ID: 433426
Cookbook: browseurl.jbs
Time: 19:41:08
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

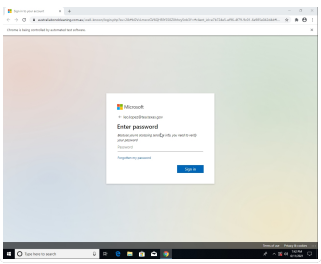
Analysis Report https://list-manage.agle1.cc/click?u=htt…

Overview

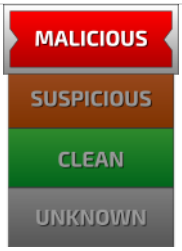
General Information

Sample URL:	http://https://list-manage.agle1.cc/click?u=www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=
Analysis ID:	433426
Infos:	

Most interesting Screenshot:



Detection



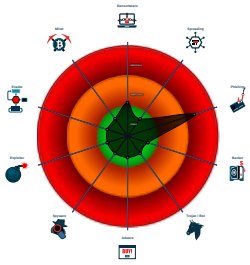
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- Submit button contains javascript call

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6468 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://list-manage.agle1.cc/click?u=http://www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6712 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1624,4652876236295108038,17951007052133139354,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

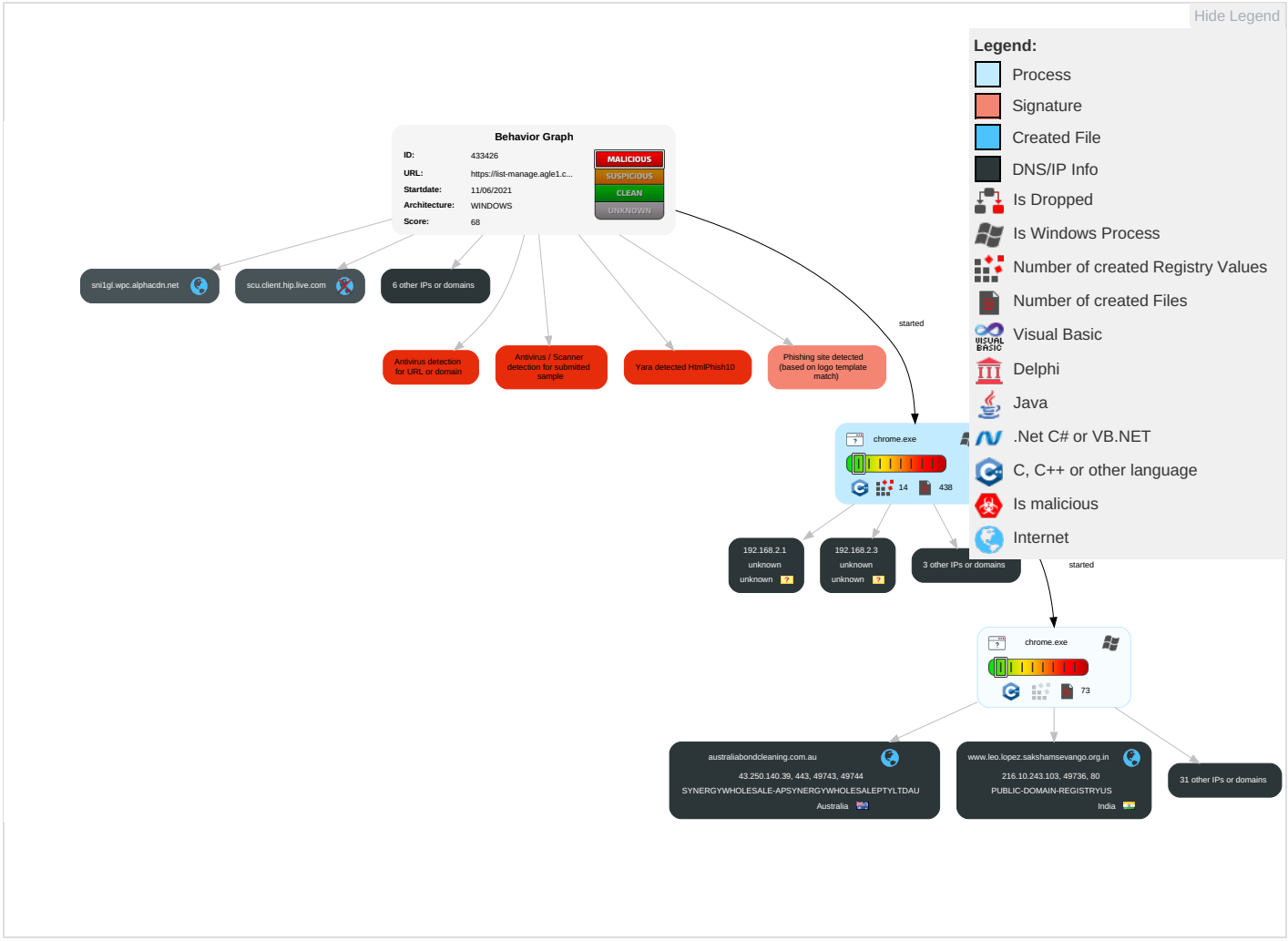
Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

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	Im
Drive-by Compromise 1	Scripting 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Ca Bi Fr

