCBBC23761E5187A71586A4242F86
SHA1:	078A7D4E754E437CE5A531AA0B2D852343E46E89
SHA-256:	1C109D7CB2AF889AC76A0B9B5D283E1FABDB45765F953C28C2ADAAC71C79D942
SHA-512:	B25FDB1D60884C67F52BBDFD1C71748FDC338AA8B13993A7B10E37C9F3C61A5E1C4D6E61185E6CB12238D678DC0CF1F82DFFC4C70F4EFAC0A17FD1A2C0771E6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....g....._keyhttps://pub.lucidpress.com/292c4e00-83b0-4a5d-84f0-b0f2e3086142/en.js .https://lucidpress.com/..$J'/.....,W..N.H...Q.Ok..9...{.]..5S.A. .Eo.....K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7050a61d8ecb7565_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.640778840670169
Encrypted:	false
SSDEEP:	6:mudXY8SNXmZdTPJ7QGIZh3cdn/Iz4k5/llhK6t:r902vPJcFh3M2Zhll7
MD5:	95FA3D405DF01ABDAC9999ECD47FDDF0
SHA1:	9434C207C3BE863389F1402F022FF17594C4E154
SHA-256:	EEEA8C4D2C418259B676758EBB40D72D90D2C01AE759E2E3623A581754E6B634
SHA-512:	C96874883239B0E779C4B59ECF94506D389CEE57444BC5657E37D2DA2C8064BAADBAFCAD86C00AC4DB7A19CA222D6652F60EBCE812380DDB0685DD6654C511A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...XO.A...._keyhttps://pub.lucidpress.com/292c4e00-83b0-4a5d-84f0-b0f2e3086142/i18n.js .https://lucidpress.com/6L.$J'/.....p.....?.RqP..|.....FF.+}p...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\70c4e67f3fb74bfe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1344
Entropy (8bit):	5.6136264388924575
Encrypted:	false
SSDEEP:	24:ItvNk12tvNI2tvNSa2tvNwp2tvNZRSzbX2tvNmvK7:Id62da2d8a2dyp2dR072dgvq
MD5:	3B86B7BE6F293C6AD3EF218E9B601EA5
SHA1:	63F7EDFBA4D9F0916581E2FF300E1D5A467BE34A
SHA-256:	68460AC49D2DBA4D3F20C9CB519F5750FCE9C82B44E7E635BD5EF6CF61889A3F
SHA-512:	40C3356742C69E45A351F7C835F9AA7BFF2E1915941A203DAEE33F9D31B71BA08F967227E8C7746C631BB90372E889178938E81947778EA2FCA3D30D75CFE914
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\....._keyhttps://js.hs-analytics.net/analytics/1628017200000/19908047.js .https://lucidpress.com/...+J'/.....^.(...l.3.^a.T.p.\."... ...!l...A..Eo.....A.a.....A..Eo.....0\r..m.....\....._keyhttps://js.hs-analytics.net/analytics/1628017200000/19908047.js .https://lucidpress.com/D..+J'/.....^.(...l.3.^a.T.p.\."... ...!l...A..Eo.....(.....A..Eo.....0\r..m.....\....._keyhttps://js.hs-analytics.net/analytics/1628017200000/19908047.js .https://lucidpress.com/...,J'/.....^.(...l.3.^a.T.p.\."... ...!l...A..Eo.....t.....A..Eo.....0\r..m.....\....._keyhttps://js.hs-analytics.net/analytics/1628017200000/19908047.js .https://lucidpress.com/..,J'/.....3=.....^.(...l.3.^a.T.p.\."... ...!l...A..Eo.....fN-.....A..Eo.....0\r..m.....\....._keyhttps://js.hs-analytics.net/analytics/1628017200000/19908047.js .https://luc

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\717025da8c1cabec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.538064551711969
Encrypted:	false
SSDEEP:	6:myQ/VYGLUxGBztT2mABSguG3BYlHaFanu7aD6Yx7bDK6t:tTGBt6mkSguGJAnu7I17J
MD5:	78BC2A0C216558DACD147629D1BC4A27

