



ID: 383792
Cookbook: browseurl.jbs
Time: 10:07:27
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report https://sunmatrixsolar.com/TO/tomboard@paragon-cc.co.uk
Overview 44
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 9
Private 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 41
No static file info 41
Network Behavior 41
Network Port Distribution 41
TCP Packets 41
UDP Packets 43
DNS Queries 44
DNS Answers 44
HTTPS Packets 44
Code Manipulations 45
Statistics 45
Behavior 45
System Behavior 45
Analysis Process: chrome.exe PID: 2336 Parent PID: 968 45
General 45

Copyright Joe Security LLC 2021

File Activities 46
Registry Activities 46
Analysis Process: chrome.exe PID: 6020 Parent PID: 2336 46
General 46
File Activities 46
Registry Activities 46
Disassembly 46

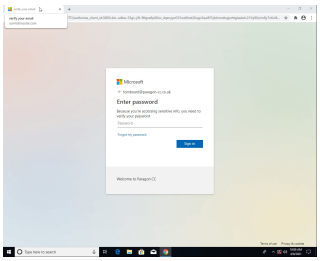
Analysis Report https://sunmatrixsolar.com/TO/tomboar…

Overview

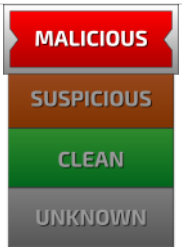
General Information

Sample URL:	http://https://sunmatrixsolar.com/TO/tomboard@paragon-cc.co.uk
Analysis ID:	383792
Infos:	

Most interesting Screenshot:



Detection



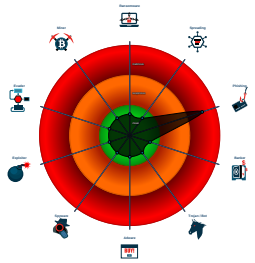
HTMLPhisher

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 2336 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://sunmatrixsolar.com/TO/tomboard@paragon-cc.co.uk' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6020 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,16681490481336671047,18098486573724332923,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1704 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

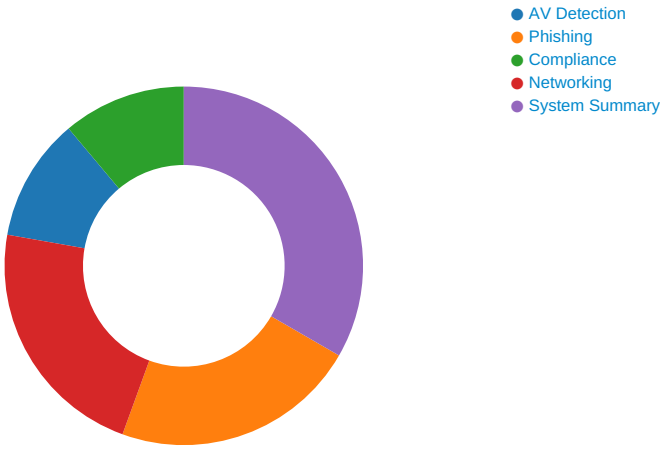
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:



Phishing site detected (based on favicon image match)