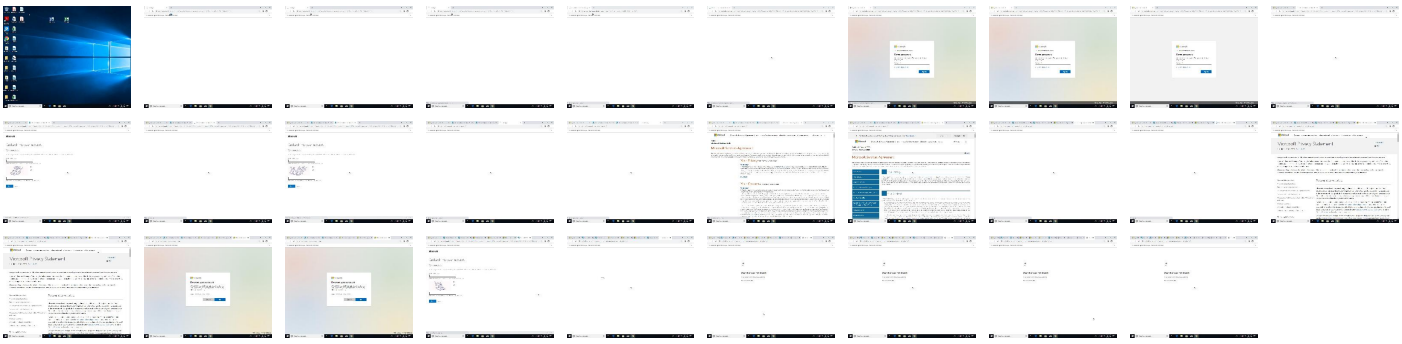
Behavior Graph

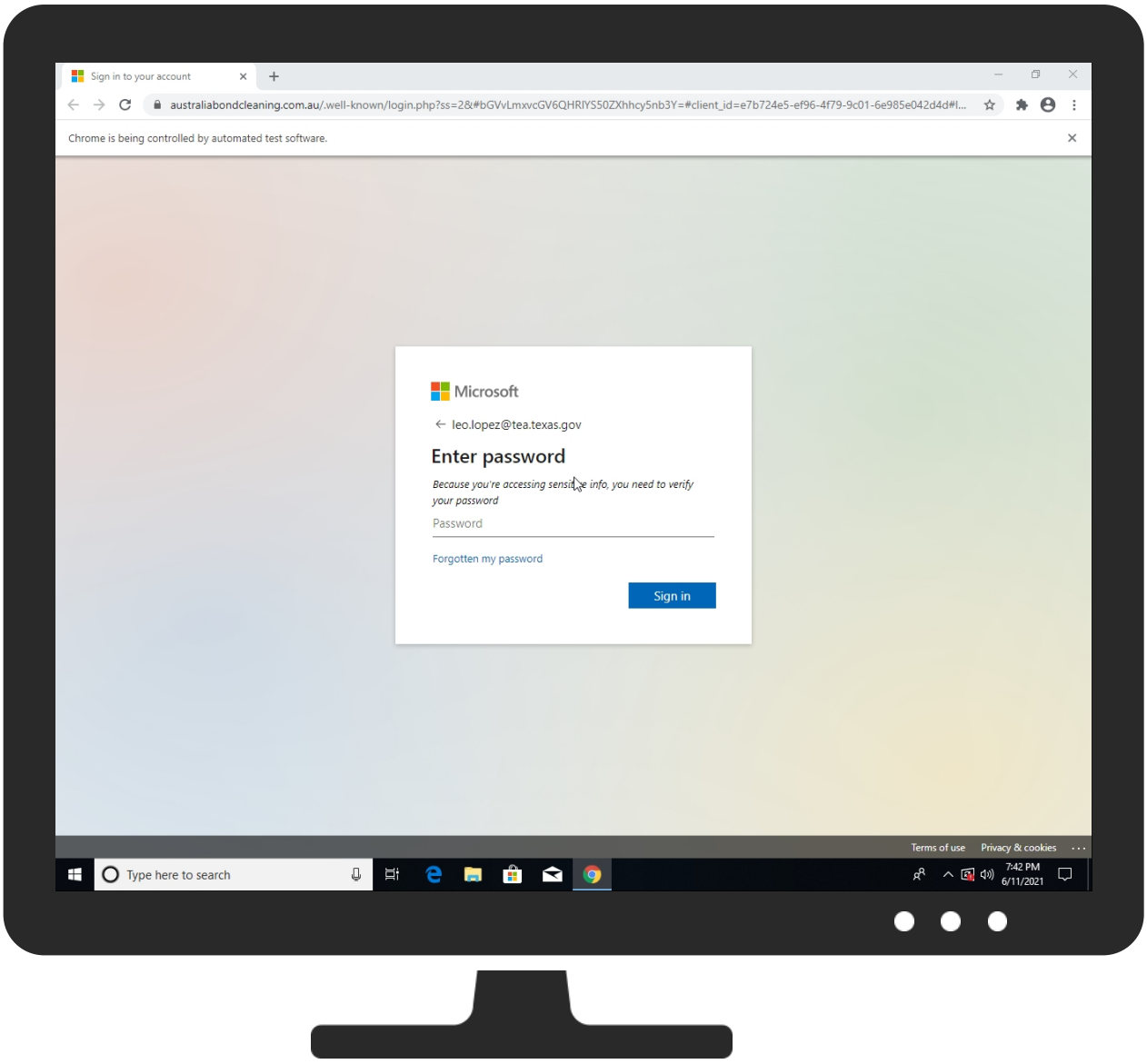


Screenshots

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://list-manage.agle1.cc/click?u=www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=	0%	Avira URL Cloud	safe	
http://https://list-manage.agle1.cc/click?u=www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.australiabondcleaning.com.au/.well-known/login.php?ss=2&#bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=#client_id=e7b724e5-ef96-4f79-9c01-6e985e042d4d#loginpage=https://live.microsoftonline.com#reff=6d17fd2bdeb846c7987fc53a49f81755	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://assets.onestore.ms/	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1	0%	URL Reputation	safe	
http://https://www.australiabondcleaning.com.au/.well-known/?ss=2&email=bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=	0%	Avira URL Cloud	safe	
http://www.leo.lopez.sakshamsevango.org.in/br/?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=j	0%	Avira URL Cloud	safe	
http://https://list-manage.agle1.cc	0%	Avira URL Cloud	safe	
http://www.leo.lopez.sakshamsevango.org.in/br/?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=Sign	0%	Avira URL Cloud	safe	
http://https://list-manage.agle1.cc/click?u=www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlY	0%	Avira URL Cloud	safe	
http://https://www.australiabondcleaning.com.au/.well-known/?ss=2&email=bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=x	0%	Avira URL Cloud	safe	
http://https://australiabondcleaning.com.au/	0%	Avira URL Cloud	safe	
http://https://www.office.com0(https://www.australiabondcleaning.com.au2	0%	Avira URL Cloud	safe	
http://https://www.australiabondcleaning.com.au/.well-known/js/maximum.js	0%	Avira URL Cloud	safe	
http://www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=2	0%	Avira URL Cloud	safe	
http://https://www.australiabondcleaning.com.au/.well-known/?ss=2&email=bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=2	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/resetpasswordpackage_X7k_NcCIooflIFuKCGNtCw2.js?v=1	0%	Avira URL Cloud	safe	
http://https://australiabondcleaning.com.au/I	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.icoj	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js	0%	URL Reputation	safe	
http://www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=T	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://www.leo.lopez.sakshamsevango.org.in/br/?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=2	0%	Avira URL Cloud	safe	
http://www.leo.lopez.sakshamsevango.org.in	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/knockout_old_GJ62c6D9R5HuKFdkoO8XYw2.js?v=1	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.icoP	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/accountcorepackage_YD-Y5A3nlj0ms1Ks9fXU6A2.js?v=1	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1	0%	URL Reputation	safe	
http://www.leo.lopez.sakshamsevango.org.in/br/?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=	0%	Avira URL Cloud	safe	
http://https://www.australiabondcleaning.com.au/.well-known/login.php?ss=2&	0%	Avira URL Cloud	safe	
http://www.leo.lopez.sakshamsevango.org.in/br/?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=P	0%	Avira URL Cloud	safe	
http://www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=Sign	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/	0%	Avira URL Cloud	safe	
http://https://www.australiabondcleaning.com.au2	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauthimages.net	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/wlivepackagefull_2169QIWB52Tqqm3jo5_AUA2.js?v=1	0%	Avira URL Cloud	safe	
http://https://www.australiabondcleaning.com.au/.well-known/?ss=2&email=bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=Sig	0%	Avira URL Cloud	safe	
http://www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.australiabondcleaning.com.au/.well-known/login.php?ss=2&#bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false		unknown
australiabondcleaning.com.au	43.250.140.39	true	false		unknown
HHN-efz.ms-acdc.office.com	40.101.137.82	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		unknown
ghs.googlehosted.com	142.250.180.243	true	false		unknown
googlehosted.l.googleusercontent.com	142.250.180.225	true	false		high
www.leo.lopez.sakshamsevango.org.in	216.10.243.103	true	false		unknown
www.office.com	unknown	unknown	false		high
r4.res.office365.com	unknown	unknown	false		high
aadcdn.msauth.net	unknown	unknown	false		unknown
assets.onestore.ms	unknown	unknown	false		unknown
account.live.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
acctcdn.msauth.net	unknown	unknown	false		unknown
outlook.office365.com	unknown	unknown	false		high
client.hip.live.com	unknown	unknown	false		high
passwordreset.microsoftonline.com	unknown	unknown	false		high
aadcdn.msauthimages.net	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
scu.client.hip.live.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
www.australiabondcleaning.com.au	unknown	unknown	false		unknown
list-manage.agle1.cc	unknown	unknown	false		unknown
acctcdn.msftauth.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.australiabondcleaning.com.au/.well-known/login.php?ss=2&#bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=#client_id=e7b724e5-ef96-4f79-9c01-6e985e042d4d#loginpage=https://live.microsoftonline.com#reff=6d17fd2bdeb846c7987fc53a49f81755	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://www.office.com/prefetch/prefetch	false		high
http://https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2freprocess%3fctx%3drQIIAYWSO2_TUABG46RNH0MpCAESUlUkBoTk5NrXj7oICT8Sp4kT14mT1BFSFL8SO341durGAzNjJ4ayMVYwwIT6D-jUGXViQkwICQkx0f4Clk8633rO-gpVgiVQAk8LWAnbfUxAghzROoMyIwqiBIMBdETgFApJSEEcYCYJ4OzO-ubLk1cfr943xLeXxrMv-StwhmxNkiSKd8vlNE1LoW07hlUyQr_sjQLTCcafEeQSQb4jyGI-2QpQkTvLxxSksZ0dQDMAhxACigYlzeXcll_1NFdJBoI5aflAaJlBSqrnaC6baG7L0_Cq28oUUlarU1msLFqqQTQzJdHUlqM5ADQzDUj9PWIgVK6_ga9lWjoQ2u5AGHhf87dkdp5M8JsJZ05m_cqv2eHMH0ZhnJwW3uQP60ToNoei01EFfOCyrhdg42goHmViTTJQUpsuaDrSiYNYbfPGHIuq9a44IElZSlpHRz0mVXuSPqaVTE77vm4e18eNiO3NzERXycjsuKZtMpYrqtzUttrjflDrs3N0UWmgaVusy9Wu74mEjqITz8d1ZsZJUtTgjuUDs88y-6jepuI-nMYeQxyLkcKiOxWhzx3UmirhdHncaxBGV-dNRbFsKuTZdlhNDZjZ8DiLWShjZKLQknY0z9p-A9SVoLOQx2qmcXIvVaeZ3ZMXcM5HI67RodEdHTYzjwQ1_ABvsJ8KxWuZfhhcFDbCyAocczuahbbjWd8KD-PEiiZWkDpeHAYvvDAww0AfLW70Xy4hP5burRY3Cw9y27knd0Fhd3V1fTN3Q3-WkHfL1y0xzBahP_rAnt_fL278_Z27WC4fjg1P163uqOZ0Nc4dE_tJJYisiOdHlBXZoEscliW2o_GHzef0LnZSRE6KxYvi7T1h2KqoHZVtCWxbwIfgZ7HweiV3vvafOv8B0&mkt=en-GB&hosted=0&device_platform=Windows+10	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2freprocess%3fctx%3drQIIAYWSO2_TUABG46RNH0MpCAESUlUkBoTk5NrXj7oICT8Sp4kT14mT1BFSFL8SO341durGAzNjJ4ayMVYwwIT6D-jUGXViQkwICQkx0f4Clk8633rO-gpVgiVQAk8LWAnbfUxAghzROoMyIwqiBIMBdETgFApJSEEcYCYJ4OzO-ubLk1cfr943xLeXxrMv-StwhmxNkiSKd8vlNE1LoW07hlUyQr_sjQLTCcafEeQSQb4jyGl-2QpQkTvLxxSksZ0dQDMAhxACigYlzeXcll_1NFdJBoI5aflAaJlBSqrnaC6baG7L0_Cq28oUUlarU1msLFqqQTQzJdHUlqM5ADQzDUj9PWIgVK6_ga9lWjoQ2u5AGHhf87dkdp5M8JsJZ05m_cqv2eHMH0ZhnJwW3uQP60ToNoei01EFfOCyrhdg42goHmViTTJQUpsuaDrSiYNYbfPGHIuq9a44IElZSlpHRz0mVXuSPqaVTE77vm4e18eNiO3NzERXycjsuKZtMpYrqtzUttrjflDrs3N0UWmgaVusy9Wu74mEjqITz8d1ZsZJUtTgjuUDs88y-6jepuI-nMYeQxyLkcKiOxWhzx3UmirhdHncaxBGV-dNRbFsKuTZdlhNDZjZ8DiLWShjZKLQknY0z9p-A9SVoLOQx2qmcXIvVaeZ3ZMXcM5HI67RodEdHTYzjwQ1_ABvsJ8KxWuZfhhcFDbCyAocczuahbbjWd8KD-PEiiZWkDpeHAYvvDAww0AfLW70Xy4hP5burRY3Cw9y27knd0Fhd3V1fTN3Q3-WkHfL1y0xzBahP_rAnt_fL278_Z27WC4fjg1P163uqOZ0Nc4dE_tJJYisiOdHlBXZoEscliW2o_GHzef0LnZSRE6KxYvi7T1h2KqoHZVtCWxbwIfgZzH_eiV3vvafOv8B0&mkt=en-GB&hosted=0&device_platform=Windows+10	false		high
http://https://account.live.com/resetpassword.aspx	false		high
http://www.leo.lopez.sakshamsevango.org.in/br/?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=	false	• Avira URL Cloud: safe	unknown
http://www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office365.com/owa/prefetch.aspx	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.101.137.82	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.180.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
43.250.140.39	australiabondcleaning.com.au	Australia		45638	SYNERGYWHOLESALE-APSYNERGYWHOLESALE PTYLTDAU	false
142.250.180.243	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.10.243.103	www.leo.lopez.sakshamsevango.org.in	India		394695	PUBLIC-DOMAIN-REGISTRYUS	false
152.199.21.175	sni1gl.wpc.alphacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.1
192.168.2.7
192.168.2.3
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433426
Start date:	11.06.2021
Start time:	19:41:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Sample URL:	http://https://list-manage.agle1.cc/click?u=www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=
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:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.win@40/218@22/13
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2freprocess%3fctx%3drQIIAYWSO2_TUABG46RNH0MpCAESUlUkBoTk5NrXj7oICT8Sp4kT14mT1BFSFL8SO341durGAzNjJ4ayMVYwwIT6D-jUGXViQkwICQkx0f4Clk8633rO-gpVgiVQAk8LWAnbfUxAghzROoMyIwqiBIMBdETgFApJSEEcYCYJ4OzO-ubLk1cfr943xLeXxrMv-StwhmxNkiSKd8vlNE1LoW07hlUyQr_sjQLTCcafEeQSQb4jyGl-2QpQkTvLxxSksZ0dQDMAhxACigYlzeXcll_1NFdJBoI5afIAaJlBSqrnaC6baG7L0_Cq28oUUlarU1msLFqqQTQzJdHUlqM5ADQzDUj9PWIgVK6_ga9lWjoQ2u5AGHhf87dkdp5M8JsJZ05m_cqv2eHMH0ZhnJwW3uQP60ToNoei01EFfOCyrhdg42goHmViTTJQUpsuaDrSiYNYbfPGHIuq9a44IElZSlpHRz0mVXuSPqaVTE77vm4e18eNiO3NzERXycjsuKZtMpYrqtzUttrjflDrs3N0UWmgaVusy9Wu74mEjqITz8d1ZsZJUtTgjuUDs88y-6jepuI-nMYeQxyLkcKiOxWhzx3UmirhdHncaxBGV-dNRbFsKuTZdlhNDZjZ8DiLWShjZKLQknY0z9p-A9SVoLOQx2qmcXIvVaeZ3ZMXcM5HI67RodEdHTYzjwQ1_ABvsJ8KxWuZfhhcFDbCyAocczuahbbjWd8KD-PEiiZWkDpeHAYvvDAww0AfLW70Xy4hP5burRY3Cw9y27knd0Fhd3V1fTN3Q3-WkHfL1y0xzBahP_rAnt_fL278_Z27WC4fjg1P163uqOZ0Nc4dE_tJJYisiOdHlBXZoEscliW2o_GHzef0LnZSRE6KxYvi7T1h2KqoHZVtCWxbwIfgZ7HweiV3vvafOv8B0&mkt=en-GB&hosted=0&device_platform=Windows+10 • Browse: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2freprocess%3fctx%3drQIIAYWSO2_TUABG46RNH0MpCAESUlUkBoTk5NrXj7oICT8Sp4kT14mT1BFSFL8SO341durGAzNjJ4ayMVYwwIT6D-jUGXViQkwICQkx0f4Clk8633rO-gpVgiVQAk8LWAnbfUxAghzROoMyIwqiBIMBdETgFApJSEEcYCYJ4OzO-ubLk1cfr943xLeXxrMv-StwhmxNkiSKd8vlNE1LoW07hlUyQr_sjQLTCcafEeQSQb4jyGl-2QpQkTvLxxSksZ0dQDMAhxACigYlzeXcll_1NFdJBoI5afIAaJlBSqrnaC6baG7L0_Cq28oUUlarU1msLFqqQTQzJdHUlqM5ADQzDUj9PWIgVK6_ga9lWjoQ2u5AGHhf87dkdp5M8JsJZ05m_cqv2eHMH0ZhnJwW3uQP60ToNoei01EFfOCyrhdg42goHmViTTJQUpsuaDrSiYNYbfPGHIuq9a44IElZSlpHRz0mVXuSPqaVTE77vm4e18eNiO3NzERXycjsuKZtMpYrqtzUttrjflDrs3N0UWmgaVusy9Wu74mEjqITz8d1ZsZJUtTgjuUDs88y-6jepuI-nMYeQxyLkcKiOxWhzx3UmirhdHncaxBGV-dNRbFsKuTZdlhNDZjZ8DiLWShjZKLQknY0z9p-A9SVoLOQx2qmcXIvVaeZ3ZMXcM5HI67RodEdHTYzjwQ1_ABvsJ8KxWuZfhhcFDbCyAocczuahbbjWd8KD-PEiiZWkDpeHAY

	vvDAww0AfLW70Xy4hP5burRY3Cw9y2 7knd0Fhd3V1fTN3Q3-WkHfL1y0xzBa hP_rAnt_fL278_Z27WC4fjg1P163uq OZ0Nc4dE_tJJYisiOdHlBXZoEscliW 2o_GHzef0LnZSRE6KxYvi7T1h2KqoH ZVtCWxbwIfgZzH_eiV3vvafOv8B0&mkt=en-GB&hosted=0& device_platform=Windows+10 • Browse: https://www.microsoft.com/en-GB/servicesagreement/ • Browse: https://privacy.microsoft.com/en-GB/privacystatement • Browse: https://account.live.com/resetpassword.aspx • Browse: https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2freprocess%3fctx%3drQIIAYWSO2_TUABG46RNH0MpCAESUlUkBoTk5NrXj7oICT8Sp4kT14mT1BFSFL8SO341durGAzNjJ4ayMVYwwIT6D-jUGXViQkwICQkx0f4Clk8633rO-gpVgiVQAk8LWAnbfUxAghzROoMyIwqiBIMBdETgFApJSEEcYCYJ4OzO-ubLk1cfr943xLeXxrMv-StwhmxNkiSKd8vlNE1LoW07hlUyQr_sjQLTCcafEeQSQb4jyGl-2QpQkTvLxxSksZ0dQDMAhxACigYlzeXcll_1NFdJBol5aflAaJlBSqrnaC6baG7L0_Cq28oUUlarU1msLFqqQTQzJdHUlqM5ADQzDUj9PWlgVK6_ga9lWjoQ2u5AGHhf87dkdp5M8JsJZ05m_cqv2eHMH0ZhnJwW3uQP60ToNoei01EFfOCyrhdg42goHmViTTJQUpsuaDrSiYNYbfPGHluq9a44IElZSlpHRz0mVXuSPqaVTE77vm4e18eNiO3NzERXycjsuKZtMpYrqtzUttrjflDrs3N0UWmgaVusy9Wu74mEjqITz8d1ZsZJUtTgjuUDs88y-6jepuI-nMYeQxyLkcKiOxWhzx3UmirhdHncaxBGV-dNRbFsKuTZdlhNDZjZ8DiLWShjZKLQknY0z9p-A9SVoLOQx2qmcXIvVaeZ3ZMXcM5HI67RodEdHTYzjwQ1_ABvsJ8KxWuZfhhcFDbCyAocczuahbbjWd8KD-PEiiZWkDpeHAYvvDAww0AfLW70Xy4hP5burRY3Cw9y27knd0Fhd3V1fTN3Q3-WkHfL1y0xzBahP_rAnt_fL278_Z27WC4fjg1P163uqOZ0Nc4dE_tJJYisiOdHlBXZoEscliW2o_GHzef0LnZSRE6KxYvi7T1h2KqoHZVtCWxbwIfgZ7HweiV3vvafOv8B0&mkt=en-GB&hosted=0& device_platform=Windows+10 • Browse: '') • Browse: '') • Browse: '''' • Browse: true • Browse: ''''
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:42:10	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,....,qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j.._iK..||[.w.M.!<- .}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vI..x.R4...L.....%g...<..}'{....E8Sl...E".h...*.....ItVs.K..... .3.9.l..`D..e.i`....y....,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.126375064919111
Encrypted:	false
SSDEEP:	6:kKS0e8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:D8kPlE99SNxAhUe3OMx
MD5:	39BB82822AC1CAEA0B9414184EF94D08
SHA1:	31BFD923392407A8C3658B5C135C081C8A8A24DA
SHA-256:	E15AD74E0DA09AB67BE2D384CB21F967A581E68FE130014190C3BF4A97552A27
SHA-512:	4DF4492A0F81D21E30D55BECA12A4F75C9565A95E05985403C360FAB98BBC4A5650FE69F79A8480CE34B80828A16CBCA347088758F8EEBBBC8858EDB81FDBB86
Malicious:	false
Reputation:	low
Preview:	p..... .....6..^..(..... .....L.....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.0.e.6.c.f.e.3.4.c.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0501df76-b361-4a0d-a5f7-973b0bfe6765.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):	164056
Entropy (8bit):	6.050065772290559
Encrypted:	false
SSDEEP:	3072:4OXhf7ayQUqFqrrcIPMq+/1B85lFcbXafIB0u1GOJmA3iuRl:RRjasqFEg31m9aqfIlUOoSiuRl
MD5:	7788E4B09E1CA44AA0DF89603180C299
SHA1:	3B2F193B01EBC732D316558FAB6E8CAC5E338469

C:\Users\user\AppData\Local\Google\Chrome\User Data\0501df76-b361-4a0d-a5f7-973b0bfe6765.tmp	
SHA-256:	608C404548B94CA744EFBA3D88219E3C39CB98D7F9A1C5FCE1897EAA331D9E63
SHA-512:	EC2D6C22A5699534E7721179A6A9A0D977AD7DCC2E26F91B8766C814D6C6AAF2B82FB4E001A6CCCD579ADB6F2E6CE384537ACD7EBCED11FDC78EFB2C9217428
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623433327846222e+12,"network":1.623433329e+12,"ticks":310252858.0,"uncertainty":4689003.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922716010248"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\11a4e9ec-dcb9-4579-a2d6-3da61fb7a126.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):	172530
Entropy (8bit):	6.079898867325685
Encrypted:	false
SSDEEP:	3072:HwR0Xhf7ayQUqFqrrcIPMq+/1B85lFcbXafIB0u1GOJmA3iuRl:QWRjasqFEg31m9aqfIlUOoSiuRl
MD5:	586AD44D46130A407BA0F6B7FA8A18E4
SHA1:	4EDDB1BECB124DC6EE5A83B4D36B694EE04F22D5
SHA-256:	9FC4FEFD47D8E5EBA564E79F222B2F664C5B64DFC57FC0BC7D10A3E62E744CAD
SHA-512:	6383B4E3CD87FCF6BC4A4E4F8404C866B8530867FB095CE51D8E12D22CE35E93D205D99D0788E12BF9D46B0E1B980404C79A8507410D1E7526E61BF064BA90C
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623433327846222e+12,"network":1.623433329e+12,"ticks":310252858.0,"uncertainty":4689003.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\2e9496c3-9951-4076-909b-efa9dc9a6ba4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7503448996727493
Encrypted:	false
SSDEEP:	384:VHHAoCVrSBeIVtP0LNIrBvEg37l6THOHGvyr9iEixr2q+drZEm9xrxy4w07OqeYw:5qOJ5miInkeXuwaYvHy0KmIwtG
MD5:	10FA75F01AF5D1B72A5670A5975711EF
SHA1:	C358F4838770FA4C1F5228D9BEF57F4AA6D903C4
SHA-256:	F43437E087D0CA1CDD03500FE8F7BC95B38ED083A4CF693F5A1963A9DF5F3F6E
SHA-512:	61F982986406731554067ABDF210188626C476B548A1BE8395EB0A918D190876875FAF6C886EE04BC417A57E08BBC179429979BD75478C238357545F4D435B2F
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....<8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\522efdb9-21b2-421e-a05e-721589dbb363.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):	172530
Entropy (8bit):	6.079901440693811
Encrypted:	false
SSDEEP:	3072:H/RwXhf7ayQUqFqrrcIPMq+/1B85lFcbXafIB0u1GOJmA3iuRl:fiRjasqFEg31m9aqfIlUOoSiuRl
MD5:	DBC3AFCE0D7B2EC0FF58E706AAE21C10
SHA1:	C75F49348D38137459C4466CE26BACB232E6E40D
SHA-256:	2DEFC46D08DC3ABA09238FF1FE2775D98409E4A4796634CD37BEE80103F12F37