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\717025da8c1cabec_0	
SHA1:	470BAE5BD3E3C30C6787B0BA7571380B93A701A5
SHA-256:	5A51531EE0A9C4F1D1C2A3E06CB14B4579C8F73AD2AA8AC89C725124F3C42A22
SHA-512:	C23F9C1EF3C91F26394244049DAF721FFD4530AB3A3A3506E25F4582C9341AA0FE9677D714BB78DE57E6D22510CB9C91BEF9CC03BC4F108B70B5D9C599C60EA 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...~8.U...._keyhttps://www.youtube.com/s/player/2840754e/player_ias.vflset/en_US/embed.js .https://youtube.com/:jA,J'/..... .....8B.c.m.q.....u..B.iX.... A..Eo.....I..b.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73c009e4d2d837cd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7931
Entropy (8bit):	6.0718042409539335
Encrypted:	false
SSDEEP:	192:69F0apIJXjdbjFlFua3oaYxDwHh+Ax8V3d:QF0x1djLsamwHZx8VN
MD5:	1FCCE2FE1FA53879916002AEE59E7CD7
SHA1:	42B1A60AA91D8006F19680D338195F564AF36635
SHA-256:	1B7568DA0DAA23607256DFEEB7B604D55DDC11A71E21BA4A2ED1DEEF48F8246D
SHA-512:	99CF1A7D4DAE11F1A74E1A27C79FFC5D74AE3B72F32E28EE0275E278178D028EF810651E6A1C3BFB2C42CA06F78924FFBF9EDFB0D1C89B3F0B14D1C0F45279 E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S.....l...._keyhttps://snap.licdn.com/li.lms-analytics/insight.min.js .https://lucidpress.com/oa.*J'/.....9.....|.....dZ)..E..:.&...x..y.*.#..A..Eo.....\Z.V.....A..Eo..... .....'.....O.....{M>.....0.....(S.0..`.....L`.....(S....`.....L`J.....Rc`.....(.....QbR8.+....c.....Qb2G.....l.....Qbj..z....r.....Qb.F.....s.....Qb..X.....o. ....Qb.w-K...._.....Qb.....v.....Qb*.....p.....QbNq.H...f.....Qb..v.....l.....Qb.qj....w.....Qb...y....k.....Qbj D.....A.....Qb.....R.....Qb.7.+....U.....Qb.9.,....L.....Qb.Z.....O.....Q b.....N.....Qb.(.....y...s.....l`....Da....D%...(S.<.`.....L`.....Y...Qc.a.....getTime...K`....Di.....&.e....&.(...&.X.....,Rc..... .....Qb.....n...`....DaF.....a.....c.....P.....@.-....DP.....6...https://snap.licdn.com/li.lms-analytics/insight.min.js..a.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\744438a3b04cd6f2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.487283663846193
Encrypted:	false
SSDEEP:	3:m+l7fc/C8RzYfvd7Y8xPWyjGis+XlHC8DqJMDO/cQT7mqMmoqclltpK5kt:m8UPYt7iGG4YhJdcQT7LnM/bK6t
MD5:	2B2556840121074C24C4576E940B0A84
SHA1:	E81D931602B931274129DDF0B3E17F276B05C534
SHA-256:	2313B75B0A3ED290622D6B1248737E41E239A13D8DCC2EFC787CDB93C876B6FB
SHA-512:	C9A3AA8AC6F2BD683C47C280A6C40F698A26CD749C967E9B27F0C6B112FB321A54CBB69BFF01D9517421A5BD935CD13078370F931F4571D0EE2B8AB3CA44EF 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...i0Py...._keyhttps://fast.wistia.com/embed/medias/f2io542br0.jsonp .https://lucidpress.com/.G.-J'/.....LY..... ...+..YO~.R....@.....&A...A..Eo.....O]... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\74c4cccd4163e69e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	380
Entropy (8bit):	5.9263249499110655
Encrypted:	false
SSDEEP:	6:mMnYy2MbHYViSDrVzR3zSwluiCnfm+XBKUhTHZDGokvYMKcKL/WnK6t:/GMbvAGsuiCnuwKUFHZDIvWclp
MD5:	478EC57EF3F2A0FA7C04D4C1579D0AEF
SHA1:	BB7483C9E3505F2D1C4B87BDDF610501A7F660A3
SHA-256:	EA8CD50F1F83126F51615E6530D32631111910D1B3B5C26A4A65C7776FC06D43
SHA-512:	AA401E53FAF0E4E99827A3EA837CA53B8BCDAF5B76B153095FF6CC201D5EC48C7CAD5FEFAC4684441A339EC9067A9C1C1336B8C35C0E42BC7F8D98B50070D 46
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\74c4cccd4163e69e_0	
Preview:	0\r..m.....p....._keyhttps://app-ab23.marketo.com/index.php/form/getForm?munchkinId=805-PTZ-019&form=1310&url=https%3A%2F%2Fwww.lucidpress.com%2Fpages%2Findustries%2Ffinance&callback=jQuery112409562693395334136_1628049754155&_=1628049754157 .https://lucidpress.com/J.@-J'/.....b.....8....."q.....:wd.Ft2.T...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\753ed346724b8042_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.510272843932846
Encrypted:	false
SSDEEP:	3:m+lq3p08RzYfvd7QCeUHljGik7XlHCC/MfCJsOB3TFcScK5mCtpK5kt:mPVYt7LTRGFYCLt4sK6t
MD5:	7A2E7E4F72B68B81E09A13A76832DC17
SHA1:	6AC5A99FA6EC8B45D1B2F8EF55DF1DB2BF91D094