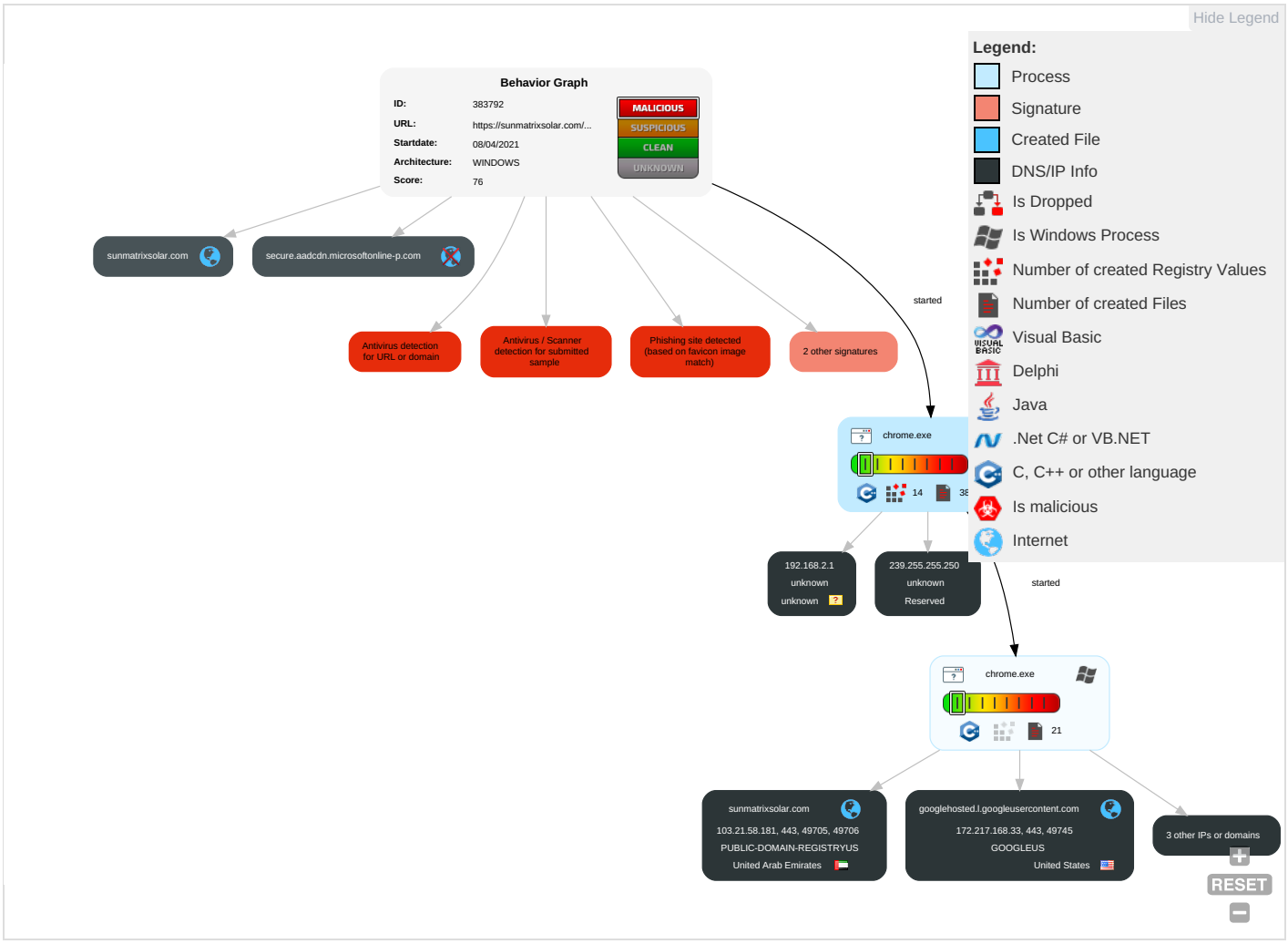
Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