C:\Users\user\AppData\Local\Google\Chrome\User Data\522efdb9-21b2-421e-a05e-721589dbb363.tmp	
SHA-512:	8E9922557B4733FDF6A1D3C43663659028F603D09FC08369F5C746BCBF2DDA252819DB65785436FF26B39B0998209288458B354D4692033A20C3F685F81FA593
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623433327846222e+12,"network":1.623433329e+12,"ticks":310252858.0,"uncertainty":4689003.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\6615a104-cf27-467b-a198-95c501166212.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):	172530
Entropy (8bit):	6.079898048512382
Encrypted:	false
SSDEEP:	3072:HoRUXhf7ayQUqFqrrcIPMq+/1B85lFcbXafIB0u1GOJmA3iuRl:IuRjasqFEg31m9aqfIlUOoSiuRl
MD5:	E1B6FE029CFF86FB15A7A46519B2558C
SHA1:	05730E47EA61563E7ACE038ACC75B1412D9C605E
SHA-256:	7E4CFF2E31D50B05DF6C240D1E453A9C28FE0E64F7464AA03A02965BD7BA9177
SHA-512:	21A6F7B4C258347357167B9D1573666BF934163211DDAF7F596140ED751BF11E30FFAB2EFCB0F68AD8D0219570EA38F2477A8A453FC4F31E1CDF00D00C4C2268
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623433327846222e+12,"network":1.623433329e+12,"ticks":310252858.0,"uncertainty":4689003.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\67735183-2479-4dba-bd01-82d1b41d0e3c.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):	164056
Entropy (8bit):	6.050065772290559
Encrypted:	false
SSDEEP:	3072:4OXhf7ayQUqFqrrcIPMq+/1B85lFcbXafIB0u1GOJmA3iuRl:RRjasqFEg31m9aqfIlUOoSiuRl
MD5:	7788E4B09E1CA44AA0DF89603180C299
SHA1:	3B2F193B01EBC732D316558FAB6E8CAC5E338469
SHA-256:	608C404548B94CA744EFBA3D88219E3C39CB98D7F9A1C5FCE1897EAA331D9E63
SHA-512:	EC2D6C22A5699534E7721179A6A9A0D977AD7DCC2E26F91B8766C814D6C6AAF2B82FB4E001A6CCCD579ADB6F2E6CE384537ACD7EBCED11FDC78EFB2C9217428
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623433327846222e+12,"network":1.623433329e+12,"ticks":310252858.0,"uncertainty":4689003.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922716010248"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2dda344b-3aae-4748-a746-802fe5bbc0b1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\39045de3-6310-467a-a3b4-436f6cd96dbd.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):	22602
Entropy (8bit):	5.536200349177714
Encrypted:	false
SSDEEP:	384:/xUt+Ll5RXp51kXqKf/pUZNCgVLH2HfDUrUzHGEnZ1D6dtHG4LO7:ZLljp51kXqKf/pUZNCgVLH2HforUTGEh
MD5:	E7A55FC6EA72DA74BCB4FCBFCC9E0D8F
SHA1:	F719A20F2C3904C3E6CA6DDB0A32CAA4A0F05AB6
SHA-256:	8C55CE15A235EC3C551F10704C27C1FDD26581972065C5455A5ABA0E3E57FCE0
SHA-512:	30ED060ABA23603AC3E9E945CB7BDD4AE44647EC84A611AEFD6938892F32926A5320CC842D6053100E26C3F617ECE07928C996A852D0D5079AD1C199F4AA581
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13267906922714667","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\3c7c14e5-c815-4e98-955d-484ff39c9d95.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):	5.17285090331134
Encrypted:	false
SSDEEP:	96:nFL/I2RHGpNxyuoLIVA5k0JCRRWL8ZkxS1VbOTlVuHn:nFLg2RHGRyI+h4RYwkAt
MD5:	43D4D905313CDA8023B73590B3E78582
SHA1:	E1F16AA97339F29C663E53A5FD98C3DBA792A38E
SHA-256:	61FF9BE3AAC5869CFFFD72B3793402EB73B712A3800BC5FD401D62CB0677913D
SHA-512:	F4E4326F9EFF2E7B1B7B0677E540C24CED441280FE214690C8D0C3C4BCAFFAE96CF28188279D9612E2385F9D2829DB61AB23DF5966BDA2745D8BEE5AA1330C2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3c7c14e5-c815-4e98-955d-484ff39c9d95.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267906923044276","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\49194089-12e9-4067-9855-1e5bf754d56c.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):	3473
Entropy (8bit):	4.884897250513757
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhd:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSa
MD5:	A1CDBC88F8B4CC8D10212775766B42CF
SHA1:	895505AE442DC20942D1D7A5094B01E3DCE208F4
SHA-256:	AFB41143BF853D6784565FA685200B22EC79DFE2A846E8C774C1D4CBD5A9C82D
SHA-512:	E12E2260702115347A053A6A323732901D440C5D391041AFD7920FCEF6AC53BF2C6376E0651F4A6BBB2A6F8DFED7C56BAD8EA7131C85A8B5B676C9CAA71F1D2F
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\49b072ba-d04a-4ff5-8eb9-7df303b61fc6.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):	2545
Entropy (8bit):	5.590191252861741
Encrypted:	false
SSDEEP:	48:YEUI9U5UT6UUhDVpU8eUyLEUVKUeiYqPeUeZUhQ7331U+aJvUCUeUNU4wUPPUeP:VUI9U5UGUUZVpU8eUyLEUVKUzHPeUQUS
MD5:	18393BEAC18DFCE9530BEE3DE057C7EC
SHA1:	C029EAD28B563D0BC554E1270C405E32D7297AD6
SHA-256:	E878F4866A01F718D3FC399818070D6EC592266B36818CD1B8A68F6681A200BF
SHA-512:	64BB79B3E81E8D8E3541EF4C3196FBA6C9CB6B9E6049D45C483FF0E7DD500CA9DE2E27000AD6696DBBEB1CBE7F562CB195696BCD918E9F4ACBE0780B1DEA14E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1654969395.697941,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kI4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623433395.697945},{"expiry":1654969406.196132,"host":"D0BW2hoy2RRjWWDvPgW7xCDsfip0ZHUjP5Pz8YbCyJg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623433406.196138},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1654969373.220797,"host":"eshUG3qy9xs3GygYkqMTybnfpxfRIn+TJp3UE+dpV6w=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623433373.220805},{"expiry":1654969395.146391,"host":"e0dnev3n5m4rUz3lgUGIx3llwf0kSf/EB+PPIf8u0SI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623433395.146397},{"expiry":1654969410.459058,"host":"flbM1ImPb6P+tqzfGDG2zPDDlHlQfdsBBmXQWf4jgo4=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c8ab708-f920-488c-984c-281359aa4590.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):	5.589986448548673
Encrypted:	false
SSDEEP:	48:YEUI9e5Umom6UUhDVpU8eUHUUKUeiYqPeUeZUTJh331U6DJvUCUeIUywUPPUeP:VUI9e5UH7UUZVpU8eUHUUKUzHPeUQU94
MD5:	0C108BCCCBA2CCC6D4E125A32692AB3C
SHA1:	98CBCAA91EF8489EC3547E8B43A16A844DCCC5EB
SHA-256:	1256E3B38C3B3B24E7A145A65A026066691432740E408739D220E5F224D77549
SHA-512:	CAF2B93FC5498D7CEC10865C239AB037055F04DAB8FF65CDEBE619780F3171BC0E4F855436185244826BFF3762A2225D99A8D16EEA16F91313390527E0AFA23E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6c8ab708-f920-488c-984c-281359aa4590.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1654969395.697941,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kl4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623433395.697945},{"expiry":1654969405.02102,"host":"D0BW2hoy2RRjWWDvPgW7xCDsfip0ZHUjP5Pz8YbCyJg=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623433405.021025},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1654969373.220797,"host":"eshUG3qy9xs3GygYkqMTybnfpxfRIn+TJp3UE+dpV6w=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623433373.220805},{"expiry":1654969395.146391,"host":"e0dnev3n5m4rUz3lgUGIx3llwf0kSf/EB+PPIf8u0SI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623433395.146397},{"expiry":1654969380.237322,"host":"flbM1ImPb6P+tqzfGDG2zPDDlHlQfdsBBmXQWf4jgo4=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6d7cc2ea-94ba-4460-8232-bace5164261c.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):	2380
Entropy (8bit):	5.5887343016233375
Encrypted:	false
SSDEEP:	48:YfUf6UUhDVpU8wUJUUKUeiYqPeUeZUTJh331U6DJvUCUeIUywUPPUeP:SUiUUZVpU8wUJUUKUzHPeUQU9h3lU6D6
MD5:	7567485B2AD73B4AE9C6EEB24425DADA
SHA1:	EFB5687E27F65158D8720AE2EDC1AB43434604D7
SHA-256:	7017064CDFBC235518FAD2E1C1A51D58221FBE55AC3ED55E339E532569488567
SHA-512:	605D31EF292DD592BEBA9690FA82C66AE68E3F3BB756EBCE5FB143C2CF78BF80A6FA0B6257BC926EBBD97C4A5AEA11223AC20908D46317A6A169201306655EB7
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1654969387.919074,"host":"AVsuOZgBg0wdpKMoxm8zihjqET8kl4Xl8bCSMk28RsE=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623433387.919079},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1654969373.220797,"host":"eshUG3qy9xs3GygYkqMTybnfpxfRIn+TJp3UE+dpV6w=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623433373.220805},{"expiry":1654969390.750038,"host":"e0dnev3n5m4rUz3lgUGIx3llwf0kSf/EB+PPIf8u0SI=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623433390.750043},{"expiry":1654969380.237322,"host":"flbM1ImPb6P+tqzfGDG2zPDDlHlQfdsBBmXQWf4jgo4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623433380.237327},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\72fad40a-67ce-4a33-93e3-6890c6366c4a.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):	1541
Entropy (8bit):	5.583588082217342
Encrypted:	false
SSDEEP:	48:Ym6UUhKVpU+KUeiYqPeUeZUdJvUCUeswUPPUeP:8UUMVpU+KUzHPeUQUdhUCUgUPPUg
MD5:	A09E6BF2ECD658553C9CCE8039E95829
SHA1:	AE0FF383565072B52B8336804418FF0E206ACD25
SHA-256:	FB145D65A1A0BE28BE840AE73B661E995F2F252B5A0E3516E50FA633C68744F8
SHA-512:	4DB087B697CB9D288BB73BB1737514DC39F813A12BB323E4F8C5F6D2537BF99ACF8BB838134A5B5E91F92775177EA4A6518DB5D6B37763B23C66D834232B91D4
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1654969335.16054,"host":"eshUG3qy9xs3GygYkqMTybnfpxfRIn+TJp3UE+dpV6w=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623433335.160547},{"expiry":1632986994.959502,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601450994.959505},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1654969334.100896,"host":"0+NBY3xIXoqmO/VaXHW6Xq8xE/jWdwRwHTX7xDnLLLY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623433334.100901},{"expiry":1654969333.678822,"host":"3uaBa4ZmCZBHnd7Qc9BElmlgTLbJ3iAXtNx2AUtm46w=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\84277d50-d269-4904-8d24-25a123a949d7.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):	16745
Entropy (8bit):	5.577452468221688
Encrypted:	false
SSDEEP:	384:/xUtXLl5RXp51kXqKf/pUZNCgVLH2HfDUrU9G6dtG4t:SLljp51kXqKf/pUZNCgVLH2HforU9//T
MD5:	E1FB2A27FD474E98AFF0859AF599B61C
SHA1:	5C0169089D0BEEB0D58AB029E6440F5366BA15BA
SHA-256:	5F370039F8DDAF7F1B53342DFE3F4FDCC0A2D4EE0DEB0EC6F512674C0CCDFD03
SHA-512:	1362FDA0794699BE2965E1ABCB6796B84F9639570CA0091ADA53B8D7DAB2EAF08939C73A2D98A59286A63917AEE467543D1B8923A7F1576D0BF9768E5B3500BE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\84277d50-d269-4904-8d24-25a123a949d7.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":"13267906922714667","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):	5.234556184130455
Encrypted:	false
SSDEEP:	6:mwpKcBE9+q2Pwkn23iKKdK9RXXTZIFUtpDp8cBEJZmwPDprZ9VkwOwkn23iKKdKT:4cC9+vYf5Kk7XT2FUtp+ZJ/Pv9V5Jf51
MD5:	1EF2965964F0FCA841B33B6CCF55D975
SHA1:	058C8E37EA226BA40491E4C3D50030A008061A5D
SHA-256:	3C9C213133F2745500F3CB5BBFD08F5A6B05CA1A9B9C29535F8C773A88D8C941
SHA-512:	C2349F9C2A8C54A0453BB03F52414473D10EF5F8032EE3EC2549C52D91099A230C610714F173A8A4FA2377975CE2483AC18CA300B22F96FCC34C7CC214797B28
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:23.601 19dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/06/11-19:42:23.607 19dc Recovering log #3.2021/06/11-19:42:23.608 19dc 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):	5.244313366650332
Encrypted:	false
SSDEEP:	6:mwpRfwGN9+q2Pwkn23iKKdKyDZIFUtpDpRcQgJZmwPDpRcS9VkwOwkn23iKKdKyX:LwE9+vYf5Kk02FUtpfgJ/P59V5Jf5Kky
MD5:	26420D9874D88C8CD35BEB386004A298
SHA1:	86E2BAC714310032BD1E7BDA143747385B26C951
SHA-256:	5DDE84A58735BD097152F58E80A330947D152D07091DF076851E7B9B2CE01450
SHA-512:	131645DE0BAB9102708EF3A90ED9B9397D2E4A2570ED9BC01D3265FFB5088D2A4574DB5EC04C0F9189E9B93FA024C94DB9EDC0A9B46BD8C15A2264546D0516A
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:23.589 19dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/11-19:42:23.595 19dc Recovering log #3.2021/06/11-19:42:23.596 19dc 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\00e9eabc0bc6d2eb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1140
Entropy (8bit):	4.981520491616877
Encrypted:	false
SSDEEP:	24:5/cjlJaGN4zXk16FHPtJ8dw1wUUuzi19EJkuLUkI5E/9RLFePpeIa8:5UwaGQXi6Odw1NzLJk+UkeE1nePpna8
MD5:	876CE05E21CF2D3FA1A6F12FA4F9FE4A
SHA1:	48B1141C4F764B3AA4A3958745C133D31C8141C6
SHA-256:	0E3D0B36DA4DD905E26C7E1E90468C7E42ECFBB0D13DD4F34D47ADA88BDB8B02
SHA-512:	FA0E88B1DB6329FADA21916EB745D5403BFBA1F7507F721DE71E9F921152DC71C6540A34283982BDF30CC4F0050714433499BE33B1CEC4626E247B3E75926496
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://c.s-microsoft.com/en-gb/CMSScripts/script.jsx?k=0502864a-b6ef-2f14-9f8e-267004d3a4e0_c5ea3348-55af-729a-2641-14f0312bacf3_742bd11f-3d7c-9955-3df5-f02b66689699_cb9d43d2-fbae-5b5c-827f-72166d6b87fc_49488e0d-6ae2-5101-c995-f4d56443b1d8_7dea7b90-4334-c043-b252-9f132d19ee19_38aa9ffb-ddb5-75be-6536-a58628f435f5_e3e65a0a-c133-43e7-571d-2293e03f85e6_c7a4393f-7c9b-39d3-762d-af461a6d6564_4ca0e9dc-a4de-17ba-f0de-d1d346cb99e2_06310cd8-41c6-3b11-4645-b4884789ed70_5c27e8aa-9347-969e-39ac-37a4de428a8d_d6872b5a-5310-a73c-7cb3-227a3213a1c5_be92d794-4118-193f-9871-58b72092a5ac_64c742e2-b29c-b6c1-fdd9-accf33ec40bd_cf2ceca9-3467-a5b3-d095-68958eee6d4c_cec39dd8-f1d3-56f1-abfc-a7db34ff7b46_ec5fa2c9-3950-ff57-a5c3-1fa77e0db190_d19f9592-65df-bcc9-e30e-439b875c3381_76a3d06f-f11f-77ef-9bfd-6227ba750200_5e1caa45-461c-3b04-f88b-8cd50af16db5_c2dceda8-20b4-7d3f-13b6-9cac67d7df17_914fa41b-cc86-d3b0-4e15-2fdfa357bcc7_40c6c884-da6e-7c2c-081f-4a7dfe7c7245_ae79ba96-1a9d-debd-a5b1-f306

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\05711a550dadec40_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2934
Entropy (8bit):	5.504708735853742
Encrypted:	false
SSDEEP:	48:tgsKns6ZGoFhhgsKIeuTTyTi7b3HDv8IKtGPb4dXCJEK0jZX6ZPyQCMcjJ7riept:tgs+sC7gsbeu2i7bz8M4dSJXgX69uZ7
MD5:	ED43EDBFC6FA91CE971E760F1BCD2BC4
SHA1:	A9471B8D99C03B9B0E186AC7C075ADEABCDB4182
SHA-256:	135A01993A54C54281D5AAEF95DC0812F01BF1F1FAD810E948B8B28AAB631C24
SHA-512:	3AD4C78C209F40ED634118543ACFFEBF19E5977FD19DF2D8EA4813D4BF6135CFE3410A8CBD0BC717A3FDF8FD0744B89A5A7546D4349B3A84F9796E648A743A32
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...`6....._keyhttps://passwordreset.microsoftonline.com/js/Captcha.js?v=1342177280 .https://microsoftonline.com/..)P.#/.....z8A..2.....$.0\....G...A..Eo.....A..Eo.....)P.#/.H.....'.....O.....<.....(S...`.....lL`2....(L`.....(S.....Ia..... ..f.....Qc&. .....DoLoad..E.@.-....PP.1.....D...https://passwordreset.microsoftonline.com/js/Captcha.js?v=1342177280a.....D`....D`....D`.....T...`&...&...&..A..D&.(S.....Ia..... Qf.X5.....checkIfCaptchaLoadedE....d.....&.(S...Ia..... .f..... Qf.....refreshOutsideMenu..E.d.....D&.(S.....5.a.....Qc.x....WLSPHlP0...a..... Qf.....menuOutsideCallback.ai.....E.d.....&.(S.....a.....Pd.....getError...a.....Qc.[.....getErrorE.d.....&.(S.....a.....Pd.....getSolutionaz.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\094e2d6bf2abec98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.562024676190314
Encrypted:	false
SSDEEP:	3:m+lP9Ola8RzYJb9yKlf8QPKxWStHWFvDFYtRNSsKlvXlHCNg/bl58tyGdDmp/5lH:m3VYyK08fNH1D820yL6p/5llZK6t
MD5:	009DABA4CD1D45DB8A3CB377ABD27513
SHA1:	8504EB72D055936EA0A5DFB7F38A1E55FA2BF04E
SHA-256:	AEFE25E337D8A5273A7860288242B5A4FCB3CDE4578E39067A3147D64F04F67D
SHA-512:	32EB8C335E965FE498A5F08F63E357A14B7DBC6BD22EB6E3EB32F1BBF9C628AEE70B9FD04683635CF2C403C6AEF6357A5EE66C696FD63112DA5AA071C694D2D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js .https://microsoft.com/..S.#/....._C.....=.z-.7.K]..~..=..9.....8...A..Eo.....}x.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0decd6ee54701714_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.661851306172752
Encrypted:	false
SSDEEP:	6:mJEYcRTXhr7fFNdp7+AMLXBrKapzH4AK6t:tHFNdp7aLXRpj9
MD5:	7515E08D4C07DD749504921CF4A153C0
SHA1:	FAEC6AB79A7DBF5FB8CA4185EC8C3B085566BB29
SHA-256:	01180902DAD34C4690B4B634B7BD8B99B4A5CD29D4A855535D515383DB0DE5ED
SHA-512:	6C154B65E4FFAB856755CDA302EA0C3722551702314A9730D0125EB0D081D8D6D48B5D19EDE7E14B5FA8448F6E4A3D3A6977082C5F269B8A53A16C241BBE597
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a....._keyhttps://acctcdn.msauth.net/wlivepackagefull_2169QIWB52Tqqm3jo5_AUA2.js?v=1 .https://live.com/...S.#/.....Zv.....l...R.U.vh:e.M..a..h..-'....A..Eo....._.,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\13216249a71837e7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.4980678075544285
Encrypted:	false
SSDEEP:	3:m+lScb/yOA8RzYP2FycyG8ZFvDqMu6CKNrgflHCuhl/lDPRJ7Qcpzu4VhMmheAtP:mgOEYeMWcgAux1mcplVhhvbK6t
MD5:	A067C16C98B73D1E5F3D5B02603C0559