SHA-256:	361E8D612FDEAB4224AACF64E247E2DF5F2150C6CED397A63A6EA0A3466E9C38
SHA-512:	9CF1A093C8A84AE7703CD8C31A6CC2C13B26C58A07567E0CE2261D58C8DDD542706376CF9D16FACC552261AECCAA866776A0F694C28FA7BBFAEEEAFD9BD2 84C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...8.a....._keyhttps://fast.wistia.com/embed/medias/n95q2k1da9.jsonp .https://lucidpress.com/.r-J'/.....zq.....Z'M.m:....4).a:....%d.....[H..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\760b8d90b587e9be_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.878914938475192
Encrypted:	false
SSDEEP:	6:m3+EY4rgdsj//NcttjJJ5YGQBYxt47fgp23wvARSK6t:g77jXNeFYxB8t4cp23I
MD5:	64E44CCA5AEF212EF3477AC8F806DC99
SHA1:	8C6218C3611AE938005042579B052A734C463C8F
SHA-256:	54649FE770BB7974EA233F55FE9F61639AAF6E03ED370B9D22A2C24A8630177F
SHA-512:	35FDDADDCFD63659D885198E16B53AC80F1258F774803CEB68C89DC944B98FD255295F56CB09393B660776041E4E6551CBAF575C21F8D83221600194C3EBD40
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z>B...._keyhttps://s.adroll.com/pixel/DPYX46NNDVH3LEFFJGQU52/2DEQJ47H2BCHDFEEMMMO52/2CTM4X74SRH65AWOK2XUOS.js .https://lucidpress.com/. .+J'/.....x.+..Fj"..L.-F...yQ.....!&...a..A..Eo.....p..T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76bc4d890f98c7fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5117
Entropy (8bit):	5.7275194582725995
Encrypted:	false
SSDEEP:	96:GqvFK+1wp3GaZrhLFnQGyfmUFBjZUVsqt+L0b:XHwp3GaZlRyfmCUp+A
MD5:	788534B0C5BF9E3434769959036EE2D2
SHA1:	16EF6A0E6FEB378AA603C864CBAB29184C1B78A0
SHA-256:	3D75F057BBF4CD44EDA1549BE9D0E06AFAF9F28C58C609E91D160582B1BA5EBC
SHA-512:	D061E50CD11CAD2D9A5C3F17D073202C7D0DCC10E1E13780121F445F9EBA76C41CD7E293F9CC78AE0B7022D3B0461277ACD560DB3C03C8053DC9AFAFDBB0 D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e....._keyhttps://www.lucidpress.com/pages/webpack-runtime-2912c4c8bff1fb38771a.js .https://lucidpress.com/3..*J'/.....r.+....c...R\..4I.$@S;.....A..Eo.....f[.....A..Eo.....'.m.....O....p....l.....(S.0..`.....L`.....(S.=..`4.....L`T....xRc8.....QbvE".....e.....QbF.....t.....Qbj..z....r.....Qb.....n.....M...QbR8.+....c.....Qb..X.....o.....QbNq.H....f.....S...Qbb..{....d...i.....l`....Da....R>...(S.....Ia?.....@.-....TP.A.....H...https://www.lucidpress.com/pages/webpack-runtime-2912c4c8bff1fb38771a.jsa.....D`....D`<...D`.....`T...&...&....&...&.(S.....`r....8L`.....<Rc.....A...A.a.....l`.....Pb.....d.O.a.....Xa.....M.....E...Qb.Z.....O.....Qc.....every....(S.H.`H.....L`.....K`....Dl.....&.(...&.%.*..&...&...*..&.Y.....,Rc.....l`....Da....D.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7897f5c0a911aadb_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\7897f5c0a911aadb_0	
Size (bytes):	55913
Entropy (8bit):	5.901005558813432
Encrypted:	false
SSDEEP:	768:5lZ940mHysGodD7JhfMdt0J4kVe4HvFngjkT6T0320kXHhtBRCH:5rgySnrG6mkVJHdngYT6OVkXHhg
MD5:	35A7F865067B69575C432C3ACFB0B990
SHA1:	77DA3FC8EF116C15AC37A8D17BB181503A486BD3
SHA-256:	7C677079A14FCC0597C1D7AE253B1D09576701D3045BCFD95E48026BAD2EED75
SHA-512:	C418E0D0D40C346AE22982DBEDD1A2C1A0151F96328BCDC2537DFD3210EF2DE56FA23F780A9C3D1E926F591595EBAFEA0C227B7E9772402AB1FF007751213A 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.X...._keyhttps://d5x2n72glkaxl.cloudfront.net/js/cookieSyncClient?compiled=1&version=20210422-142202-054eb930 .https://lucidpress.com/..*J'/..... ..j.....{....z.n..m#.q...J.W.~_.....lMRU.A..Eo.....1.....A..Eo.....'.-.....O.....a.z.....(...x.....8.....D.....(S...y...`.2 .....e.L`.....L`.....Qcn.....Reflect..(S.....Ia.G...H.....d.....,...QbZz2j....cscaE.@.-....pP.....d...https://d5x2n72glkaxl.cloudfront.net/js/cookieSyncClient?compiled=1 &version=20210422-142202-054eb930a.....D`....D`$...D`.....`V...&...&.(S.\.`p....8L`.....Qcn..0....assign...(S.....Pd.....t.__assign..aZ.....IE...#d..... Q.@*=.....__assign.(S.=...`2....$L`.....HRc .....Qb.....n.....Qbj..z....r.....QbvE".....e.....QbF.....t...c....d.....d...I`.....Pd.....t.__decoratea....n....M.....!..QcF.?n... .decorate.e...K`