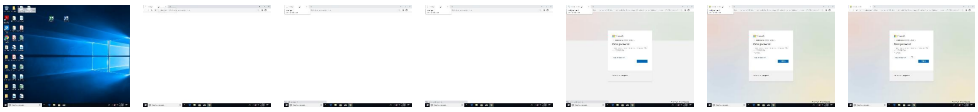
Behavior Graph

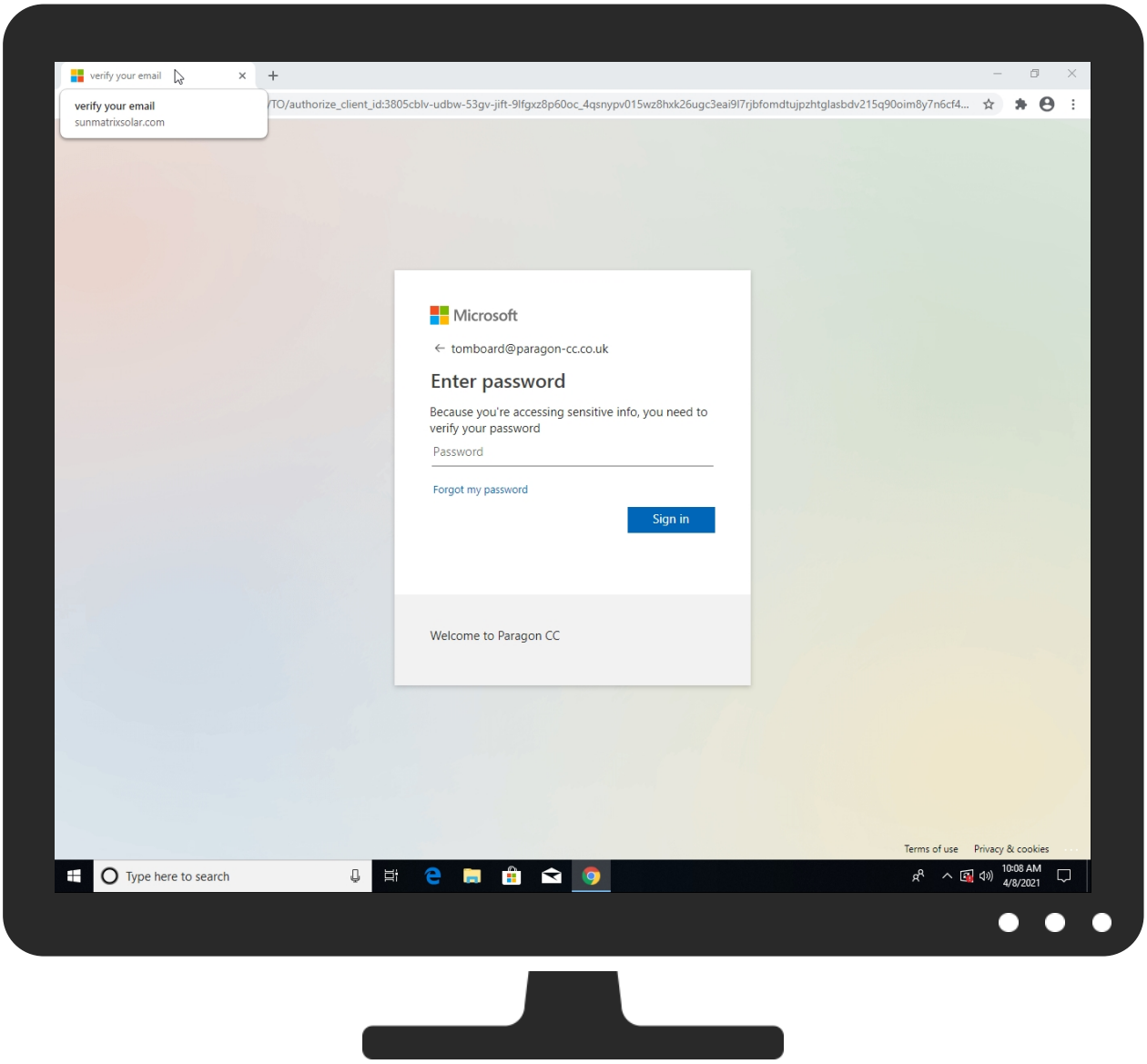


Screenshots

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://sunmatrixsolar.com/TO/tomboard@paragon-cc.co.uk	0%	Avira URL Cloud	safe	
http://https://sunmatrixsolar.com/TO/tomboard@paragon-cc.co.uk	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://sunmatrixsolar.com/TO/tomboard@paragon-cc.co.uk	100%	UrlScan	phishing brand: microsoft	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sunmatrixsolar.com	0%	Virustotal		Browse
secure.aadcdn.microsoftonline-p.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://sunmatrixsolar.com/TO/authorize_client_id:3805cblv-udbw-53gv-jift-9lfgxz8p60oc_4qsnypv015wz8hxk26ugc3eai9l7rjbfomdtujpzhtglasbdv215q90oim8y7n6cf4ewk3xr540rjq2gabtn1y8is3kv9oduwhxpemcfl67z?data=dG9tYm9hcmRAcGFyYWdvbi1jYy5jby51aw==	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
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://dns.google	0%	URL Reputation	safe	
http://https://sunmatrixsolar.com/TO/tomboard	0%	Avira URL Cloud	safe	
http://https://sunmatrixsolar.com/TO/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://sunmatrixsolar.com/TO/authorize_client_id:3805cblv-udbw-53gv-jift-9lfgxz8p60oc_4qsnypv015wz8	0%	Avira URL Cloud	safe	