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\13216249a71837e7_0	
SHA1:	576600C1C323903400E59E7A0BF5DCED78F90713
SHA-256:	70BBB91C55D8DE0825327C9B1045F681CE1B8A58083946D016A08A640DAA94A4
SHA-512:	4B23818709A0D29E589BB7C6398AC353E3FB94E21D50B57FCDB627C34B303A729BD73359FB896A00345944469A459619F9A4ABB6771818F03702D6CF62983D0E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....A.Z...._keyhttps://code.jquery.com/jquery-3.1.1.min.js .https://australiabondcleaning.com.au/..O.#/.....|...G..J[.e.OZm.....i=...\&.A..Eo.....[{..... A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\263002cf0fbb71e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.625141630630371
Encrypted:	false
SSDEEP:	3:m+l7YllLA8RzYcRKIQ7Qd2FWLjrUZyh/NTJ39XlHC9E3bi6VrpKTdHaTUmIt/pK+:m3/VYcRT0uLjiyxNd3y9EW4rpH7SK6t
MD5:	C90EAEA67C8E4DAA0978006EBE3B2B7D
SHA1:	99A50FE6116657CB873F0BA81FE1CB6C67662165
SHA-256:	79C6369493F8019A13270FB3DE3AA255F17A8D00F27ED1B01CA7E2B71BAC1A6D
SHA-512:	C84FDA016DE41A423C97DD7C0A8F554E7ED40226ACA23BB7B1CC72FB64AF35C5F5F22CEEF355870B1CFD314CB27DC11BCDEA0F733564461DAAD33D92B731(9F4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...fj@...._keyhttps://acctcdn.msauth.net/accountcorepackage_YD-Y5A3nlj0ms1Ks9fXU6A2.js?v=1 .https://live.com/A..S.#/.....v.....|@._i.:...X,.mj..`. .N....p?.E.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\280762aeaed2bc04_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	327
Entropy (8bit):	5.916269760853667
Encrypted:	false
SSDEEP:	6:mQYMjdSEQMeYeoBHcsNXYzbJpQF9VYmQsEbyspY8r4RDK6t:hjdHQM7Hcs6JpQ56sa3Q
MD5:	5A20D7F1719F730D4BD7BDE8D49E5D3C
SHA1:	86EDC031B036BCEEC703C2C4BB3343F258DB52AF
SHA-256:	AEF12A8D6BDEB77D3062D553FDB46649661C77C68198DA53A216259C8DD6ED99
SHA-512:	697BECC4FAF5CE2F21E3C7499E337BCC29D74CF9228FAA5C3791557B5A5338F867A55EB78285F02562F2F1112E4861E4287873E80E634F7E9498F3BD1FDA4513
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\C.W...._keyhttps://client.hip.live.com/GetHIP/GetWLSPHIP0/WLSPHIP0?fid=8a89a375569c494ab67c45a2dc38fc59&id=282555&type=visual&mkt=en-GB&bla=a4b57412d82541939ad10615e29f8141 .https://microsoftonline.com/t4.R.#/.....z...N'f..zu...`....r....A..Eo.....f.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\308e7fc8113abdbe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4309
Entropy (8bit):	5.436049767556891
Encrypted:	false
SSDEEP:	96:SgsisnsfpOgsbP6tZfRLt7NppbBcUaf+24:jpBB2+24
MD5:	A1DDD1CF4CA69A006FC9907B78F1C79C
SHA1:	3C8CC523EEEF70DE155786BA79D540BF8F8DF994
SHA-256:	327233DFF2378E9F6B318DCAB4D4660626FE0B2C9060A6006E12BAE74EF212F0
SHA-512:	FBA7D4AC488D0975764A9F42B1E6008BB675CD00AAC5D6C8822414B0618BB2C567B4A5DC78BD4163D50B02C5E0EBAB32D24F3D220111C65E41B95686F4EFD8 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...p].U...._keyhttps://passwordreset.microsoftonline.com/js/Button.js?v=1342177280 .https://microsoftonline.com/..)P.#/.....5.....CG.'..}k\.`y..w0 ..D.A..Eo.....N".]....A..Eo.....)P.#/.....'..2....O....`...U.MR.....$.....(S.....`.....L`.....L`.....Qc...I....Button.....Qd.....ActiveButton..Qd. +.K....FocusButton...Qe.....DefaultButton.....QdRPl.....CancelButton. Qf~.....ActivatedButtonID.....Qc.1.....Groups...(S.....5.a.....Pc.....SetTexta.....IE.@.- ....PP.1.....C...https://passwordreset.microsoftonline.com/js/Button.js?v=1342177280.a.....D`....D`....D`.....`<...&...&....&.(S.....Pd.....Button.Clicka....r...IE..1.d..... .....&.(S.....a.....Pc.....Enable.a.....IE.d.....&.(S.....a.....Pc.....Disablea.....IE.d.....&.(S.....Pd.....Button.Show.a....Z...IE.d.....&. (S....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\397eaf5d020aa337_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97840
Entropy (8bit):	5.831683250419546
Encrypted:	false
SSDEEP:	1536:8h/TtYGyN/9swTJBtAm2vxPoytoae9NaebqK3TgCPNa1wpRVamr:2riG6TJaelK6r
MD5:	938EA3E30CBF141004740B050953CFAA
SHA1:	8997809E2353C0B001BAEA7F7CD3FA83B60517A3
SHA-256:	7BDA35B3D889F1C1E6D98E337903EC5B0F471EBEE2C7652A8A994EEC4526167F
SHA-512:	F13648E8FD082F0CAE9623192400194062CAA36EA3177F37C7E70CDC0AB786E14B2348B5D9EB21D6BDB0C02ABC33282EA15E8E46F20549C27CAD5BA7BFAD82A4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....93AD318221ADFACBC823CD345A984C5331DB343CE2E728D881C62B60C3CC8EF2.....'..]....O!....|....Q{.....`&.....`.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....Qb.....t...`....l`....Da....j.....Q.@".4,....module....Qc.=l.....exports...Qc..\P....document.(S.....5.a.....a.....a.....a.....A....a.....a.....Pc.....exportsa..../...I.....@.-....HP.....:...https://ajax.aspnetcdn.com/ajax/jQuery/jquery-3.5.0.min.js..a.....D`....D`....D`.....`....&...&..!.&....&.(S...a&..`|L.....L`.....Rcd.....*.....QbZ.....C.....Qb..WH....r.....Qbfh.....s.....R.....S...Qb..B[....n.....Qb.....o.....Qbn.w.....v.....M...Qb.(.....l.....Qb...O....y.....Qb.....m.....Qb.....x.....Qb.C.l....E.....Qb.G.n....c.....O...Qb^"o.....w.....Qb>.7*....S.....QbZ.s;....p.....Qb.p^...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4278acc4333443e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.781838543953145
Encrypted:	false
SSDEEP:	3:m+l7vTLA8RzYcRKIQlM6lpjwIR5NTJO+s+XlHCWllZ3iKqkozK5mivttpK5kt:miJYcRTSMiqIR5Ndj2W/bwK4ivRK6t
MD5:	6BF7841AA5C75DD7EBF7438B6EE65DA9
SHA1:	5563C8EDA1ECC57D64054EA6A7A8B7037A404000
SHA-256:	F6BE0EDE5A1BE263FBA2DDD1643D58CE3AFA1C438315D6A3FA767BDFEA84DB10
SHA-512:	46B9316A50A487BB8D4C9D9F023A182B3495D8D24D3992791C92DE7DAC818A7C1AD137F54D4045FFEDC2EFA0423236D43CF204272E0429982478C7CEB1B3D15
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...-9.Y...._keyhttps://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1 .https://live.com/|..S.#/.....Lv.....(....-…5.....K.y....x.\<..A..Eo.....t.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\59f8bbf14d4853fd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.684124987813755
Encrypted:	false
SSDEEP:	6:mYoLnYcRT/REXA5Rhj5l1Z3NdPw6rykH6JRGh0K6t:FokAPhFl15NdPw1k+
MD5:	B98AF6B4ACDD69EF536A3B83CE1B3D2F
SHA1:	3AABBB302582A9E35C5A2C1EACB7F6ADBE3CC310
SHA-256:	F2BBB2B20AAD60598308769761861DFC1F18A76343D4B4913D595795B9DBCED3
SHA-512:	9A9DB21BECE60BA0D49AA56167988D5D883E95D13EA298A03D80C4E67067711D9FFAC1E78EB352A63A84CCD084A43432B9963ACB4E9A78198F0DA6D189DA63A
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....._keyhttps://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js .https://live.com/...T.#/.....x.....B..%<.....,.%..).H.8.>.Y....Y.A..Eo.....a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\64ea806cd0219a37_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.535354581614467
Encrypted:	false
SSDEEP:	6:mUsYSHT8NWQATbjALkEzkk/FKgkvP4+K6t:pqz8NWQsjYtKgkPj
MD5:	183F49F135E47A3B9C86F51D679526AA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\64ea806cd0219a37_0	
SHA1:	D7B2E19D3A60071AAE33E1D827DEFCDC9692BFA2
SHA-256:	46B1FDD540D22DA303F84B523AADE99B44E332FC554F64D6B311514E9DBD79D5
SHA-512:	F9532FF374DAE61AE30384D8DB72BEC945568B67FF55D27FD0498FDB10D0C1E6BF761A1F3834E152D1D63CAB7313DACDBCBE65EE65B8E430134879F2C9133CB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....I...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js .https://australiabondcleaning.com.au/..O.#/.....7.....I.]..sc8..P.....y.N:..{....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7cab34efca253074_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.661037337963448
Encrypted:	false
SSDEEP:	6:mmKVYcRTbVYXvCVJumSrR5Nd3mrlA9twn9YH69hdbK6t:KBEaixR5Nd3S+w99FN
MD5:	5D7EBC339107B429FDD01C2B09A68B53
SHA1:	6DE366FD2EF94D9A82D058244812B2736DB88D4C
SHA-256:	7D2F200105C0273BD01264E85E06D1F34D359E2133731CCE196ABBB56734E62D
SHA-512:	EACD307AA8F3902F8531DCFF8B95A812BC5EE87F50C10710129FF0F5114FEB293C61D691891D8147F549E9C8A998069EC403648A2511705F56F292097186A5D2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...d....._keyhttps://acctcdn.msauth.net/resetpasswordpackage_X7k_NcCIoofIIFuKCGNtCw2.js?v=1 .https://live.com/. .S.#/.....v.....l.....e.GS.;.m..5.1.^R....A..Eo.....\.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7e4cea594f77c74d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.660870391695421
Encrypted:	false
SSDEEP:	6:mOEYcRTdFAwhTT5NdJ9jbqMKL2lBy4WSl/bK6t:KFAwhTT5NdJNqtol1
MD5:	2295FE26DA0E15EBE8FB98C48A0D69E2
SHA1:	05FFCED37B0D1331C5F9E8292C9FBC984FF66398
SHA-256:	185996BC981388C9C83D39FA9B3F5101D677A78DB5DA5BF1FE103B18C9A6CA08
SHA-512:	78DCAD2EEE2C20131B71AFC264AC3002F46767E67E436E3B27800357BED4CE9BA1E6442C765A442358AFEBE91D15803B075DC91BAADEF8E09EAF5DCFCB97EF48
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...$.DV...._keyhttps://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1 .https://live.com/Ri.S.#/.....;x.....}OZ.\,...mg.:Y...b..;.p.kg+..''S.A..Eo.....X.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7f239fb82bdc9a15_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4466
Entropy (8bit):	5.710482385771977
Encrypted:	false
SSDEEP:	96:OgsAR1saIgsAR8SVoc9lVWqQe7JwTgjRJA5TWJLN+0Ysa9:TLdm6ocDVWqR1wTgjLgaJB+0YL
MD5:	12D661F2170857155B0BDA65112E5585
SHA1:	FA43FE031213B7626FE92BF99ED4FA60E3618ACF
SHA-256:	E2495BCB16558204DE7C5AC91606FF33288554B98B7366C1D0112EA8072A76B4
SHA-512:	24C3B6494EC77B815715D10914E6EC43B0522AF88A732A376606F6D43F5F1706F6472C039EC7510C5A66000CFB35A92407D507979D0DF05D95638DCAFEF70A8A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L.QM...._keyhttps://passwordreset.microsoftonline.com/WebResource.axd?d=K8SG-wKQphiVYLIldWNflHCKk9laM7b9jg1MsaXMuAxomyw71qZtQovvIEUujLpY5PYeYO7PJZL958QBRn8hMMu9YShw_wcswEwx8RhkJadOevd7dApopiRvDtu5vQXazFVxjmTLIqDYYcfR-juoDw2&t=637560635036175728 .https://microsoftonline.com/.i)P.#/.....D...g..F.7"...t7.|<K.|.?&^1.A..Eo.....A..Eo.....i)P.#/.....'..Z....O....X...j..... .....(S....`.....LL`"....%.L`.....(S.....Ia .....$Qg.?N@....WebForm_PostBackOptions.E.@.-.....P.....https://passwordreset.microsoftonline.com/WebResource.axd?d=K8SG-wKQphiVYLIldWNflHCKk9laM7b9jg1MsaXMuAxomyw71qZtQovvIEUujLpY5PYeYO7PJZL958QBRn8hMMu9YShw_wcswEwx8RhkJadOevd7dApopiRvDtu5vQXazFVxjmTLIqDYYcfR-juoDw2&t=637560635036175728a.....D`....D`....D`.....`D...&...&....&.(S...Ia....v....,Qi2.2.....WebForm_DoPostBackWithOptions...E..Q.d....&.....&.(S.....Ia....<"...$..g.....D....(.D.P...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\83b9c3db1088f864_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.704922534673388
Encrypted:	false
SSDEEP:	6:mY2nYiRDHjfRpA7eIAX3TH5R2DS1JUeJsyAvK6t:KxDHIeB3L5gDS41R
MD5:	A7B995F305993DC4B6520CB786A9BC3E
SHA1:	20E1AB8420577803E721D039DCB5F0F7C686DA12
SHA-256:	C9BD97BFF58135C2CD3AD19599AE8A14639C9B27EBA336116EEFD390EF6DDA17
SHA-512:	9AB52FA5C50ED2F49ADEA0B7EB2E84D3A21A1B133273051548C9A8B8679A27D3F74FE08B06A02463A43710DB753A164EDE9021AC5F5B4EED659FC4554AFDF37 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x....._keyhttps://c.s-microsoft.com/en-gb/CMSScripts/script.jsx?k=8c84dc53-9dee-f42a-46b1-5a93c0e43d70 .https://microsoft.com/..S.#/.....J.....1o... ...h.....KP..e.9.k..A..Eo.....SU.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8ba90312ac6aad2e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.501632331501648
Encrypted:	false
SSDEEP:	6:mHb/PYGL2crnUALVNM3JdlAz+AacRkzjU4LORK6t:inRLVC3ltA9mzpOr
MD5:	1FDD7DA7262829A9A9A0B42AA948AEE3
SHA1:	28686B3143EA6CC90D021FD550FFDB74B692EDF0
SHA-256:	850F7B7DDBB4C395F1928E63512F73243C31891D5EAB0C7282258DA27BBEA814
SHA-512:	C99A00DFFA618DDD86803D14D351FD8FC1970D3126015C1787D4465472BB465414DFF7C8893150EFC352D213D16CC9C53779120D83BA069B6093AF65E2743C6E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....f....._keyhttps://www.australiabondcleaning.com.au/.well-known/js/maximum.js .https://australiabondcleaning.com.au/I.O.#/.....$.d.H...4..... .e..gR?0.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f3c2e2c260a7099_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.366177240859455
Encrypted:	false
SSDEEP:	3:m+lSd7ta8RzY/VW4McTtRAJOIGQHLRSVNRFYtROM1lXlHCHlMWUBl0iPy2wd1UmB:mXYI4McTDsJegDO06i1TrlEPhK6t
MD5:	4C9C9140B9F85384B0E3ECEF6A4BDCBC
SHA1:	34AC5E977512E228D14B1F3A2C5FE545E7E856DD
SHA-256:	204C1938BD5B61AE204AF97B074900F2EF7531685D717E6C4EF821A41536FA2D
SHA-512:	7549A60154307689058E1BDC2166CEC218423A23FED83340227E264A5AB23826994C2190E9A2CA2345450593EEEBF03E85C1181068E7C990E01B149CEFA981C4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...|.L\...._keyhttps://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js .https://microsoft.com/...R.#/.....(.....<.S....l....*.W.U\..E?`..r.A..Eo.....g..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\914981e1a3a6bf84_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5451
Entropy (8bit):	5.748594871176021
Encrypted:	false
SSDEEP:	96:CgsxW7sw8ttsj6MgsxW464dx+65Pr1GJN3w9psxEh5orpbFdZAakjSa+aEvGKr2c:z8ts6Q64dxz5PZGJNA9psxEh+rpbFd6o
MD5:	FFF658856FA789B71D8D5200A4696468
SHA1:	3FF337807A86AA090F77242465B2A81A6D41EDF4
SHA-256:	6A3F829D2B9FFD4CA1F917E3D680CA400BBF6F6CD012BFE7EF3718E6597010CF
SHA-512:	9743977E435EBE923C46B95AADE0DE9035099DE362430D51CE9E8456A16474CC07B4DCD566A8C08344C72DE8952E368DE46E317BAA2853BBB947ABE644949F3 F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\914981e1a3a6bf84_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K.....T?...._keyhttps://passwordreset.microsoftonline.com/ScriptResource.axd?d=4g-KgwMm_BqPQdbE5kksnnK4aEUO_ElVq3B3iOZt602As-6zd-qGoSUfRd8O3Vfr3ztVg6Kgv6hzs6X9i6vEvG5jDjXGyu9R_kvNc7FtGlUYGpIaVHs9AMrU6lF2-qovibj4TUVrTiY3D2iuGF5igO0xtcYq6BAzsFcC3CWykwxJCmR_aR4y-50ntGBlFElN8zvLOq-tpW5Ev7-IqKmeDw2&t=ffffffff6474071 .https://microsoftonline.com/v.*P.#/.....\..d.;.UU.'k.6.I..]M...h*#w.A..Eo.....b.z.....A..Eo.....'.Gi....O.....;E.....(S.h..`.....4L`.....L`z.... Qf.....Page_ValidationVer....Qd*.....Page_IsValid..Qe.....Page_BlockSubmit.,Qi&.b....Page_InvalidControlToBeFocused....Qe.h7.....Page_TextTypes...(S.....Ia+.....$Qg&M.....ValidatorUpdateDisplay..E.@.-....9.P.....)...https://passwordreset.microsoftonline.com/ScriptResource.axd?d=4g-KgwMm_BqPQdbE5kksnnK4aEUO_ElVq3B3iOZt602As-6zd-qGoSUfRd8O3Vfr3ztVg6Kgv6hzs6X9i6vEvG5jDjXGyu9R_kvNc7FtGlUYGpIaVHs9AMrU6lF2-qovibj4TUVrTiY3D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\949d2b57c43cbcd6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.939507401107233
Encrypted:	false
SSDEEP:	6:mhnYyK08fOVdL71sXj4jmDGRPh9pr3nK6tWq0o5slWtAUdb3F6QmDGRPh9pr:eKjfOVdH1sXGmDGhPAosALF6QmDGh
MD5:	E250869EB17FFACF7933BED29793B522
SHA1:	E909F3D237FDC94447AF274FE02D91EE1611FA2A
SHA-256:	F166308DD598AB6578CD31B7E43F1BC1375DB6FBCAC89013FE00638BA581937D
SHA-512:	8E2FBB6100DB2330D521F6C13E1DC2ADD4E8A5D26A33B27211B8AC85A241180A2FA7DF29EE1E43781A357E2FB519E3C74ABA34612BA4FD3F07FCE5C19562619
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\...b....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-3.5.0.min.js .https://microsoftonline.com/L.*P.#/.....e.....+ U.uN.eD....>.....K..4.?....A..Eo.....:.....A..Eo.....L.*P.#/..}..93AD318221ADFACBC823CD345A984C5331DB343CE2E728D881C62B60C3CC8EF2..+ U.uN.eD....>.....K..4.?....A..Eo.....;.XL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\98431752fa0d1df4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24768
Entropy (8bit):	5.409748930694823
Encrypted:	false
SSDEEP:	384:XhDy1gHdHS/D0WWph3EH6BfeUx0kf4tgkfaFKYYJbB25oGuyt:JFW0Kgx4etWN2
MD5:	BEB055258ED1A2F964327A5A4248C989
SHA1:	1AE680E058DC64F079209EEF1B938F5E0DA70AE6
SHA-256:	222B7194974CA5110B35E623C254B613EF612009FD58AC745256340E43B25920
SHA-512:	E102C1F9480882530A0873FDD7FC1D452FA79DACD7BDD908175FF6E8165E7E9753FB1FC185F6ABFC068C4E485FE6BD7D6B2A36383A1247586A3420A2F9AE9F3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....t...._keyhttps://passwordreset.microsoftonline.com/ScriptResource.axd?d=lpJqtggTHYeoqLfPDGjso-Zm_BE4vd_5wolP-aHjqMozfJukJKmmbewM8aMqQIYIHpbl8ZM0pF1dQkt1MN945Scet5QTy9fSd7sq7be9t1RFkZUncHITOPbq0lM5-ILGtrcNm4b8DmbkyrlCENpMQWOVEzOzAiJWyUBIjfyEKry4iKasLhjsXIHiAnnJmX4HkvAHm_34QH8RDZFHrvB9onMiXEWGisdElqbIi8V2UZM1&t=2fe674eb .https://microsoftonline.com/Z./P.#/.....V.V.#...s&...2...5.gmGT....mK.A..Eo.....z..N.....A..Eo.....'.....O....(^..e.8.....0.....(S....`.....L`.....QbN,.....Type..Qen.F....._registerScript..$Qgv.(D....MicrosoftAjaxWebForms.js.....`.....M`..... QfR..r....MicrosoftAjaxCore.js.,Qi&.....MicrosoftAjaxSerialization.js....$Qg.....MicrosoftAjaxNetwork.js..,Qi.....MicrosoftAjaxComponentModel.js... Qf*.#L....registerNamespace.....Qd..|.....Sys.WebForms..Qb.f.....Sys...Qc..P....WebForms.(S.....5.a...".....A6...a.....a.....6...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a64bbd896a35b6e4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1112
Entropy (8bit):	5.25697758931309
Encrypted:	false
SSDEEP:	24:nWgsGsdYMk+82b7/np9EAgswb35jo+2Rrr7Je2z8YMk+A:WgsGsdYMk+82/tgswTlHWrr7JUYMk+A
MD5:	8399B307EC44C82993A61CDB91E4E43E
SHA1:	BA33D57841C8A052552CE72034070C4228B38C06
SHA-256:	360A8F86A0937A1DC957820051706E8A67F2A2C43BA431983EEBDFBD61E4563D
SHA-512:	BC8048331475CA6FB52CC0AAFCC19947B02E8C27B55FD472BF53D1D44920497836E2A382B2573BE1F4FF84084B2A6BBC3742928B59220B3DC9D3BFE11DA5984
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a64bbd896a35b6e4_0	
Preview:	0\r..m.....X...Ow....._keyhttps://passwordreset.microsoftonline.com/js/Common.js .https://microsoftonline.com/.&P.#/.....o.....z....Z...v.x...D`....V..../...A..Eo.....j.....A..Eo.....&P.#/.8.....'.9.....O.....\f.....(S.0..`.....L`.....8L`.....(S.....Ia.....QeNL.....GetCookieValue..E.@.-....DP.....6...https://passwordreset.microsoftonline.com/js/Common.js..a.....D`....D`....D`.....$..`....&...&..q.&.(S...Ia.....Qd.....DeleteCookieE....d.....&.(S...Ia....b.... Qf.....GetUserSessionData..E.d.....&.(S...Ia..... QfF.....SetUserSessionData..E.d.....&.(S...Ia....p....$Qg.EL/....DeleteUserSessionData...E.d.....&.(S...Ia....9.....,Qi.&.....ToggleAdditionalDetailsSection..E.d....'.....`....DI]d.....`.....a.`.....`.....`.....a.`.....`.....K`....Df.....&.'..a9.....$Rc....`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cb15386b3caf164a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	327
Entropy (8bit):	5.884219589973809
Encrypted:	false
SSDEEP:	6:mIYMjdSEQ99HSFNXYzbJ5XBkGdcmBIMwSsC9Qwf7VkH4s/bK6t:NjdHQ7A6JJBlc2n7sLE7OHl1
MD5:	4C81B35BC3005F9EC6CE7BC890B38A4D
SHA1:	37E20724E3F9C8E7AC73BBE46F08174975E6680A
SHA-256:	E98C57B3E44B541AB287491AC0B2A1C59C1B00336022841FD05821782BE66982
SHA-512:	30B34C83315E2596A7DAB01EEC80A8042C613E45D9A734B061BBF66542762A98606DF6DAEAAD9F28D334C14E13FD5F8CBC0D04841EADA5658F0C08F2AA57BECF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t..M...._keyhttps://client.hip.live.com/GetHIP/GetWLSPHIP0/WLSPHIP0?fid=9eee0ddc2b4e42129178b8f55c049679&id=282555&type=visual&mkt=en-GB&bla=32e9980e5989472c89443d5cc752297f .https://microsoftonline.com/D-DT.#/.....j.|$+f_.....{j.....".....A..Eo.....|..u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d2d66a99f78ccae1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	608
Entropy (8bit):	6.30883480642587
Encrypted:	false
SSDEEP:	12:oR5XyZsts/vnmAyABzwNA0qVa2sO4sIbmr4uG5Bd9dsa:ogsKnSAB0602a2sO4vK4uG5BdzV
MD5:	75D78E5F4EBD331A66D9C965AE6733B0
SHA1:	45D64DFC9EFB60AA5A93CDA30ACFDBFD7D907258
SHA-256:	33D465DFE9302CA62F9B081B0202D7CC5A5529FB742DCAF67B19A9534761606D
SHA-512:	112D7521B009B49ABCD8AFE35FA738440C67C2D2E17F05B7FDE7608C44571C869214A3A06001C391B6F4610AADAABD14963FD76BC0D990527D501B4EAA7201CB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X....-.7...._keyhttps://passwordreset.microsoftonline.com/ScriptResource.axd?d=7mNLgzlwuZkA9TAssKpNEJH0oT16Rgo-ReAyNXQwHT9wRhRx_M1IlwiCCtMk0_Xt0gbKmXCCilKfTYZO2VeK95CaMTFtOCc_dfveQouwE2i4mp2CPYVeXK0GrnuQYZeiN7RsfBmNBxycjNH8fHKWIZNjl4J1V69AAq4G-VIyPzGxRdDscKGQrpMhbxOFiTX0ibyf95DVidgfD6w_4rBjRV2u7FQLAyc0Tm4GoHy0kUc1&t=2fe674eb .https://microsoftonline.com/N.*P.#/.....Y...7.{0.Xt.....L...DZ!.0.$.A..Eo.....S_.....A..Eo.....N.*P.#/.Ps..060383795AF5623DB52E621A7828CDEE7CA6976C867ABC1799BDEA075EFAC823..Y...7.{0.Xt.....L...DZ!.0.$.A..Eo.....KT..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ef31c506f3510843_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	327
Entropy (8bit):	5.8613734890960725
Encrypted:	false
SSDEEP:	6:m+llVYMjdSEQQT6fhSYRDsNXYzbJb20ngsh3YYHGE5lQnK6t:vTjdHQQTIEj6Jb20ngsTcp
MD5:	D06F16EEE2A88287894A0D6F0A6946B1
SHA1:	E49AA033B162020E03B67CBB8E4170E87D17513F
SHA-256:	9C8DDF29B3CCE616B51615398E79615B6266E1CA248EABD2C012AA241A403646
SHA-512:	DBC6AD072A9260C6666B4604F3F52AF9841D1E311931FC3EA8629E7BB17DC2601E23056178CC99499E225D72129133BFB2735614F69DFACCABF0BB119110D004
Malicious:	false
Reputation:	low
Preview:	0\r..m.....4L7...._keyhttps://client.hip.live.com/GetHIP/GetWLSPHIP0/WLSPHIP0?fid=0256f3f1c27e4d6e932d97776c3cd4c1&id=282555&type=visual&mkt=en-GB&bla=81ec5b18706e4de0b309ca901935aceb .https://microsoftonline.com/..vR.#/.....S..2..6...l.g...h!....!.:....C.A..Eo.....Ep.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f12d30eb3faa08de_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\f12d30eb3faa08de_0	
Size (bytes):	6995
Entropy (8bit):	5.269216379093415
Encrypted:	false
SSDEEP:	96:QgsnsEEoU0gsK5l9Rhs7uM8LPbFqydTo8lXjDrzCUKdp94tKDX/AYRClsUvu+oc:SvUFThs4FqK9dDrhKp4mXoYRClp
MD5:	41941112EB3885AAA004E087F846EAA2
SHA1:	16C9EA7896C11AB7466711C71322B398A7C5607D
SHA-256:	9A72C157FAEF0C95D3BA7941F803EC02BBCC253F37C07FB13BB918FB99AEDEEA
SHA-512:	6F0D0895EA4B5AD00379B985DEE4212705F74E8CA515D3943CEA3C281FCFD9A4852C4F08FCE87206DB9AAFD740B6D4FFE96B9DDF8907308480CFA3A0D5E60FC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[.....b..._keyhttps://passwordreset.microsoftonline.com/js/Webtrends.js .https://microsoftonline.com/..'P.#/.....{.....a..Y.a..t.(g.wm...r..td..qm...A..Eo..... .UZ.....A..Eo.....'.(.....O.....T..\.....d.....(S....`.....L`.....0L`.....(S.....Ia.....Qd&go.....WebTrends...E.@.-....HP.....9...https://passwordreset.microsoftonline.com/js/Webtrends.js...a.....D`....D`....D`.....`t...&...&.....D&.(S.....5.a.....a...Pd.....dcsGetId...a....1...IE....d.....&.(S.....a.....a.....Qd.....dcsGetCookiea_...-...IE.d.....&.(S.....a.....Pd.....dcsGetCrumbaZ..._...IE.d.....&.(S.....a.....a.....QeN.%.....dcsGetIdCrumb...a.....IE.d.....&.(S.....a.....Pd.....dcsIsFpcSeta.....IE.d.....&.(S.....a.....Pc.....dcsFPC.a....k...IE.d.....&.(