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\79ada431a13d1e1b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	343
Entropy (8bit):	5.855595097150328
Encrypted:	false
SSDEEP:	6:mWLY4rgdsj//Ncttjdz8TA/7sRG6UYdIX9XpK4wBK6t3hrvYWIX9XpK4/X:Pr7jXNeH7sRiiIX9XKb/rlIX9Xl
MD5:	13B42C2E762A30842B9C33C3BBF8EAF0
SHA1:	17434CAA055864DCF3B67C597DA13E2A647E9371
SHA-256:	E83F96104EC0306D36022672C71078C80F9CDF52D87D3995B32833626B12E1FA
SHA-512:	3908D34181E5FAB0A87EB2B4A6AB9023D27FA61F20B34302F7543A338DCC22C97D1F08D21FECC65593DFE8FD17AABB4AF002E1DE7A6BBBFCB15DFAF6FF638 DED
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://s.adroll.com/pixel/DPYX46NNDVH3LEFFJGQU52/2DEQJ47H2BCHDFEEMMMO52/EGVXETWO6JB5DGYNJAFJKF.js .https://luci dpress.com/o..+J'/.....h.C.5..Uv.._.A..!~...g.<?.>.0.A..Eo.....L.....A..Eo.....10,J'/.....h.C.5..Uv.._.A..!~...g.<?.>.0.A..Eo.....gv.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7c0da8815cfc18e0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5970
Entropy (8bit):	5.672915158870535
Encrypted:	false
SSDEEP:	96:XxK0oS8hdDQPIpECJW4YU/xljlNqNjL1NQ7d4tglAj:XkS8hlGIpv5xlJNqNjZN9glu
MD5:	1EA3607E0EDEBBE47AB6638F082C713A
SHA1:	78305FBABF3F35C9CC33A324F723153CE3AADD8E
SHA-256:	3553CD511BF353D55A9CE66FF9849D1C90A234033A1C60DDDF2C786C0F12EBA6
SHA-512:	8A478B4E091CF2C57FE5DB92C8F9BB70707D0550757383BA072CE3FBD6AFA3560E404622CCC05B9FA210361971B732C79F7F7782F380774C85DD47ADAC550B7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....._keyhttps://d2slcw3kip6qmk.cloudfront.net/common/js/userTimingPolyfill.js .https://lucidpress.com/..w,J'/.....5..E..3$4...@N./...D<.a.O2.8.. ...A..Eo....."....A..Eo.....'.5....O.....,.....0.....(S.@..`:.....L`.....(S...`.....L`j.....RcD.....M...O.....QbRp~.....h.....S...Qb.kM.....j. ....Qb..7O....k.....Qb.....l.....Qb.l.....m.....QbB2w.....n.....Qb.G8v....o.....Qb.....p.....Qb.....q...ld.....I`....DaF....(....QdZ.....performance..,Q .....G...._perfRefForUserTimingPolyfill.....Qe.....userTimingJsNow..$QgvZ.D....userTimingJsNowPrefixed..$Qg.....userTimingJsUserTiming...,Qi..eJ....userTim ingJsUserTimingPrefixed...,Qi...7....userTimingJsPerformanceTimeline..4Qk....'...userTimingJsPerformanceTimelinePrefixed...Qb".....now.....`.....M`.....Qdn.....web kitNow.....Qc.....msNow.....Qc2..l....mozNow