Domains and IPs

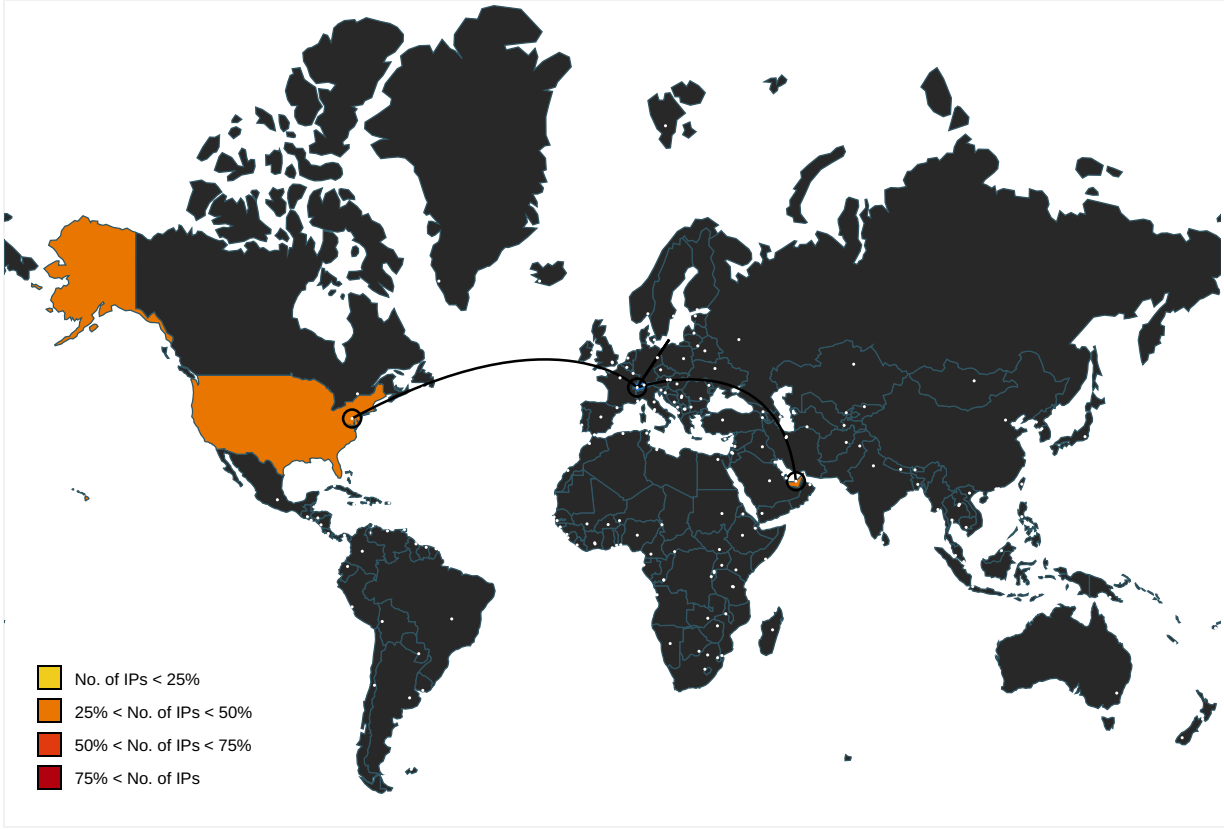
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sunmatrixsolar.com	103.21.58.181	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dns.google	b72bc0c5-c02c-495a-a99a-fa202cbaeab4.tmp.1.dr, bbaf7a03-81b8-4350-81af-5993d03a5972.tmp.1.dr, a0220e3f-3006-4336-9d7e-ad7540a095e2.tmp.1.dr, 84375109-a45c-4963-b994-df044772f908.tmp.1.dr, 8f121532-b5d0-4a2d-9c6e-dc5c7e486a4c.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients2.googleusercontent.com	bbaf7a03-81b8-4350-81af-5993d03a5972.tmp.1.dr, 8f121532-b5d0-4a2d-9c6e-dc5c7e486a4c.tmp.1.dr	false		high
http://https://sunmatrixsolar.com/TO/tomboard	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://sunmatrixsolar.com/TO/images/favicon.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sunmatrixsolar.com/TO/authorize_client_id:3805cblv-udbw-53gv-jift-9lfgxz8p60oc_4qsnypv015wz8	History.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.21.58.181	sunmatrixsolar.com	United Arab Emirates		394695	PUBLIC-DOMAIN-REGISTRYUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383792
Start date:	08.04.2021
Start time:	10:07:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://sunmatrixsolar.com/TO/tomboard@paragon-cc.co.uk
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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Copyright Joe Security LLC 2021