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f2f9dc233f4dd8b6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	6.010493316271766
Encrypted:	false
SSDEEP:	24:ngs/FgYLDoXoSSsvuNG0mW492NAgs/FgYLDoXoSGNtjGGNMy4lAzY5ZFG:ngs/KGD4SsyG0m8ugs/KGD4GLGGNMblU
MD5:	B7B17E42209BDDA40465C43C5652063D
SHA1:	F65E5B18F9BFE3EEF0A1675B1723643E5F469FDB
SHA-256:	F13870FA3416CB53691C6169A16464E99E28F5764B36C57A6DA66D76C23813E8
SHA-512:	04850B660CDF3FF9BB1AE614F7FE03C03A951FD082106BFEE99E3387A6FB13AB459C31326E2346A2729678E3FF480C09CC01F76684FB420C73C7A96D335F4630
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B-...._keyhttps://passwordreset.microsoftonline.com/WebResource.axd?d=HAV6PjMKiAmtAvxBgE9JDGqR1xYgZB9pt2QBI2F1xTQSAFrYUiGM1BxJOdDWhZpxCNFUfRU3SlziYUoa1F09hk3amXnacSgCXVRaH-uYw6yAQB2PQi_-Ypkq4d_dItTGjGKE2EOOrlXy_zc-y4WHcA2&t=637560635036175728 .https://microsoftonline.com/.P,P.#/.....,.&...uQ.P.YKN.....+Z..''..A..Eo.....7b.....A..Eo.....P,P.#/.....'.....O....h...P.+.....(S.0..`.....L`.....0L`.....(S.....Ia(...'....,Qi~'.....WebForm_FindFirstFocusableChild.E.@.-.....P.....https://passwordreset.microsoftonline.com/WebResource.axd?d=HAV6PjMKiAmtAvxBgE9JDGqR1xYgZB9pt2QBI2F1xTQSAFrYUiGM1BxJOdDWhZpxCNFUfRU3SlziYUoa1F09hk3amXnacSgCXVRaH-uYw6yAQB2PQi_-Ypkq4d_dItTGjGKE2EOOrlXy_zc-y4WHcA2&t=637560635036175728a.....D`....D` ...D`..... ...`....&...&..Q.&.(S...IaC..... Qf.....WebForm_AutoFocus...E....d.....&.(S...Ia....o.....QeV..~....WebForm_CanFocusE.d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f31034cd60667b7f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.711310216190712
Encrypted:	false
SSDEEP:	6:m6ZPYiRDHjfRpA7qYsDpNdNFvNgD964kjmRZ1FBHhJ7K6t:rZpDHIqn/xNgD9Zkyf1F5t
MD5:	377A5B4F1EBB5CDF72884564EF45D328
SHA1:	96958EA7074B205181567BD8AC9093CF0C618F37
SHA-256:	175F410F8659CC40CDBDE77E7271C93677DAD3E10B1944AD086A80864D5BC9C6
SHA-512:	64A1C2DE4FFC00D33980D0C7CDC1CCBDC9A08CE6392CFBA57F01B0304F18FA939CCFFAB1CF05A04FB6FE10066CACD5422CC37900CF7A9CD620B4690F464F487
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...Q....._keyhttps://c.s-microsoft.com/en-gb/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4 .https://microsoft.com/...R.#/.....,.....n..,..P[.7Nj.`...D'.....A..Eo.....7i.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f469a98fdcf53c25_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.706522024626243
Encrypted:	false
SSDEEP:	6:mTJIEYcRTRKGKcqdsHKT5NdnSVnAqPdzfDLgrBZK6t:SkcG5NdIn1PdzLUVT
MD5:	E62EEAAE1278D673ACB14A51BCAD25B4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f469a98fdcf53c25_0	
SHA1:	3CA74EAA7BDDE3541596173DDE752068451C66F0
SHA-256:	8E53E4C405BC8771E426FF17358C1F089928F82679D40756665EB04A42E07505
SHA-512:	303929A0FA54D071CD26AAFBD2A72161D49072D555DE608E3C2EB33097ED60D3A374913A9301471BAE0DE51C11F3D05AA0506082872256FDB16A0D496CB3A60
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...z.>...._keyhttps://acctcdn.msauth.net/knockout_old_GJ62c6D9R5HuKFdkoO8XYw2.js?v=1 .https://live.com/...S.#/.....`v...../fe-*h.8.jd...L....J6..N.$.d.A..Eo.....HC.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f46ad1d2652b0b43_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.52159615309936
Encrypted:	false
SSDEEP:	3:m+lSxla8RzYJb9yKlf8QPKxQBHWFvDFYtRG3ydlvXlHCIHgXlDjyq5EzDHz4mMlR:mfYyK08fUH1Dw6gaq5EfzrkZK6t
MD5:	6C869023DCD5AF14CB1D3DB49FA1EA03
SHA1:	25959BC496602BAA883C18095743AE37CE3D78F5
SHA-256:	E2159A54509F761D98A6D7D520BF04169598FAF7BE07872DFE180E6AB84D4E55
SHA-512:	1B42D9D260B6F3FA0B8DFB9D64CE8048B2634B75ABCBE900BB418D9706D1ABE494C7F58CA52015C4570145C7CC1AC309CE615FE03176202B23F6AACD3C8D3A21
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...T....._keyhttps://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js .https://microsoft.com/Wl.R.#/.....-".....f....cB..cWhT..6..(..$....G..A..A..Eo.....x.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f6ef8939da32ec75_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.658590851907274
Encrypted:	false
SSDEEP:	6:mKYcRTOWxEDLU4G3eLPDNdbtA6ltyZVl/hbhK6t:eRLU4MUrNdbTXOlR
MD5:	452B3B3EC54E1A913F78266C2F998A15
SHA1:	07AEFD08BD4CEAEE77C0EE406A538CD5ACF1F0CF
SHA-256:	B11224C7F113C2B8B7C8B54F23B070F581F8B7271E5EA2CE75E8FA249B265F4F
SHA-512:	D0FD1089A6746A636988D23C1F6E1427D9CBE683AD89DA0A2556C7FAA8A23C5590F430595227EA7F204000E8F1567B0FD57DDE6F62BEE6FDAEB249BEDB081AF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...Z..U...._keyhttps://acctcdn.msauth.net/bootstrap_3.3.0_B68S-_daR6nLiLVZsh4XiA2.js?v=1 .https://live.com/i..S.#/.....Pv.....&<.}...k4E/q..Py..p.8W.G..*.2....A..Eo.....p.i.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fca8dda49898d420_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95224
Entropy (8bit):	5.633776454995954
Encrypted:	false
SSDEEP:	1536:BudV2uwIWd5ZCY3VTSoa/6PTnADxTj9Q4sTFQFHuIsy7MRZjsLYNSncvsy7+j:IVjwF5Xwi41jrsTF8Xlj
MD5:	806A7229B2867BCFED65AD5F920721CB
SHA1:	DB6391696F5976EBC9C60FBE033640456C07B468
SHA-256:	42882DBD7E4CA6E1A56229D4AFF3F83923B3200EFA67BF669D0F18F17825DAB2
SHA-512:	B5CFF348EF80F0917B0D42192C8DDDA93C604ACE81C47B09B7DFD3BF76939DF1A3062E2951525445F635144920F9B52859ECB8264CE964DF27EF8BAAE85F88C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...+].....060383795AF5623DB52E621A7828CDEE7CA6976C867ABC1799BDEA075EFAC823.....'.....O ....r..fM(a.....(...;.....0.....(S...;..`.u.....9.L`.....DL`.....(S.....Ia.E...G....QeJj.....Sys$Enum$parse..E...@.-....E.P.....6...https://passwordreset.microsoftonline.com/ScriptResource.axd?d=7mNLgzlwuZkA9TAssKpNEJH0oT16Rgo-ReAyNXQwHT9wRhRx_M1IlwiCCtMk0_Xt0gbKmXCCilKfTYZO2VeK95CaMTFtOCc_dfveQouwE2i4mp2CPYVeXK0GrnuQYZeiN7RsfBmNBxycjNH8fHKWIZNjl4J1V69AAq4G-VIyPzGxRdDscKGQrpMhbxOFiTX0ibyf95DVidgfD6w_4rBjRV2u7FQLAyc0Tm4GoHy0kUc1&t=2fe674eb..a.....D`....D`....D`.....Y....`....&...&.(S.....5.a.....a.....Qe.....createCallback..a$.....d.....(...IE...d.....D&.(S.4..`$.....L`.....8Rc.....O....M.a....$...I`.....a.....a.....Qe.$.....createDelegate..a....*....(S.....Ia.....I...'.d.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fd9925bdad311f6d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19486
Entropy (8bit):	6.01516179293452
Encrypted:	false
SSDEEP:	384:ExLxEkL5B6H1cwJvB1eFS5GWvenAff8qKvaN:kkK1WveAbK+
MD5:	490CE23BCDAA246DBCA555813E4894C0
SHA1:	B58F6070F1BD9923D6265E8E9F87948861A71DF7
SHA-256:	0D829B23C271C33FFC8A1A6AE51B9E66EBD919D799003273A0564F2A523CD367
SHA-512:	9B080FA2929E6CB6F58D778794370332A1B90E767F3AD08808A5C51672E7C545755568FF0C3EE5AD11978D2734367BE09C6543E2E8EBA5F80B1B575D3E2B1140
Malicious:	false
Reputation:	low
Preview:	0\r..m.....% .3...._keyhttps://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/9d-b58f60/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/6a-234a32/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1 .https://microsoft.com/..R.#/.....(.....):.l&.A.....G.,_0..p.~.A..Eo.....W.....A..Eo.....'.Y.....O....H...!.....4.....(S.0..`.....L`.....(S...`.....L`.....LRc".....Qd.xn.....requirejs.....Qc.nuy....require...Q.@..;....define....Q.PZ..3...__extends...d.....l`....Da.....&...(S...`.....L`>.....Rcf.....*....Qb".J.....n.....Qb.....r.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Maple help database
Category:	dropped
Size (bytes):	1032
Entropy (8bit):	5.390287303256244
Encrypted:	false
SSDEEP:	24:MciiQqzH9jHMtHPHSgHtnHOyby/DHu2hUW0jpFSYom/u8iyxscEcKI:McZQ+H9jHMtHPHSgHtHOyGbu2uNdjiyt
MD5:	117AD56EAD44A01EF447C94F80AEDCE1
SHA1:	3370203B38CDB096B1951F022360F60AE2A76E37
SHA-256:	34EE34236E8D3A32180C0D065FC61D4A324ACA32990C0D75AA2A26257C9C1501
SHA-512:	58A9924F33070138FA21265ACA93296E8796035B30CCF6FE4D6ECED65D41D5866CC45C0B10C6A323A8D28B5791BFEF18F36413EE82A067BA6800C516C3B3705F
Malicious:	false
Reputation:	low
Preview:	.....p:.oy retne....).....e.....J..<k8....tR.#/.....SHM..Y..7R.#/.....M.wOY.L~..7R.#/.....t0%..4.|.e(R.#/.....q....0&.e(R.#/.....%<...i..e(R.#/.....pT.....e(R.#/.....u.2.9....e(R.#/.....C43.xB.e(R.#/.....d.....Q.#/.....k-N...bQ.#/.....{f`.4...{.Q.#/.....{.Q.#/.....m.1..%.....Q.#/..P.....p.&,.<..8.P.#/.....C.+e..j...P.#/.....C.Q...1..P.#/..... .....tR.#/..u.....7...].~9.neR.#/.....b.(..@P.#/.....M?#....0P.#/.....R.C...tR.#/..d.....j...0P.#/.....I...tR.#/.....@..U.q...0P.#/.....:....0..0P.#/.....+..#...0P.#/.....?.0-..neR.#/.....5j..K...0P.#/.....<.W+....0P.#/.....7.!.l..d@..O.#/.....j.....@..O.#/.....7..Ib!.@..O.#/.....^}.Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.0085675789099615
Encrypted:	false
SSDEEP:	96:dNwnscAjEscqscEzYs2sJi4assqUbzkmcsZsmq6sTxG4xscAscdscRwsrsnsOXsI:dugjIzyFbz2xYQSu9NgG8/mxLzqxwT
MD5:	9F0394797E37B4FD9E95C40C8DF952F3
SHA1:	00973A9102AB4F2A0A61251465B027AD6014BAD2
SHA-256:	292BA4B2E9A7A7F34AD7896FDC27186A926928164F510B63CAB49BAF1143CEEF
SHA-512:	61E8D83BDDBCFEDF881FB8EC3BA9B252F4D5BD488FE7F3E509B94BABF80BEE6C1DE99BD8767C4240A69DB19BFF4FBE3929BFE08EEA3786A563F1AD1663242C99
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	25672
Entropy (8bit):	1.8850989012619388