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\85763b6d81129b54_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.894672116376534
Encrypted:	false
SSDEEP:	6:mVMY4rgdsj//Ncttje2LIGycYDT5nmuQoErGDK6t:b7jXNe7LIy25nvH
MD5:	9F1195BA83EA218366E1335F9D6DEE50

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\85763b6d81129b54_0	
SHA1:	BEC467C98432851F72110D2E53FCDCD5E6483DD6
SHA-256:	D7A796CDBF0441AD528BC31546B41A411DAE12005E22D825734199CA0E77C6A2
SHA-512:	3F8C69F7DF5D92897382BED484A88BA7C129E30C339A3D6B79AE1000CBB419D9EA07BA149A809ECCCEC335018972E186DB22A18298ED8ED1E91E75B5967178 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}...._keyhttps://s.adroll.com/pixel/DPYX46NNDVH3LEFFJGQU52/2DEQJ47H2BCHDFEEMMMO52/ZPOEDXQGG5HMJCGDSDMVVG.js .https://lucid press.com/g..-J'/.....&.....''...g5.....Z.o.a+.f.A..Eo.....T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86148923446bd99f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	645
Entropy (8bit):	5.505750874567768
Encrypted:	false
SSDEEP:	12:BExqhRhg8Pr5NLExqhRhM63rE7LExqhRhJMrMN:BSqhvXTLSqhvM60LSqhvJFN
MD5:	423B3D560425E9B983DFD4E9C4A5A7A7
SHA1:	14627D48B83F7EC23346DE038C0C73CF03CD62B1
SHA-256:	E1F2D76237AAD8E600C5B91EC7772398858835AE53184C1E1464A4F62380B28F
SHA-512:	20E48F896F7A3B32E550A9752C3CE1BD573A9D27CDF914CBF75D9107BA400C16571C5B8D0EF12F074EFFCEFE2FFA94E2E9BB1DFA33AD75E3CDE4AF56CDC5F 0CD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....xv-...._keyhttps://www.lucidpress.com/pages/misc/drupal.js?qwihau .https://lucidpress.com/v.,J'/.....;3.....[...Fw....].PD&;....}.y|...|t..A..Eo.....s.....A ..Eo.....0\r..m.....S....xv-...._keyhttps://www.lucidpress.com/pages/misc/drupal.js?qwihau .https://lucidpress.com/8\.-J'/.....W.....[...Fw....].PD&;....}.y|...|t..A. .Eo.....*.....A..Eo.....0\r..m.....S....xv-...._keyhttps://www.lucidpress.com/pages/misc/drupal.js?qwihau .https://lucidpress.com/..q-J'/.....o.....[...Fw....].PD&;....}.y|...|t..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\879405f047052d89_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	587
Entropy (8bit):	5.661334154884849
Encrypted:	false
SSDEEP:	6:mwn/VYyyf0Gb9Y8lhfeb0nK6tBBXl0UiTdXKLlEcelbfeN3B9Y1/DfedsPB9Yytp:dO0c80pRyklmoSDkspDiQx
MD5:	B8C1B47EEC52AD7915CF94491620FDF4
SHA1:	7C1E032CBB5CFEF90730F4AACF49A7528B4C65EA
SHA-256:	F868B2169CDE218D312DF193303D8E4A4A313C8AA2AB497EE9EE0EE062842760
SHA-512:	5EC6B9E5C25DC6C2A7B4E510ACCA2E9F5E7EB3D1D615997B9C00B10348E60E5FD556100840D5B9D73BB4E60841A6AA4F7AAA804F46C3A3C3E24B3B6C696143 E5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G...''{.4...._keyhttps://app.lucidpress.com/js/metriclogger .https://lucidpress.com/E..*J'/.....`..D.{.u!6o.#E.....x\..*Bv..A..Eo.....o.....A..Eo..... .E..*J'/.....2AA8C8329D3B8368279A0F0604B23FF521801A9454F62DC7E2D1FA03CC58CEB3.`..D.{.u!6o.#E.....x\..*Bv..A..Eo.....fG..L.....E..*J'/.....3.....`..D.{.u!6 o.#E.....x\..*Bv..A..Eo.....}l.....E..*J'/.....X.....`..D.{.u!6o.#E.....x\..*Bv..A..Eo.....).].....E..*J'/.....Dp.....`..D.{.u!6o.#E.....x\..*Bv..A..Eo.....vh.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8b047c8ca3185f09_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1404
Entropy (8bit):	5.736245147941755
Encrypted:	false
SSDEEP:	24:shDR7HahDR486ahDRRskrahDRV6ahDRRTGahDRzYut7:shD1HahDf6ahDUoahD/6ahDDTGahDBYa
MD5:	64FB6813868DCF0598D8A60436E127DA
SHA1:	F451A28B9E4B1F0F44A37F8725BF8F70DC9839FB
SHA-256:	C29FE8F7EEF225681A358AC152C254911DE1FCE9C9482EF3851915740B612482
SHA-512:	A6C3E027A796CD295A6CA8934E52726AD54EEDEE374E7191F95DF460A645EACCE01F975EBD179333BB31D17E7C06FEDF49BFEB6FF23E8ED2D5F6F0BB65EF1 F4A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8b047c8ca3185f09_0	
Preview:	0\r..m......f....?......_keyhttps://www.googletagmanager.com/gtag/js?id=G-QEXLWR84HV&l=dataLayer&cx=c .https://lucidpress.com/.h.*J'/...................V..p.n...)..aV... \....'@N._e.....A..Eo......P.M..........A..Eo.................0\r..m......f....?......_keyhttps://www.googletagmanager.com/gtag/js?id=G-QEXLWR84HV&l=dataLayer&cx=c .https://lucidpress.com/h.z+J'/...................V..p.n...)..aV...\....'@N._e.....A..Eo..................A..Eo.................0\r..m......f....?......_keyhttps://www.googletagmanager.com/gtag/js?id=G-QEXLWR84HV&l=dataLayer&cx=c .https://lucidpress.com/R..,J'/............a.......V..p.n...)..aV...\....'@N._e.....A..Eo......a./.........A..Eo.................0\r..m......f....?......_keyhttps://www.googletagmanager.com/gtag/js?id=G-QEXLWR84HV&l=dataLayer&cx=c .https://lucidpress.com/m..,J'/.............6......V..p.n...)..aV...\....'@N._e.....A..Eo......g".6.........A..Eo.................0\r..m......f....?......_keyhttps://www.googletagmanager.com/gta