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.phis.win@27/164@5/5
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 23.54.113.53, 104.43.193.48, 172.217.168.78, 216.58.215.238, 172.217.168.13, 173.194.160.74, 142.250.34.2, 52.147.198.201, 172.217.168.35, 104.83.121.18, 172.217.168.42, 172.217.168.74, 216.58.215.234, 172.217.168.10, 95.100.54.203, 20.50.102.62, 13.88.21.125, 23.0.174.200, 23.0.174.185, 104.43.139.144, 23.10.249.43, 23.10.249.26 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, r5.sn-1gi7znes.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, clients2.google.com, redirector.gvt1.com, audownload.windowsupdate.nsatc.net, e13761.dscg.akamaiedge.net, arc.trafficmanager.net, edgedl.gvt1.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, accounts.google.com, secure.aadcdn.microsoftonline-p.com.edgekey.net, r5---sn-1gi7znes.gvt1.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, www.googleapis.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\3acb944c-6bdd-4422-8459-b75663f461f3.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):	164171
Entropy (8bit):	6.08207806331793
Encrypted:	false
SSDEEP:	3072:LV0ZM4iTMFp3l+7LSx8sogeEFcbXafIB0u1GOJmA3iuRM:xEgMTo7Jsog1aqfIlUOoSiuRM
MD5:	0FFBEE2059B5A2BB36641A3989CCBF6A
SHA1:	FB93D2392920E69484B88D28E489DB4540A0B62F
SHA-256:	5A3CF96FE2E0AEB51ABE62800DD0F3908D0829B7E63C51C7A46E6C6EF197EFF6
SHA-512:	6344A2589B820907CBD9F688EDFBB5D17CF8DBBED4557F8688C71752D5F0736715194AB03819AD90652094D6CA33AA170710D12A8A35198C036D4D56FBB42DC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\3acb944c-6bdd-4422-8459-b75663f461f3.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.617901701706121e+12,"network":1.617869303e+12,"ticks":100689872.0,"uncertainty":4306838.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6c17c36e-bd98-4485-8af4-cae0428b6e6a.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):	164171
Entropy (8bit):	6.082077716326327
Encrypted:	false
SSDEEP:	3072:LwVZM4iTMFp3l+7LSx8sogeEFcbXafIB0u1GOJmA3iuRM:8LgMTo7Jsog1aqfIlUOoSiuRM
MD5:	E412C409830BF22DF629C524518257F9
SHA1:	A5BF98F86D5733221E4B6CDBD2E5DD607DFA994B
SHA-256:	08A847C3A79080BECA1E23307BCE05A7243E5FF146990787AB93379289040FD2
SHA-512:	D7B17C920DA1400EC2869A89EAD2CFF731ABDE47C9EA328246CDFFE3AD018F9BC58F2E36303237C27DBBA8F59DEFEBF4389234B368DBA5CAD511E1D6A528EA08
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.617901701706121e+12,"network":1.617869303e+12,"ticks":100689872.0,"uncertainty":4306838.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4fefed59-c375-492c-9109-0f8daeb269f4.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\833be432-1719-48de-b7e4-81befd1225be.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\833be432-1719-48de-b7e4-81befd1225be.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1207
Entropy (8bit):	5.572740555826838
Encrypted:	false
SSDEEP:	24:YI6H0UhVsTG1KUerkq/HeUeXby2qUeXv37wU1pwUd9RUenHQ:YI6UUhVseKUewqPeUer2UefrwU1pwU52
MD5:	338C6168608496232BC9FD242842D880
SHA1:	DD335FD74344F780C2547059818EE5960084AB6F
SHA-256:	330B9D87F3BDD6FEAC06F61A97E68460C428D45A6C5F456876D2B6FE6C0B5D42
SHA-512:	D9C8F292DFACF8C87243C2A1290A989782A3138DBEAE68D7D3894A8124AB4ECF83113D8556952CE7C13F61075D7C1DF1C81CACA577B16FF2ADE34B94BA2947 1
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1649437701.758601,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1617901701.758605},{"expiry":1649437704.132169,"host":"+LCYPikJxOjeTMeNwsPDpkFmxWXugWYr8RjEVTinl5c=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8f121532-b5d0-4a2d-9c6e-dc5c7e486a4c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.17359938973192
Encrypted:	false
SSDEEP:	6:m1xuv4q2PWXp+N23iKKdK9RXXTZIFUtpkx0vJZmwPkxmzDkwOWXp+N23iKKdK9Rn:oY4va5Kk7XT2FUtpY+J/PYOD5f5Kk7XH
MD5:	C8CE9EA6E651803D733A3F6F416EA2AC
SHA1:	2A1904498ED069BD8D1766743E15F141373311DF
SHA-256:	2F25FF3E1104EF2987F6AB4AF05AEC44AC60C6942451554E451841624D026755
SHA-512:	49CA7DD5F0DDB49EC91204D5BF751D51F6BC538D1A13C60F79355751B29BA109CBA675349197FE1A6357297669D09FACA7D78ED48E51D87865341EB1524A438
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:40.413 1660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/04/08-10:08:40.419 1660 Recovering log #3.2021/04/08-10:08:40.420 1660 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):	5.161560956606264

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Encrypted:	false
SSDEEP:	6:m1xrv4q2PWXp+N23iKKdKyDZIFUtpkxiiJZmwPkxiUu3DkwOWXp+N23iKKdKyJLJ:orv4va5Kk02FUtpYnJ/PY3u3D5f5KkWJ
MD5:	678772A9EBF006143388500493EA2DA1
SHA1:	026102E2CC8BE555CE8724A4C89823DED1FE7BBA
SHA-256:	334DF69D6E778D814C26CFB5792A71F2C2B5EA118B2168F96F85FA5351F88768
SHA-512:	6473819F293AA6991C22A1C61738B9662B9A6A9231482F2CF650388044BD815649474457041B304F9982301E583C9D623710E5BD870AC7EE265A1277627B2310
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:40.351 1660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/04/08-10:08:40.360 1660 Recovering log #3.2021/04/08-10:08:40.361 1660 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\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	12288
Entropy (8bit):	0.8448440721711986
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwaezExIl6pgV:TLyqJLbXaFpEO5bNmISHn06Uw9zEal6i
MD5:	A54490C1E90FD002C8C065E536752D21
SHA1:	BB0BC539CFD057ED7ED9137A49C180F72B7F0643
SHA-256:	F6404E87BB1A26AF34BA42E4BBFFAC2B4326A05BD3DE333F753089D564A4A367
SHA-512:	534B0FFF9FD6F9F9AFC4EDA11828841531E965ACA8A63F2AFF3D77DCD0FED7A1D2776F94DE422194D35A1A1EA343836C3CCBD1737E315961A86B439F6D10E7B
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:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9673929407226849
Encrypted:	false
SSDEEP:	24:1cLgAZOZD/BqLbJLbXaFpEO5bNmISHn06UwZ8:18NOZBq5LLOpEO5J/Kn7UG8
MD5:	1D65A5FF058E3CEA6762FFCB03040AF7
SHA1:	E8E1F4E3D604DBC31FE7D5DD09379789C77954B2
SHA-256:	431A9FA34AC805F52ADFCF00148D6FFCE5BC7F260034DE44BE00614F35C9DEC6
SHA-512:	6E3CA24756A845BE953AB8CBA08722B36F2C6D197B334F780A11FB7EAA8B64D5D36787BDD5126C24CC0D5F0F624DB4872013D87A150B239467FC0A18ABEBB12
Malicious:	false
Reputation:	low
Preview:	.....vn.~..... ....