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Encrypted:	false
SSDEEP:	96:KNeWcNwkIscAjEscqscEzYs2sJi4assqUbzkmcsZsmq6sTxGPxscAscdscRwsrsR:KNeWcuijIzyFbz2xlQkMuk
MD5:	DD996338F08E0005D26CFB402087DC90
SHA1:	A72DF683FE687AEC65DF69C1D3862E617AE5AFB7
SHA-256:	9EE3187C2EF2ED87D15C027C2B9FA79C1B3A6F2CBBB3FB36CD789047EC58652D
SHA-512:	8FDC92391985750D0BA6E884486E6C9F44E63A402958FEC5C33F30E1F98FFFC725A1ADF7C7C9E9B395CE3C4DD1BF172E9639DE5078305754401374C0B962B9C
Malicious:	false
Reputation:	low
Preview:	.....T..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25751
Entropy (8bit):	4.648353433479462
Encrypted:	false
SSDEEP:	384:5vQFQUNiPHSQ5QIQUNiPHlQKQIQzQUNiPHSQIycl:5vKQ9HSunQ9HltUQ9HSf
MD5:	C08E495DA8ED4F65C23DE3388528B6EB
SHA1:	B081F093482D8533A7B9F6C8BD5EDF8454872E71
SHA-256:	08F30F375CD71A23BAC664F57F042FC06561CA376630EEF7F48CF0DAB0A11A35
SHA-512:	1960FF63E3D909B73C6E533E6309AD4E733D5905C7FA2215FD2F9F9C45B8000C53CC41556B94731388AE506ABE558D6041FA2ED79EE23351B18609D6F6437971
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...9677db6a_ccef_4386_8b86_155ea5f82df0.....q.3..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....O...http://www.leo.lopez.sakshamsevango.org.in/br/?bG VvLmxvcGV6QHRlYS50ZXhhcy5nb3Y=.....h.....`.....6.....6.....H.....`.....O...h.t.t.p.: ././.w.w.w...l.e.o...l.o.p.e.z...s.a.k.s.h.a.m.s.e.v.a.n.g.o...o.r.g...i.n./.b.r./.?.b.G.V.v.L.m.x.v.c.G.V.6.Q.H.R.l.Y.S.5.0.Z.X.h.h.c.y.5.n.b.3.Y.=.....8.....0.....8 ....s...https://list-manage.agle1.cc/

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.185004597724087
Encrypted:	false
SSDEEP:	6:mwr4M+q2Pwkn23iKKdK8aPrqIFUtpDrpFsZmwPDrWMVkwOwkn23iKKdK8amLJ:f4M+vYf5KkL3FUtpPpm/PPWMV5Jf5Kkc
MD5:	E3848D312C1171AB9643700BB404685A
SHA1:	04093EF13F171951BF3D11292662DDDA6CCB2F57
SHA-256:	EF36C056091056FC5A68C341F0EDC4C93ABB2DEE6E1F156458D077F7D1C4359D
SHA-512:	EC40948DCE1EA4C02B4BDAFB16414A89CDBE5DE61B95D9A1D58CE28164227761D0EB97C057E63652FAF847D80173405F4BEF060F9557A0B80AEAB565D9992F 6
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:03.095 1a6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/06/11-1 9:42:03.096 1a6c Recovering log #3.2021/06/11-19:42:03.097 1a6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f. 5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.. .....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.200508968163976
Encrypted:	false
SSDEEP:	6:mwroHN+q2Pwkn23iKKdK8NIFUtpDrOZZmwPDr73VkwOwkn23iKKdK8+eLJ:foHIvYf5KkpFUtpPOZ/PPh5Jf5KkqJ
MD5:	DC282A811089E6EA8723F4893F6EC720
SHA1:	022A59A055347388E56E5A0058C867FC00B491CA
SHA-256:	BF8A7FA81EB82124CBD16A22511E1475DCC806EA4DDB6E7ED367D0CCAD9CE8C1
SHA-512:	AF41EB360ADDA5988213E7734467F21D766EC3C295A6D8CC3C1C0504692651DFEB85E1CE9ADE4249E946386D3131E6718FEE0BD24D73AEB62765A5FDF47B0C E
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:07.321 1a68 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/06/11-1 9:42:07.323 1a68 Recovering log #3.2021/06/11-19:42:07.324 1a68 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
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):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	92160
Entropy (8bit):	3.166042956868858
Encrypted:	false
SSDEEP:	384:gyk5XGOnxQWI9xrI6GGQDQb5QKJFGOOFY5QSsFGOvlYUMY5QelVY5QDsFGOTY:hk5jxdCMUbNCGBsN9uG/rGMsNTY
MD5:	65647BCAFE524248BAB3BB544E5B14F5
SHA1:	40620F11C2372A302094F41C21EB9E374FC69D9F
SHA-256:	9C3D431CEDAF9E1B0592A056224E02E2F43BE9B0CB7A643BBC4292E71D63126D
SHA-512:	2152088DACCDA54423A59FEAD49DD01F7A7521A02813E8D5D7EF3D123BDF21B58ED5B47747C130E92CCD10334B0963D30E046C8CC6CD6DEFACF6EC9244533E
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Size (bytes):	82804
Entropy (8bit):	2.375118332623693
Encrypted:	false
SSDEEP:	384:pXtBkYFGOki5QdSFGOtdY5QzsFGORLBlqMY5Qi:pDkUhJNvGssNtNGV
MD5:	C492223F894B4443A9AB76F09737CE42
SHA1:	312949945C2FEE58C10F0036A7986E9A871DBA82
SHA-256:	6EA3BA7C210AB30A7FBCCAE8BCBB7DB2AE8F6577F5A2954210F90BEAF5A9915F
SHA-512:	1880D3C6D6E48DC17FCD2A089DB3CE8A4E435CAF63CE11A5986C8DAA92E63D6D9A009CC0F5E36CD7E1D346C7BD27DAC7521F12598C98F6B4729887676058E2F
Malicious:	false
Reputation:	low
Preview:	.....@..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.302305142534411
Encrypted:	false
SSDEEP:	6:mwpRQtN9+q2Pwkn23iKKdK25+Xqx8chI+IFUtpDpRQlJZmwPDpRQA9VkwOwkn23U:WN9+vYf5KkTXfchI3FUtpCJ/PT9V5Jfk
MD5:	48318654D450FD1A489D617EFEBA9B92
SHA1:	9A09612CB69F562FBA81F6431DD159705E1D498A
SHA-256:	A4AF1DBF1A01069C4C30B019DB5E4F875A1D518E15769930A1A45E42FCEB7C19
SHA-512:	7FD0CBEB9EBDB0A635C12AEB6C7B7A5D80B35F63699C26CDAE9F5D48531DB7EA584284D4779320D766020EF3B37E0797264DE78433102FFD3B6316F59EED462
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:23.555 19dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/06/11-19:42:23.557 19dc Recovering log #3.2021/06/11-19:42:23.558 19dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.201002317455247
Encrypted:	false
SSDEEP:	6:mwpH9+q2Pwkn23iKKdK25+XuoIFUtpDpUJZmwPDpU9VkwOwkn23iKKdK25+XuxWd:t9+vYf5KkTXYFUtpKJ/PK9V5Jf5KkTXp
MD5:	617FD2D24B4DC4684C623FB2FECDE613
SHA1:	84FC2E41D66880AD92E25D2DD053AEA4408EBB5F
SHA-256:	F70D7C7EA4887B46B9935008EF7716B10F375B339A523AFE48E676D6B9A8CBDD
SHA-512:	F2819969908969E8C7F06BB98FEB32A82790E43B638D0F5DA11EC038630F620640D834DEC37E9922BE8A7A7BC1A0936EF174DE8606E090844136E905868510A1
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Reputation:	low
Preview:	2021/06/11-19:42:23.242 19dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/06/11-19:42:23.243 19dc Recovering log #3.2021/06/11-19:42:23.243 19dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.233188622357525
Encrypted:	false
SSDEEP:	6:mwpV/MQQ+q2Pwkn23iKKdKWT5g1IdqIFUtpDpVUvgZmwPDpVRISQVkwOwkn23iKN:/MQVvYf5Kkg5gSRFUtpcg/PhrI5Jf5Kg
MD5:	E9917BE10006B60D464524B879561288
SHA1:	4DB08EEECE7CCA6F3671C5982DCC38E500AC0E9D
SHA-256:	1EF7092DE0311C4FEA420F545B94B68C840494724715F090829E23038D5EFAF7
SHA-512:	EBF8A95E9A313F202A5C973A8EAC3C6027001DFB9F873A60CB97A30461B9F31D964DDF402637EBF023DE597224C691C88E4B066BD77CF3AA5ED234925D21CE8 3
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:23.101 1f58 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/06/11-19:42:23.102 1f58 Recovering log #3.2021/06/11-19:42:23.103 1f58 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	1.550373763960367
Encrypted:	false
SSDEEP:	192:SYSYC2i4QZQyYSY2Z2+QYQ3aQZQyYSYRZ2HqaaQZQyYSYMZ2MqTQfaQSQsISYcZ9:fQZQmQYQKQZQtJQZQ9TQSQc
MD5:	8E133DF2FDD2587BFA89BD5C77C1CAD6
SHA1:	2DC90E031B12399FF18F423AC38BF670EF967A72
SHA-256:	93F50A9250F98E5B5D979ADECC9A2B0D5D04C74943DEDAAA15E84DD67B9F7A05
SHA-512:	143FD71BC4337D1E56FBEE8FEE5B6F6A509A3A6E94316C90965DD9BFF180209158443E1C55DEB48B321B029AC637949D201AEC7F9C4911558168E7F1AA32956E
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7061
Entropy (8bit):	6.454008091278636
Encrypted:	false
SSDEEP:	96:J3MsldH8TgFNEzq8s/sINMysDQ4ZZNoq7l/sVsKsTQgsrs2j46hQvixwIsEhQ+Jn:DdxmP3rtZS0C7sTqQqOohBJn
MD5:	8C2F108BA3E4D9B9F871E00240570DC5
SHA1:	A507E0F16C800D6D622039B72CAEA2850848F46A
SHA-256:	134C1CB5163C8FF836B637AF217E5C609E21893AE19C1A0222B6DA3789514DB0
SHA-512:	D4204A57F8F3A17B5558B3AE136AEF2A901A9BC710777496D093FFA84DCFBA9D051939A6B5A1E32E0557DD767B7DECAB121B14E9F4FD739B1A112370C18C8D1 9
Malicious:	false
Reputation:	low
Preview:	....."...K..1nfdjboi5afiaajlbsqrnac6bag7l0."2qpqktvlxxsksz0dqdmahxacigylzexcll..6jepui.,a9svoloqx2qmcxivvaez3zmxcm5hi67rodedhtyzjwq1.$abvsj8kxwuzfhhcfdb cyaocczuahbbjwd8kd..com..common.-cq28ouularu1mslfqqqtqzjdhulqm5adqzduj9pwigvk6...cqv2ehmh0zhnjww3uqp60tonoei01effocyrhdg42gohmvittjqupsuadrsiynybfpghi uq9a44ielzslphrz0mvxuspqavte77vm4e18enio3nzerxycjsukztmpyrqtzuttrjfldrs3n0uwmgavusy9wu74mejqitz8d1zszjuttgjuuds88y..ctx.%dnrbfskutzdlhndzjz8dilwshjzkl qkny0z9p..fl278. ga9lwjoq2u5aghhf87dkdp5m8jsjz05m.'ghzef0lnzsre6kxyvi7t1h2kqohzvtcwxbwifgz.7gpvgivqak8lwanbfuxaghzroomyiwqibimbdetgfapjseecycyj4ozo..h ttps..jugxviqkwicqkx0f4clk8633ro..login..microsoft..microsoftonline.!nmyeqxylkckioxwhzx3umirhdhncaxbgv..online..password..passwordreset.<peiizwkdpehayvvdaww0afl w70xy4hp5burry3cw9y27knd0fhd3v1ftn3q3..rant..reprocess..reset..rqiiaywso2..ru..sjqltccafeeqsqb4jygl..stwhmxnkiskd8vlne1low07hluyqr..tjjyisiodhlbxzoescliw2o.Ntua bg46rnh0mpcaesulukbotk5nrxj7oict8sp4kt14mt1bfsfl8so341durgaznjj4aymvyw