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8df26d7862269223_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	189448
Entropy (8bit):	5.94242938636841
Encrypted:	false
SSDEEP:	3072:uLG1rvYqQSzJu4zT+P2WQR4rhOCjR58fmOVLaFRn+jcgWx:OwjoSzpz4BQRGxj4fMJgWx
MD5:	6557236235D2D5973B10ECCBEBD3F0AB
SHA1:	CB710723ABFCD514D371C844EDBA1852E2EEAE38
SHA-256:	16AF9F914BC857590CB0B6F479B2A80521432E8C20BEA4FBC9F7E14720BEE307
SHA-512:	C6845229F826A92AF013AF51DE5A32B5A386EA93A794A8992F0E23481F08464C805F4204221F5FBD8D3D4F4B634F6623F4A528D3F91FCECA81C30E44FA394C0F
Malicious:	false
Reputation:	low
Preview:	0\r..m......@......x....7CCDEDC602480CE9333CB637D243A860790E0341DE655FE79060FB5F85DC004C.............'.......O8...X..................(....P..0.................................. ....&...................................4...........$..(S....P..`r......1.L`.........L`<.....Qcn.......Reflect...Qb...a....beca.(S.....Ia.G..8H......d.................,...Qc..V.....becaa...E.@.-....hP.......Y...https://d5x2n72glkaxl.cloudfront.net/js/bacon?compiled=1&version=20210422-142202-054eb930...a........D`....D`(...D`............`N...&...&...(S.\.`p....8L`.........Qcn..0....assign...(S.......Pd........t.__assign..aZ.......IE..1,d.....................Q.@*=......__assign.(S.=...`2....$L`.....HRc................Qb......n.....Qbj..z....r.....QbvE".....e.....QbF.......t...c....d.......d...I`......Pd........t.__decoratea....n....M........*..QcF.?n....decorate.e...K`....D...`...(........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8fe07a2eac9bbdcf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	81160
Entropy (8bit):	6.073311780402887
Encrypted:	false
SSDEEP:	1536:qVb4lmDNt9dJhaLGokdfWk7o5cEO9Me/YdC2GbuIfh5WZlqF9dzAA:y4lMt9hXokdWP5cEO9VwdC7b9fh58AFx
MD5:	09A3DA08592094A7F1A4ABA93D5A66E3
SHA1:	2F8C6B1661E633507A451CF920C3FC317A578541
SHA-256:	FD6DF23E31EC1523350078478C5CED5130F171FFD7E953D57D365050599AC761
SHA-512:	1B7FFC60FEF5E9F6E938496A1C00AE5D990E81B3A610D0AADE7C08141D05C3E7D51ED9E664439DE31D4560FE64EC6B7BF74E9DE175FA3520FDD64CB42638261
Malicious:	false
Reputation:	low
Preview:	0\r..m......@...j7t9....B95C478DA5630A1B1CA32F428436518A98511E18FEDFCE0FCB735D56E573231E.............'.......O.....;..DY.............8.......`.......D............................ ...........\...................................t....................(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc............R.....Qb......n.....QbZ..k....q.....Qbj..z....r.....QbF.......t.....Qb........v.....Qb2&......x.....Qb.(.....y.....Qbv......z.....Qbj D.....A.....Qb.`.?....B.....Qb*.(.....C.....Qb.\......F.....Qb..p.....E.....Qb.v.....D.....Qb2..f....G.....Qb.@-/....H.....Qb2.F.....J.....Qb..v.....I.....Qbzg.B....K.....Qb2..$....aa....Qb.9.,....L.....Qb.......N.....Qb.Z......O.....Qbv......P.....QbN.T.....M.....Qb2.~1....da....Qb6<......ea....Qb.}.M....Q.....Qb6......S.....Qb.......R.....Qb........ia....Qb.7.+....U.....Qb..N.....ha....Qb...b....T.....Qb*V......V.....Qb..z.....W.....Qb..f.....Z.....Qbr.%.....Y.....QbFs.I....X.....Qb.v......ba....Qb.._....ca.....................................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\912d957790332ec4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.6028494954162475
Encrypted:	false
SSDEEP:	6:m1YGLUxGBzPv2c7MN7GSzYYYmKqnWrPllZK6t:rGBPv2cIJPlnWjllT
MD5:	4EE9D79869263D3F2353EAD281333454
SHA1:	F1AEEDA0F759F514EA5A38A0E3A59B10EDB0B317
SHA-256:	60005433F7DBF152267CAE91DAB8AB330A9A2531634F3DFC94FF5DCC2856E138
SHA-512:	4BD39ADC908EB018EE5AC1EC5EDFF6964098C6E441C76127681242037394FBF00C9DDC92DD7D88ADE945CE298E2096AA68C392FF7C19D3FE09351AF48B96B1B
Malicious:	false
Reputation:	low