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):	1597
Entropy (8bit):	4.09375361230366
Encrypted:	false
SSDEEP:	24:34SXhlrlA5l4sPGgUIHkQUOq7qvHb32nVQnocFGInmqyicosnlL:34OzxiDPGgUYq7qvHT2nVqocDmp4slL
MD5:	31DEE4C674D12FE60F08E732392450F0
SHA1:	5119CA595CB19A3E4FF34BD9A8012D5DA5F633F8
SHA-256:	CA5501B16C49A7437519A8C76DA20B6342F7A81F7C67E632875397CA58FF5F44
SHA-512:	B4957A7AF5190F72B9FE2E0D4D287D31C7FC11D478359D1DAD9D3898F0D210610DAC7B513DFAC6102968DE433321714727361032E9AB94922CA90E297AD64F15
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...97e937cd_219e_4186_8dee_17ded5908994.....a_..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....https://sunmatrixsolar.com/TO/authorize_client_id :3805cblv-udbw-53gv-jift-9lfgxz8p60oc_4qsnypv015wz8hxk26ugc3eai9l7rjbfomdtujpzhtglasbdv215q90oim8y7n6cf4ewk3xr540rjq2gabtn1y8is3kv9oduwhxpemcfl67z?dat a=dG9tYm9hcmRAcGFyYWdvbi1jYy5jby51aw==.....,...(..... .....h.....`.....H.....P.....H.....L.X.y...M.X.y..... .....h.t.t.p.s.:.//.s.u.n.m.a.t.r.i.x.s.o.l.a.r...c.o.m./.T.O./.a.u.t.h.o.r.i.z.e._.c.l.i.e.n.t._.i.d.:.3.8.0.5.c.b.l.v.-.u.d.b.w.-.5.3.g.v.-.j.i.f.t.-.9.l.f.g.x.z.8.p.6.0.o.c._.4.q.s.n.y.p.v.0 .1.5.w.z.8.h.x.k.2.6

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:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
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):	5.192474566491836
Encrypted:	false
SSDEEP:	6:m1xWiNjyq2PWXp+N23iKKdK8aPrqIFUtpkxWi7z1ZmwPkxWidZERkwOWXp+N23if:o1Ova5KkL3FUtpYzz1/PYlm5f5KkQJ
MD5:	367D1EF9885346BAB6C953089E127E3F
SHA1:	123ABCA44B349370DB3DB54382A3C4AB5A497BF9
SHA-256:	F00BE73C684A5363F054A25584C9698A9B568869A1C5DFFE23E0314AC26A6C6A
SHA-512:	F7762302DB915A1AEE6A9151428FC5E92505C55D94276EE413E78291643D8C413F565F886705048DCDE31BF13412FB3740AEFF11CFADACA3C54E36CB2D4B274
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:18.943 1314 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/04/08-1 0:08:18.947 1314 Recovering log #3.2021/04/08-10:08:18.948 1314 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
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.....