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	154468
Entropy (8bit):	1.2058107608661848
Encrypted:	false
SSDEEP:	192:G59YSYs/28QZQyYSYxZ2yyaQZQyYSYpZ2+aaQZQyYSYkZ2t:G5pQZQdQZQhJQZQb
MD5:	FCF08B71CC245F705D2DDD0FA61A7C2E
SHA1:	7D635475A0BBBEB0E27C3EBE96D0A83E901B826E
SHA-256:	6659AC5E26CCC448FAEFE0A11A44690CE8378B94ADB471D8879365B636FBE615
SHA-512:	B085F209889AD2234B939BAE09208918A4CAFA8142175734B92B7CDA9A15A4103B6219A621A9ACA84901D237474D2F4E94586B67E6992561C0500D98AE7BD87A
Malicious:	false
Reputation:	low
Preview:	.....ha..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Sub-key -
Category:	dropped
Size (bytes):	2953
Entropy (8bit):	5.481600285474561
Encrypted:	false
SSDEEP:	48:NbGcB7a7CMp8dbLs8AbQSefgGFNrS0U9RdiN9pZV:1a7CMqdbLs8AbQ5fgG3rS0v
MD5:	45F1162EC709A6B86423832C7F1F6C49
SHA1:	3628951437CADB1038ABDAEA93C601DC3525C008
SHA-256:	281F3CDF243247E37029465FFD6DCC865B7C8BB15E7F28BD25FA436B6BDB5151
SHA-512:	122A71E439D8FF4979319FEB33E07D66B110DD58A76113FE9131FE249221123BE1D5221E822E81C5FFC52D3D07267E4022B5A5B88D7D489BBB3941177DEDF449
Malicious:	false
Reputation:	low
Preview:	..._...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..1166000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-06-11 19:42:25.18][INFO][mr.Init] MR instance ID: 473d2df2-4e28-4320-9062-db93689d7765\n","[2021-06-11 19:42:25.18][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-06-11 19:42:25.18][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-06-11 19:42:25.18][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-06-11 19:42:25.18][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-06-11 19:42:25.18][INFO][mr.CastProvider] Query enabled: true\n","[2021-06-11 19:42:25.19][INFO][mr.CloudProvider] In

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.201014186753408
Encrypted:	false
SSDEEP:	6:mwrxt9+q2Pwkn23iKKdK8a2jMGIFUtpDr3l3JZmwPDr+RdN9VkwOwkn23iKKdK8N:fxuvYf5Kk8EFUtpPVZ/PP+RT5Jf5Kk8N
MD5:	43F33E441828DC3609B3E8E090A31EA3
SHA1:	ED8EC15E39D3DED87B66775A5C28416E0A008D26
SHA-256:	2F163BF7B08F596CF6DF854DA5FA58D979D41AFFE6EAC2060C93488A127053DB
SHA-512:	68FA78B25CD06EC7A94D87F042517FB63D49821EBF34045E7414418035E4452F792E4079B30D5689F62C1439C661471BC79808613B8AAE8C1D773C13EE5E57AB
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:02.743 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/06/11-19:42:02.745 1a48 Recovering log #3.2021/06/11-19:42:02.746 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	122880
Entropy (8bit):	1.4381537619971774
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	
SSDEEP:	192:HtehVAUfUUHFUeQmALUHFUCMpJ/LUHFUtILUHFUg:HtehVAYU+bQmE+ZMpV+WM+9
MD5:	50268AAD6347936B09F7457FC53159E5
SHA1:	53271B18AF80392D2F79CD4FDD576380FEBA9E60
SHA-256:	F8028877006C8719E7830076E06EE948959C4F31D3AA39A7055177B7F09677B1
SHA-512:	CE1130DF81D23748E37DBC39DED93F1367AC9FF7180B90681889C76E27CD75E68895A0FC3BA66631D9BC193DE788703BA48120B90C11066F14AC24E2B30193D
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....,.....\.t.+.>..,..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	128360
Entropy (8bit):	1.3115209188086248
Encrypted:	false
SSDEEP:	192:Bygi5kYSiC+UZydJUHFUQiFLmxCYLUHFUey2/LUHFUuiz:Bygi5kYSiC+uydJ+PiFLmxCc+NyQ+Niz
MD5:	E014FC25DDDDD808A3D861C6012B4E1F
SHA1:	68F1E294B17CE77C5831EA41495FB645FD536BC4
SHA-256:	8A9ABFEDBF786428CACE3EF99C0D3B33A549A0F49436742AE403C76434F3A460
SHA-512:	A06A04C96FFB5D08ED8CFAACA66F7062C6E1058285C7CD7CA1694D0FEEF6574825D579BE49C0754A30759212DE5F14AE6B9404DA83C8B4E4B84537BC3DBC317
Malicious:	false
Reputation:	low
Preview:	.....1..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.168660933471342
Encrypted:	false
SSDEEP:	6:mwr0jyq2Pwkn23iKKdKgXz4rRIFUtpDrT/1ZmwPDr1lRkwOwkn23iKKdKgXz4q8d:fFvYf5KkgXiuFUtpPT/1/PP1z5Jf5Kkt
MD5:	96EE3DEAC996DEE9BF055936CF2093DC
SHA1:	8A91EF3A4CE7D157B35D0708A6224EB32E32DC1E
SHA-256:	F3F10EC8E050B838FD305165BD8F75EF3CFB4C73397E8F428225240FAD931859
SHA-512:	88BD1D686D78AA919BE48F0B4CAD14B9D67FF1B100BA507EF779E394BB20B97F202B6E42BC06A37463D3B448B5178202577AA5F0330A6C035F8C0DADFA8F602
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:03.133 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/06/11-19:42:03.152 1a14 Recovering log #3.2021/06/11-19:42:03.154 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.8218828702582177
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUpDEsW7DEsb:wIElwQF8mpcSnQb
MD5:	9072BD9DD8D7650D0337C452FF0E307F
SHA1:	D7CE1687A57ECB8069CF44A9A5446F78891968E1
SHA-256:	327534E3D5C2EFAA40DCD52CA709C9909E81F1527486361A2B91E8521C07EB4D
SHA-512:	77E9D0935D9377CB4F4D9B91882248B9D1CC56CA4FD19528DE80E0FE44F7971CE679E2CF89649019627B86E4AA655E837A6E9A2263713DACEA8117D519EAD3E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6281002083009191
Encrypted:	false
SSDEEP:	48:ogMgwHKFHXxqkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUQ4:og7wHKFHXxhIElwQF8mpcSj
MD5:	AACA768BE0395DAE37CDCACFB639E5F7
SHA1:	C9CF4B2FED80BE74F2F3993A60D37020D0558150
SHA-256:	8DB012A687BFB62974AE3D161A82F202354AD0857FF6A086997FC7EF7A23CCE2
SHA-512:	78A2539637F4D043BDB8EBF1374D50547ABFFD67EBA35A373AEBCC0017BD56C6E5B8C6C261E679459E41AE03F99FC21E2A58EE3F307F3D0E090D9B52B36562A 3
Malicious:	false
Reputation:	low
Preview:	.....^..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	495
Entropy (8bit):	4.999610287537274
Encrypted:	false
SSDEEP:	12:5ljljljlgnHllu0f81R5XyZsQvDld3uauRR1R5XyZsQ3A/XiXQN/6SlhBMxR5Xyt:7ZZZgfu0+gsGT3uau31gsvXiXKBlXsgr
MD5:	77AF19B5CAE4B46DF54BE64CE8B33B7D
SHA1:	E136A7B4C6A1320974DD023FA3DC443E57E51ABF
SHA-256:	6EE3B5BE8E27779C22E5D865C3C1A957901DF71FF6B7DB7C9A033F3FA65D4D68
SHA-512:	5A05A9CD903A34BFE8CDDDB0DEF5238F87614BE06DDD4D3E087EECB5ECB2151B79E8E4452836E1EDCFAEF32F0AE7AEDA74FFA86DD431F328E41AA4AD7C55 58FD
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....Bx.....next-map-id.1.Ynamespace-9c9f1125_a9ff_404b_a721_ea9c1522b6a4-https://passwordreset.microsoft online.com/.0FK.$x.....next-map-id.2.Ynamespace-c5b1f6a3_010d_47db_87f3_44d2bd2a13dc-https://passwordreset.microsoftonline.com/.1. .....V.x..... .....next-map-id.3.Ynamespace-080b9d42_7902_4bdd_be91_d34b5733bb79-https://passwordreset.microsoftonline.com/.2.R.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.1100435717036135
Encrypted:	false
SSDEEP:	6:mwrxyq2Pwkn23iKKdKrQMxIFUtpDrvS1ZmwPDrvERkwOwkn23iKKdKrQMFLJ:fUvYf5KkCFUtpPvS1/PPvE5Jf5KktJ
MD5:	D3016BE087294C3B8B03FABB0A252FA4
SHA1:	B822AF2E815BFFB92E0F92B01702B579106ED21F
SHA-256:	A901F9614DA57E7F21019DD7E0D7C2E09773AE86172185E88B919F908C3ED4C0
SHA-512:	C95F1D557252BE4180114B4D673B3092113ED1A7587B1D3CB78CFE72558A060B4496E9C6137BF25F902F05405B62AF960D10C1571927C7A9B8FFF03A67026FAB
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:02.988 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/06/11-1 9:42:02.990 1a14 Recovering log #3.2021/06/11-19:42:02.990 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.153688928728381
Encrypted:	false
SSDEEP:	6:mwrgCOyq2Pwkn23iKKdK7Uh2ghZIFUtpDrgdW1ZmwPDrg0ClRkwOwkn23iKKdK7w:fgCjvYf5KkIhHh2FUtpPg41/PPgz5JfI
MD5:	873A25E8F684534F1E2EC977370482C3
SHA1:	F66F26CD124A8B5AA5C88791AB0396E82F82A189
SHA-256:	6BC66FA6E7EA483E594652786FB709EBD5F586B572AC4B9E1AC3A4321290CA3B
SHA-512:	FC3E2AB84CED505BCD01DED938D7DC578147E734A78B9E072E490D6B7A64C5586725DAD1517D9198029D0CCF13646042635A326A3DB158C3D046C9139B67617
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:02.653 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-00000 1.2021/06/11-19:42:02.658 1a14 Recovering log #3.2021/06/11-19:42:02.659 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\26c40031-9f82-44c3-8d35-6e35403 19a60.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):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\33c44a09-f198-46e7-82f2-a99a935 d3993.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):	325
Entropy (8bit):	4.975147286312194
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sdHfHYhsBdLJlyH7E4f3K3X
MD5:	A6C1D2076E0E7FFE40E5BFEC0BEAFAA7
SHA1:	F1CD6815325610D07455A215A1C4E724D2F1DC17
SHA-256:	3B3BD7020547A67DD4A6A30E8ADBC4A5921570268D7E0182053BF5412F5BFF50
SHA-512:	7534CBC15D48BEC22E52459AA3832DBA67CE0EF7A0C6B6A1192BA8425C056E8629176C2EF92BA977CC3A6BBB019236243C1C551630D0BC8902F7456AC90B8B7 0
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.244313818862519
Encrypted:	false
SSDEEP:	6:mwrjpM+q2Pwkn23iKKdKusNpV/2jMGIFUtpDrlmZmwPDr6MVkwOwkn23iKKdKusO:ftM+vYf5KkFFUtpPlm/PP6MV5Jf5KkOJ
MD5:	A667EAD90C28CCF003E493EB59AE0628
SHA1:	DF2A31F03B1D4759177BFCF59F54124FCA268F36
SHA-256:	5CC16BB7F1DB40A01CCB1D5493E0B9B8B5090C08EE790A108E1F42031A4B61DB
SHA-512:	071F676F947ABB547EB5734F3CADDC3D53714CD0B09C5976AA9F7DD1C17BE8E77CD12BBC3830EC4FC9C016BBB20515BF8770498B8FD7606BE568B7906841E1 1
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:03.072 1a6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/06/11-19:42:03.074 1a6c Recovering log #3.2021/06/11-19:42:03.075 1a6c Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.277960318101349
Encrypted:	false
SSDEEP:	6:mwr23+q2Pwkn23iKKdKusNpqz4rRIFUtpDrAZmwPDra3VkwOwkn23iKKdKusNpqS:fDvYf5KkmiuFUtpPA/PPaF5Jf5Kkm2J
MD5:	E81C27227BB2A5E1F627DC14981EDC10
SHA1:	D3F41C7226C46917930A92DBDC7175302ED8A206
SHA-256:	41773D5F9CA6A0D2DCA3F91CDFB362D702A148ADFCD33055C9D1371E44199FCD
SHA-512:	D97C713C8C0F9D491BA671355D46C6416D1D45753BDAEFB49BD6F180B1A81AC0A7B9A6B39F90225ECE0861965C424A23EBFA5C6C6D2C68EE01030ED745B1B8 C1
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:03.132 1a68 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/06/11-19:42:03.152 1a68 Recovering log #3.2021/06/11-19:42:03.154 1a68 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Entropy (8bit):	5.254558541587051
Encrypted:	false
SSDEEP:	6:mwpii+q2Pwkn23iKKdKusNpZQMxIFUtpDpCAWZmwPDphVkwOwkn23iKKdKusNpZb:Ii+vYf5KkMFUtpJW/PvV5Jf5KkTJ
MD5:	EB64C027920E5F3416477616A742365A
SHA1:	9B93F59866B0198A4A8804F23C93349326E85A1D
SHA-256:	660D4554847F66C8D5383F756324DBCDDC855DFDF4B39A1810D14265DBF7B6A3
SHA-512:	6D0022EB5B34608564B6044161CA9E6D21B5170115F827F6F69CF21398F7A1BA4BF0D9FDAF4DCB7FB83F9B61FB7321925225D565D85D1216A15548BE7EAB5350
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:21.353 1a5c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Session Storage/MANIFEST-000001.2021/06/11-19:42:21.356 1a5c Recovering log #3.2021/06/11-19:42:21.357 1a5c Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.191169150179315
Encrypted:	false
SSDEEP:	12:ZM+vYf5KkkGHArBFUtpJFs/PeU8MV5Jf5KkkGHAryJ:DYf5KkkGgPghU1Jf5KkkGga
MD5:	2BEFD615CF2DE999A83CA243C2F064F0
SHA1:	EEE2A6AD3174C47C9B61E81C257C380AA56A61D2
SHA-256:	133A1E32AB3CD5CF68F16D675F47F977D498FED5C83E5C090255930D68176FFA
SHA-512:	6C65370532A142CAA58A4E87F6F7DFBA88B7B8F27A56BF4FAB5E15881D83EA2B390E5A98AD8D86B7BC6CAAC597F666080DBD5DBE3244D9638E14D32AA6C95A 91
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:23.816 1a6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/06/11-19:42:23.818 1a6c Recovering log #3.2021/06/11-19:42:23.822 1a6c Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.224116420047405
Encrypted:	false
SSDEEP:	12:EvYf5KkkGHArqiuFUtp2Z/Po5Jf5KkkGHArq2J:uYf5KkkGgCgUUJf5KkkGg7
MD5:	B0175C67B45C07BABA91878B519E6EA3
SHA1:	617AA6ACBE264D1E5EECCDFD2A0996CE543F6CBA
SHA-256:	259D832E1B8F9B526900EB9E41A6CDB097F21B095990428866520 83EEB49F251
SHA-512:	9D4E45E0C956E02C56CF258A7FEF08D6FD4434E7050A62AF4B318A84C39E968185DCA9E0A1A3A303602638A8B5833F8454017036606858009DDC99DB28BCFA75
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Preview:	2021/06/11-19:42:23.829 1a08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/06/11-19:42:23.833 1a08 Recovering log #3.2021/06/11-19:42:23.835 1a08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.177686052670623
Encrypted:	false
SSDEEP:	12:J3M+vYf5KkkGHArAFUtpZP/PZCMV5Jf5KkkGHArfJ:JtYf5KkkGgkgfhPJf5KkkGgV
MD5:	02F5CD2DAA058FA0F0524116D6ADD878
SHA1:	90A0CC3E54FDCBC812F1B910062DA11238A0502B
SHA-256:	B801362EAA58CC4BEE374B02BA1CB85DF7DA46AE886D56A5C022393ED2684BD8
SHA-512:	DF73C4C24DFC807356C5C6C19F1620B46C9780756B32441CF2AB1A550729762540F38A119BF215B02CCF7CFA986164FA82349BB53C1ADD629E1BE496755EE8B
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:39.228 1a6c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/06/11-19:42:39.229 1a6c Recovering log #3.2021/06/11-19:42:39.229 1a6c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\bf5ae8f0-82c0-483a-b23d-a6a465cece41.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):	325
Entropy (8bit):	4.963653940178319
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sdHirhsBdLJlyH7E4f3K3X
MD5:	E94036DF834460DF6795F5DDCCCD0B69
SHA1:	0352869460986A77961DDB65A85572FFBF4AC0FF
SHA-256:	4087DF4160118C6F53D2E18B0A65B23FD373796A4285116852AF4EF927C40FA8
SHA-512:	9DD6536B6A73DD499D2FD882A469A51B7EC85AEDB8CD62F3D9C53A08994F8B1E16416C406962050B38F6C2289F77881D814555558A94BB7C59852AB655A9D0A
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\db243429-63d0-4e4c-b9e8-3dc94e482ab2.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):	325
Entropy (8bit):	4.9616384877719995