Preview:	0\r..m......l...Q.M....._keyhttps://www.youtube.com/s/player/2840754e/www-widgetapi.vflset/www-widgetapi.js .https://lucidpress.com/..3,J'/....................Hq.x....B..?.[4C{.v......j9.B..A..Eo.......8...........A..Eo.................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\94e7ece914e4fd2a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.393587642470385
Encrypted:	false
SSDEEP:	3:m+lpd7/6OA8RzYfvdJhE/WME12uRvGiN+a+1lXlHCNvlYk3cu12shRmBg71pK5kt:mudzXYtJQeGU+TvYNvDMs/AB+K6t
MD5:	C878817EAC1FF3E67416AC3E98AFAC0D
SHA1:	AD119E11AEE338E7380C6A6D78CFE2070FB86E9A
SHA-256:	A114F5CAFA4232C976F471E4E8843A24A5489235DFCA487F35F6805808151C46
SHA-512:	791DF27C7B26EC0150B139F5EB2F1CA4DAEEE023742446EBC01D6102D6914486E696EA7D2D3DF4BB4FBF675FB65920B9DD59D8984EEA18520C7F8ED967C336 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....x7....._keyhttps://fast.wistia.com/assets/external/wistia-mux.js .https://lucidpress.com/..$-J'/.....Z.....gm..l..r....[...k.Qj^N....{&....A..Eo.....q.^..... A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\97b18308691cf543_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	59302
Entropy (8bit):	5.68427963954646
Encrypted:	false
SSDEEP:	1536:5H+LhYeohutPQoYWD//ZVnri8UkU80FTZzsOB:5H+17ohoPQoYWRVri8UN/gQ
MD5:	7BBC6EEEC103546456B5674B0B4F384E
SHA1:	FC9A9E03EBE4AC57E3DC6978907B59E4DBFACE21
SHA-256:	80E36EA7B8D73EC2CCEE809A1225B59DE78E4F7F00A8D9C2E42CD9829F943CC5
SHA-512:	5093C557A5C116BF88CABEF741CC60D7C3F6385BCEA419F1F7C53FD83F880467F6D907F1784B70F63266B6D1BF3AA441C020D27516FEEC526FC2AAE47DE3D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....~....@$T...._keyhttps://www.lucidpress.com/pages/7334108c79c0ee97fb6a8fe3441190ba93c90256-bb824e31dcb74ca23912.js .https://lucidpress.com/...*J'/... .....V.....~.Xo..)..m.=..Ys.9.....q...K..A..Eo.....A..Eo.....'.*.....O.....(.....h$.....D.....(S.....`./.....L`.....Qb:2.....self.$Q...8.....webpackChunkpress_gatsby..Qb^B.....push.....`.....L`.....`.....Ma....P...`.....b.....t...C`vC..C`\l..C`....C`....C`Jp..C`.a..C`....C`r.. .C`....C`.{..C`....C`....C`p...C`j...C`...C`p$..C`~7..C`.(..C`.A..C`....C`2D..C`hF..C`xA..C`.D..C`...C`~@..C`....C`R%..C`.3..C`....C`*M..C`.p..C`....C`(#..C`....C`....C`~...C`~v..C `....C`.L..C`8!..C`....C`....C`.:..C`...C`...C`>...C`n]..C`....C`....C`n...C`...C`L-..C`.`..C`J...C`.q..C`....C`....C`\...C`Z+..C`....C`...C`6...C`....C`....C`.y..C`p...C`.L..C`.O..C`....C`. ...C`v:..C`....C`..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\97ccc3139b57518d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1242
Entropy (8bit):	5.467882620620875
Encrypted:	false
SSDEEP:	24:4e5cgTOv3zme5cVoOv3Xme5cGOv3sme5cIOv3Gme5cOtOv3lme5cXV3Ov3h:4KmvjmKuvnmKSv8mK0vWmK7svVmKcVeZ
MD5:	9B10C5DAFC1BC47390DB52A637CC7693
SHA1:	87D987F8C6DF11AB2A3DA56D1463D7DC877E5052
SHA-256:	6A016BB6127A56C963C72A8DE74EE771A6F7E62DC236434C725DE09727D722E5
SHA-512:	F82CEC77B373B2F72C655740F8C06ECB076E4625C9659B947207B9FD19A9D393D27CAB11850201E32DFE0E4A4C643D6298DEF45724DAD999BC03B288BDD01F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K...S..;...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://lucidpress.com/...+J'/.....[.....n.s6Q..Ro4.8I...VvbvQRtE"6{.....A..Eo.....B.....A..Eo.. .....0\r..m.....K...S..;...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://lucidpress.com/|dy+J'/.....W.....n.s6Q..Ro4.8I...VvbvQRtE"6{.....A..Eo .....n6m.....A..Eo.....0\r..m.....K...S..;...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://lucidpress.com/.',J'/.....z.....n.s6Q..Ro4.8I...VvbvQ RtE"6{.....A..Eo.....A..Eo.....0\r..m.....K...S..;...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://lucidpress.com//0.,J'/.....7.....n.s6Q ..Ro4.8I...VvbvQRtE"6{.....A..Eo.....A..Eo.....0\r..m.....K...S..;...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://lucidpress.com/3N*-J'/..... ...].....n.s6Q..Ro4.8I...VvbvQRtE"6{.....A..Eo.....W