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):	5.1550704000949965
Encrypted:	false
SSDEEP:	6:m1x+h0Fyq2PWXp+N23iKKdK8NIFUtpkx+Rjz1ZmwPkx+gpRkwOWXp+N23iKKdK8n:ogva5KkpFUtpYI/1/PY5P5f5KkqJ
MD5:	28D03E9FEA4D375EE07EF816D36D8423
SHA1:	F72ED4B6BE7D95FC9E837890532F6F87A93DE2D7
SHA-256:	98E18C195D5BF1EE0F5B82530AC3122193B69DB26588FBE1D5F460C446FAD4F0
SHA-512:	E094EB770BE64F11DEEFF43C4DA76FCB2F45ECE2D3FF3CF0ADBECCB1B93B68FF671467C65C3567C8A04FCF36AF14FA18F536AA8AF21C7C9C9A76184D3484F EBD
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:21.288 1314 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/04/08-1 0:08:21.290 1314 Recovering log #3.2021/04/08-10:08:21.291 1314 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\comput ed_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):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/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=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclJ5 n0lTpw5JBHV1Kph3/KM=","i3l8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\c omputed_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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
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=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+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):	16384
Entropy (8bit):	1.778935232186087
Encrypted:	false
SSDEEP:	48:yBmw6fUpsWZPGgU5unw1Ok0ETXUBdsxxozsqcPGgUT:yBCQRwsnETkvuoJt
MD5:	9D1237DACC368A60718FE4D6A37AED68
SHA1:	E012F57ED02FF653C9B18F82638D1F89951F600E
SHA-256:	0C95BF7485D685C802A5721118DDF8D95FD0501A4295099C155C2A99EDBF9510
SHA-512:	D282ABED7273F11276F442CE2B4495DAF03E821D7A25B41E1F7D83C22F1A07695052C5B3D0B098DD2686A5B5DC5EE09FEAF42628A6850CCBAE8408BFF24BFD6
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
Size (bytes):	16972
Entropy (8bit):	0.7718966494688779
Encrypted:	false
SSDEEP:	24:71MbAbuRpymmyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uwsz3n:71MbAbuRpymmdBmw6fUxz3n
MD5:	65C5814281B7EF645AA7E97F3B394BB3
SHA1:	5591397AA834D8A5623280B931292ED7ADA7360F
SHA-256:	2468D161C0839C14839D5D2AA4CB5CE20EC2B070464D1EB86F3730294C073A01
SHA-512:	69054EA18F1FCFF38CA5C62283EFFDC1827815AE618E8D78F840B4BF8EDACDFF2E945DF8FFFF99DB4DB1E36FE9C0919D195F3BA9534FED0B85F362C0CE69542D
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	5.244179399859486
Encrypted:	false
SSDEEP:	6:m1x94q2PWXp+N23iKKdK25+Xqx8chI+IFUtpkxqvJZmwPkxMUDkwOWXp+N23iKKN:o94va5KkTXfchI3FUtpYsJ/PYMUD5f5G
MD5:	DB7A9F9C744844050C78768CD4DEE527
SHA1:	543CDA783F558CF6DF0E40DB72EB78CA68E1336B
SHA-256:	E8B2BD045D387153A567DFED40C37A9C7C2C49313C1DCBB09FFD520004D3FF2F
SHA-512:	BC88ECE16DCCE13FFCB5ACC2863D00BB26A6286CFEBC26E3DC007201C0B21AAF566CB714AE555B19C4ADDC05CC52BEA5FC2085564BC2BEA8ECDCF23484E05790
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:40.289 1660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/04/08-10:08:40.295 1660 Recovering log #3.2021/04/08-10:08:40.296 1660 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):	5.17617119737768
Encrypted:	false
SSDEEP:	6:m1xITz4q2PWXp+N23iKKdK25+XuoIFUtpkxmNJZmwPkxiaDkwOWXp+N23iKKdK28:o24va5KkTXYFUtpYmNJ/PYnD5f5KkTXp
MD5:	95DA9F42F6D2FD64085BBAF59F52D7BC
SHA1:	F036B2705162E2E57DF9882258E96A9FA724527D
SHA-256:	74595B8787D7C94F062CA81A2FDF97F828A62661D0AD4A90DCFB05B4D3C3A823
SHA-512:	3AEFAF04811C0F81035DB6463F20DB5E2CDEBBA4E98630A7A9BCE1FEEB260D2BA9B38BA13067CFE73AE9B136F1CA447E29AC2080EDA5A304077A5A1290B39CAB
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:40.262 1660 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/04/08-10:08:40.264 1660 Recovering log #3.2021/04/08-10:08:40.265 1660 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):	5.263526698410939
Encrypted:	false
SSDEEP:	6:m1xUCFg+q2PWXp+N23iKKdKWT5g1IdqIFUtpkxU0WZmwPkxUDiVkwOWXp+N23iKN:oUGg+va5Kkg5gSRFUtpYU0W/PYUDiV5b
MD5:	8DD4CD37B3EF93BA691F826F7DB822C4
SHA1:	042744D9A340991C5B4AF98D8B3CB6CF79294E4A
SHA-256:	73F51973375E4A0681F094A30018C8BBDAC14D1DC851E667B8905ABE88FD6ACF
SHA-512:	ED15DA71CEAB3BC2B6AD19F43CF7C1E0C05C8D51F24CF2CF3A9656B28CE8A68137498159B89F9406B8F80D4AD905EEF41172BE0A92C21E88DED80F7E69C638A9
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:39.668 163c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/04/08-10:08:39.712 163c Recovering log #3.2021/04/08-10:08:39.720 163c 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.33214985212788906
Encrypted:	false
SSDEEP:	24:TLxdsa+PGgUIHkQUbwRI27rOAkYPGgUIHkQUhcTsO:Tbsa+PGgUh52POAkYPGgUUsO
MD5:	1E079A5EDC93BC6046A1DAF8B4B02CB5
SHA1:	74BB8C40FBC50E3244B5A588D63DD2B0A7A7DA5F
SHA-256:	B17E9A8CB628B8E065977C52AB44A22D259B3FB482372FF8702706F7414AB86C
SHA-512:	359A461BD1C83A6D7C93D97BE39F528AE5F61AB25899CF620BA05A0C4782732FAF82A763CD59438869FFF7647889C14DA0CAC3882763AD10E4273856D74D36BI
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):	1852
Entropy (8bit):	5.934485440937492
Encrypted:	false
SSDEEP:	48:/4WsUPT1U+PNY9RLwaSb0qBWt32irSB3nMsZbGPGgU2BBkn:/4WnS8BwaWt32BB3hbakn
MD5:	C3D393684500E42E54CBA64C43D4DA73
SHA1:	E69F841FCBA3CCA9911F94B1589AD35CBEEF33E0
SHA-256:	0F927223B6A3A446A4B6554B7916B13BF388A006C9703D8B0005728206B1622C
SHA-512:	F640C93577731744A3D825582FB0F8A78A6D4747410E409A2320CAB89A752F8EE207D366813B10F0E20FA9E67D654360CED011FCF0854921636576FCDCCE3249
Malicious:	false
Reputation:	low
Preview:	....."......cc..co..com..email..https..paragon..sunmatrixsolar..to..tomboard..uk..verify..your..3805cblv.l4qsnypv015wz8hxk26ugc3eai9l7rjbfomdtujpzhtglasbdv215q90oi m8y7n6cf4ewk3xr540rjq2gabtn1y8is3kv9oduwhxpemcfl67z..53gv..9lfgxz8p60oc..authorize..client..data."dg9tym9hcmracgfyywdvbi1jyy5jby51aw..id..jift..udbw*.....380 5cblv...p.l4qsnypv015wz8hxk26ugc3eai9l7rjbfomdtujpzhtglasbdv215q90oim8y7n6cf4ewk3xr540rjq2gabtn1y8is3kv9oduwhxpemcfl67z.....53gv.....9lfgxz8p60oc.....authori ze.....cc.....client.....co.....com.....data...&."dg9tym9hcmracgfyywdvbi1jyy5jby51aw.....email.....https.....id.....jift.....paragon.....sunmatrixsolar.....to.....tomboard..... udbw.....uk.....verify.....your..2...$.....0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....a.....b.....c.....d.....e.....f.....g..... .....h.....i.....j.....k.....l.....m.....