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\db243429-63d0-4e4c-b9e8-3dc94e482ab2.tmp	
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.199609410433293
Encrypted:	false
SSDEEP:	6:mwrZyq2Pwkn23iKKdKpIFUtpDrPEIFz1ZmwPDrsVARkwOwkn23iKKdKa/WLJ:fcvYf5KkmFUtpP8S1/PPsi5Jf5KkaUJ
MD5:	AF5EEA971EB8E3CDB6C2F7A01974EBD8
SHA1:	1F71D0573BC54C926E11D551BA5DD42E6AFF7BF2
SHA-256:	FBFC6D631416332B1D1E5D1AC31A9E4185695D9B7614FEC5490054AFC4C05721
SHA-512:	73CF2204C570DD5E688B59616DF69D4A6400ED0CF0F74EDCBD176D98165B94322BEB46330C6152CA93C2E6F6919561BC79D91537DBC5DB7C005505EA0328CD
Malicious:	false
Reputation:	low
Preview:	2021/06/11-19:42:02.687 1a14 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/06/11-19:42:02.689 1a14 Recovering log #3.2021/06/11-19:42:02.690 1a14 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.283276639106687
Encrypted:	false
SSDEEP:	12:KvYf5KkkOrsFUtpCEZ/PCEz5Jf5KkkOrzJ:wYf5Kk+gZJf5Kkn
MD5:	AFFAF46819A4CEF67E0570BFCA7324BD
SHA1:	7C24D86889BBD6907A3C27BA6D95B07DDC0D5B7E
SHA-256:	23EBC6DFF091BF6318E040BECBB322D13F5EFD9822D35EDF0054D25807818D76
SHA-512:	51BEDFCE55F698659AE703B90E1364A7ADE908BB478D7A0B1709DF403E3FF996550210FF9E59E95AFA3CAED264E684EB7EFCA4BB309E8D8DA6D3D1442E27C7C4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Preview:	2021/06/11-19:42:25.199 1a08 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/06/11-19:42:25.201 1a08 Recovering log #3.2021/06/11-19:42:25.201 1a08 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 19:42:07.339359999 CEST	192.168.2.4	8.8.8.8	0x93ba	Standard query (0)	list-manage.agle1.cc	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:08.200275898 CEST	192.168.2.4	8.8.8.8	0x97a4	Standard query (0)	www.leo.lopez.saksha msevango.org.in	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:10.058444977 CEST	192.168.2.4	8.8.8.8	0xdbe1	Standard query (0)	www.austraaliabondcleaning.com.au	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:13.054867983 CEST	192.168.2.4	8.8.8.8	0x9ddd	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:13.569386959 CEST	192.168.2.4	8.8.8.8	0x1157	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:13.627360106 CEST	192.168.2.4	8.8.8.8	0xd20c	Standard query (0)	www.office.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:14.068401098 CEST	192.168.2.4	8.8.8.8	0x8fa0	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:14.400403023 CEST	192.168.2.4	8.8.8.8	0x7673	Standard query (0)	passwordreset.microsoftonline.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:15.187150955 CEST	192.168.2.4	8.8.8.8	0x6cc6	Standard query (0)	r4.res.office365.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:16.258021116 CEST	192.168.2.4	8.8.8.8	0xc08	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:20.221597910 CEST	192.168.2.4	8.8.8.8	0x9eac	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:21.570316076 CEST	192.168.2.4	8.8.8.8	0xf74c	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:22.926176071 CEST	192.168.2.4	8.8.8.8	0x4504	Standard query (0)	client.hip.live.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:23.320987940 CEST	192.168.2.4	8.8.8.8	0xfc61	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:23.516002893 CEST	192.168.2.4	8.8.8.8	0xf5a9	Standard query (0)	scu.client.hip.live.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:24.891966105 CEST	192.168.2.4	8.8.8.8	0x8332	Standard query (0)	passwordreset.microsoftonline.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:25.049236059 CEST	192.168.2.4	8.8.8.8	0xea79	Standard query (0)	scu.client.hip.live.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:41.482995033 CEST	192.168.2.4	8.8.8.8	0x704b	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:54.983903885 CEST	192.168.2.4	8.8.8.8	0x1417	Standard query (0)	account.live.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 19:42:55.472831011 CEST	192.168.2.4	8.8.8.8	0xb323	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:55.548459053 CEST	192.168.2.4	8.8.8.8	0xcf4a	Standard query (0)	acctcdn.msftauth.net	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:57.046129942 CEST	192.168.2.4	8.8.8.8	0xf9a7	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 19:42:07.406696081 CEST	8.8.8.8	192.168.2.4	0x93ba	No error (0)	list-manage.agile1.cc	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:07.406696081 CEST	8.8.8.8	192.168.2.4	0x93ba	No error (0)	ghs.googlehosted.com		142.250.180.243	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:08.262068987 CEST	8.8.8.8	192.168.2.4	0x97a4	No error (0)	www.leo.lopez.sakshamsevango.org.in		216.10.243.103	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:10.116786003 CEST	8.8.8.8	192.168.2.4	0xdbe1	No error (0)	www.australiabondcleaning.com.au	australiabondcleaning.com.au		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:10.116786003 CEST	8.8.8.8	192.168.2.4	0xdbe1	No error (0)	australiabondcleaning.com.au		43.250.140.39	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:13.108041048 CEST	8.8.8.8	192.168.2.4	0x9ddd	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:13.639193058 CEST	8.8.8.8	192.168.2.4	0x1157	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:13.689044952 CEST	8.8.8.8	192.168.2.4	0xd20c	No error (0)	www.office.com	home-portal.office.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:13.689044952 CEST	8.8.8.8	192.168.2.4	0xd20c	No error (0)	home-portal.office.com	home-office365-com.b-0004.b-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:14.130014896 CEST	8.8.8.8	192.168.2.4	0x8fa0	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:14.130014896 CEST	8.8.8.8	192.168.2.4	0x8fa0	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:14.130014896 CEST	8.8.8.8	192.168.2.4	0x8fa0	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:14.130014896 CEST	8.8.8.8	192.168.2.4	0x8fa0	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.82	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:14.130014896 CEST	8.8.8.8	192.168.2.4	0x8fa0	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.162	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:14.130014896 CEST	8.8.8.8	192.168.2.4	0x8fa0	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.18	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:14.130014896 CEST	8.8.8.8	192.168.2.4	0x8fa0	No error (0)	HHN-efz.ms-acdc.office.com		40.101.136.242	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:14.476310968 CEST	8.8.8.8	192.168.2.4	0x7673	No error (0)	passwordreset.microsoftonline.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:14.476310968 CEST	8.8.8.8	192.168.2.4	0x7673	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:14.476310968 CEST	8.8.8.8	192.168.2.4	0x7673	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:15.247145891 CEST	8.8.8.8	192.168.2.4	0x6cc6	No error (0)	r4.res.office365.com	r4.res.office365.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:16.316536903 CEST	8.8.8.8	192.168.2.4	0xc08	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:20.284436941 CEST	8.8.8.8	192.168.2.4	0x9eac	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 19:42:20.284436941 CEST	8.8.8.8	192.168.2.4	0x9eac	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:21.630825043 CEST	8.8.8.8	192.168.2.4	0xf74c	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:23.004326105 CEST	8.8.8.8	192.168.2.4	0x4504	No error (0)	client.hip.live.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:23.004326105 CEST	8.8.8.8	192.168.2.4	0x4504	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:23.004326105 CEST	8.8.8.8	192.168.2.4	0x4504	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:23.390731096 CEST	8.8.8.8	192.168.2.4	0xfc61	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:23.390731096 CEST	8.8.8.8	192.168.2.4	0xfc61	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:23.582937002 CEST	8.8.8.8	192.168.2.4	0xf5a9	No error (0)	scu.client.hip.live.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:23.582937002 CEST	8.8.8.8	192.168.2.4	0xf5a9	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:23.582937002 CEST	8.8.8.8	192.168.2.4	0xf5a9	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:24.959245920 CEST	8.8.8.8	192.168.2.4	0x8332	No error (0)	passwordreset.microsoftonline.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:24.959245920 CEST	8.8.8.8	192.168.2.4	0x8332	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:24.959245920 CEST	8.8.8.8	192.168.2.4	0x8332	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:25.123492956 CEST	8.8.8.8	192.168.2.4	0xea79	No error (0)	scu.client.hip.live.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:25.123492956 CEST	8.8.8.8	192.168.2.4	0xea79	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:25.123492956 CEST	8.8.8.8	192.168.2.4	0xea79	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:33.915946007 CEST	8.8.8.8	192.168.2.4	0xdf16	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:41.580223083 CEST	8.8.8.8	192.168.2.4	0x704b	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:55.037874937 CEST	8.8.8.8	192.168.2.4	0x1417	No error (0)	account.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:55.037874937 CEST	8.8.8.8	192.168.2.4	0x1417	No error (0)	account.msa.msidentity.com	account.msa.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:55.542870998 CEST	8.8.8.8	192.168.2.4	0xb323	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:55.542870998 CEST	8.8.8.8	192.168.2.4	0xb323	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:55.542870998 CEST	8.8.8.8	192.168.2.4	0xb323	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:55.612926960 CEST	8.8.8.8	192.168.2.4	0x6949	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:55.612926960 CEST	8.8.8.8	192.168.2.4	0x6949	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 19:42:55.625595093 CEST	8.8.8.8	192.168.2.4	0xcf4a	No error (0)	acctcdn.msftauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:55.625595093 CEST	8.8.8.8	192.168.2.4	0xcf4a	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:55.625595093 CEST	8.8.8.8	192.168.2.4	0xcf4a	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Jun 11, 2021 19:42:57.115179062 CEST	8.8.8.8	192.168.2.4	0xf9a7	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:57.115179062 CEST	8.8.8.8	192.168.2.4	0xf9a7	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:42:57.115179062 CEST	8.8.8.8	192.168.2.4	0xf9a7	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.leo.lopez.sakshamsevango.org.in

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49736	216.10.243.103	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 19:42:08.445276976 CEST	1127	OUT	GET /br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y= HTTP/1.1 Host: www.leo.lopez.sakshamsevango.org.in Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Jun 11, 2021 19:42:09.495276928 CEST	1325	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 11 Jun 2021 17:42:07 GMT Server: Apache Location: http://www.leo.lopez.sakshamsevango.org.in/br/?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y= Content-Length: 287 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 65 6f 2e 6c 6f 70 65 7a 2e 73 61 6b 73 68 61 6d 73 65 76 61 6e 67 6f 2e 6f 72 67 2e 69 6e 2f 62 72 2f 3f 62 47 56 76 4c 6d 78 76 63 47 56 36 51 48 52 6c 59 53 35 30 5a 58 68 68 63 79 35 6e 62 33 59 3d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>
Jun 11, 2021 19:42:09.504017115 CEST	1326	OUT	GET /br/?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y= HTTP/1.1 Host: www.leo.lopez.sakshamsevango.org.in Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 19:42:09.950078964 CEST	1400	IN	HTTP/1.1 200 OK Date: Fri, 11 Jun 2021 17:42:08 GMT Server: Apache Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 61 33 0d 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 61 75 73 74 72 61 6c 69 61 62 6f 6e 64 63 6c 65 61 6e 69 6e 67 2e 63 6f 6d 2e 61 75 2f 2e 77 65 6c 6c 2d 6b 6e 6f 77 6e 2f 3f 73 73 3d 32 26 65 6d 61 69 6c 3d 62 47 56 76 4c 6d 78 76 63 47 56 36 51 48 52 6c 59 53 35 30 5a 58 68 68 63 79 35 6e 62 33 59 3d 22 3c 2f 73 63 72 69 70 74 3e 0a 0d 0a Data Ascii: a3<script type="text/javascript">window.location.href = "https://www.australiabondcleaning.com.au/.well-known/?ss=2&email=bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y="</script>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 19:42:57.202898979 CEST	152.199.21.175	443	192.168.2.4	49921	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jun 06 01:52:36 CEST 2021 Wed Jul 29 14:30:00 CEST 2020	Wed Jun 01 01:52:36 CEST 2022 Fri Jun 28 01:59:59 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		
Jun 11, 2021 19:42:57.202969074 CEST	152.199.21.175	443	192.168.2.4	49922	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jun 06 01:52:36 CEST 2021 Wed Jul 29 14:30:00 CEST 2020	Wed Jun 01 01:52:36 CEST 2022 Fri Jun 28 01:59:59 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		
Jun 11, 2021 19:42:57.385543108 CEST	152.199.21.175	443	192.168.2.4	49924	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jun 06 01:52:36 CEST 2021 Wed Jul 29 14:30:00 CEST 2020	Wed Jun 01 01:52:36 CEST 2022 Fri Jun 28 01:59:59 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Microsoft Azure TLS Issuing CA 06, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 29 14:30:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6468 Parent PID: 2460

General

Start time:	19:42:00
Start date:	11/06/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://list-manage.agle1.cc/click?u=http://www.leo.lopez.sakshamsevango.org.in/br?bGVvLmxvcGV6QHRlYS50ZXhhcy5nb3Y='
Imagebase:	0x7ff609c80000
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

Key Value Modified

Analysis Process: chrome.exe PID: 6712 Parent PID: 6468

General

Start time:	19:42:03
Start date:	11/06/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1624,4652876236295108038,17951007052133139354,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8
Imagebase:	0x7ff609c80000
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