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99e37995f9d11b6f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1286
Entropy (8bit):	5.599614337111192
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99e37995f9d11b6f_0

SSDEEP:	24:HcmHRHPm4HRQe+knLy19zZaPtdcmH26mH01rm7/YM3rT6rt2a:1FPm4HRp+sO1NQWfl/zrTat2a
MD5:	7B049224F5F9B7F60A262D19D6AC87AD
SHA1:	9A9E073498E5C8C34793F750942DD35C2A048D39
SHA-256:	B71797B6578CABD79A7CFD2DFD1CEB8D90491F373670D4BD8FE4DF64884CE783
SHA-512:	7DE2EAB128A42D69523DA65D3AA6EE5E8B6196EEF0E0F4E5A391C77B23BA10C1C684814A3A93E4B2D7BDB805A0F0C2E90D414B44C3B40F44179C61FC6A668D43
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^.....e...._keyhttps://www.lucidpress.com/pages/d66f1a69-884d63b954c0e6b9b27b.js .https://lucidpress.com/.R.*J'/.....2.o`yT...u...@....A.....~.f.A..Eo.....+.l<.....A..Eo.....R.*J'/.....'..<....O.....|.S.....(S.x..`..... L`.....Qb:2.....self.$Q...8.....webpackChunkpress_gatsby..Qb^B.....push..... `.....L`.....`.....Ma.....J..`.....b.....:(..C`.....(S.....Pd.....push.70685..ak....<.....F.F..@.I.]..@.i.l..@.l.o..@.q.r..@.u.u..@.....*.....P.....P.....8.k%.....U.[..@.\.]..@. .....e.....Z.[..@. .....d.....j.k..@. . ....d.....n.o..@. . ...QctP.....70685...E.@.-....PP.1.....A ...https://www.lucidpress.com/pages/d66f1a69-884d63b954c0e6b9b27b.js...a.....D`....D`:...D`.....`t...&...&..A...D`....D.0QjV.(+$...d66f1a69-884d63b954c0e6b9b

Static File Info

No static file info

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5196 Parent PID: 5112

General

Start time:	21:01:35
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://pub.lucidpress.com/d2d8f4ec-03d1-433d-9635-8d794acb5292/#_0'
Imagebase:	0x7ff77b960000
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: 3528 Parent PID: 5196

General

Start time:	21:01:37
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1312,3565287986375282334,5985329352411713397,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1760 /prefetch:8
Imagebase:	0x7ff77b960000
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: 7324 Parent PID: 5196

General

Start time:	21:01:59
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1312,3565287986375282334,5985329352411713397,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6724 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: 6968 Parent PID: 5196

General

Start time:	21:02:21
Start date:	03/08/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1312,3565287986375282334,5985329352411713397,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=6568 /prefetch:8
Imagebase:	0x7ff77b960000
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