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):	33356
Entropy (8bit):	0.04761656801783399
Encrypted:	false
SSDEEP:	6:Ebe9lbElMbJ0b8bQXebObuObxg9bNFlWCj/lf+/l3n:EbMlbElMbab8bQXebObpbxqLBj/p+t3n
MD5:	21FEEED5A556CD91B5331859BF16A51C
SHA1:	06ADE26E801F7BDAC07A58B0DE6D613AB6D2F073
SHA-256:	AE082745DF94D5477CC2A5254A559CBE290AD6A4C4D7E67D86216D4D7C0D2D63
SHA-512:	EA2CE30B8C1385A672101AA8B46C7A5B37D7F8D8D397E98C611806ED74A8CE63CDD143C4B626290A5BA5EF13DB9E4183EFDE1C877797C08B8221AB712F8EFC 84
Malicious:	false
Reputation:	low
Preview:	.....>"..... ....

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:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.451029301322899
Encrypted:	false
SSDEEP:	48:XWG2cha7fMm8db1jzmbQSefgGwNrS0U9RdiN9F:1a7fM9db1jzmbQ5fgG4rS03

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
MD5:	F3F64F7472F88C8198C7318489D36E10
SHA1:	5F9ED8B173E14D2B00235E19653C6BE204FEF81B
SHA-256:	C3052676C2C0069281F3F15DADA9277DE3441373E730A9045DFDF1C664E82DE4
SHA-512:	F3DDE7F38EEFCCB9442BADCB53A8DF4EF930ECD3148EF991130B23BEC855D2FB20266D2647CD12B47C918888B01026E005181C0BDEA5E635435EDF90E6D568A
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..604457000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-04-08 10:08:41.72][INFO][mr.Init] MR instance ID: 9ed8edd2-2ff1-4fdc-b657-3f7dcd1dcee7\n","[2021-04-08 10:08:41.72][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-04-08 10:08:41.72][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-04-08 10:08:41.72][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-04-08 10:08:41.72][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-04-08 10:08:41.72][INFO][mr.CastProvider] Query enabled: true\n","[2021-04-08 10:08:41.72][INFO][mr.CloudProvider]

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):	5.179338405737704
Encrypted:	false
SSDEEP:	6:m1xWdQwlyq2PWXp+N23iKKdK8a2jMGIFUtpkxWdRz1ZmwPkxWdZURjRkwOWXp+Nt:oEIva5Kk8EFUtpYW1/PY6UP5f5Kk8bJ
MD5:	E5DBB118C49DBCC3FC884789A3D18E4B
SHA1:	0746ECA300A515AC8A68FFC06D9E1B055FB9A968
SHA-256:	FE6E249D51C3065E63277AC4B3933CC5836CD916E7BCA18655717D545605A7DF
SHA-512:	71F2100D9154BC8C5A0117B6A359D0059F3F2B82C50136D04681805A7111A27B0E092B8E2F2AEE23E5033F6821D5E45157087DEAFB60864D8909AEE3B71C1EF1
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:18.687 1314 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/04/08-10:08:18.690 1314 Recovering log #3.2021/04/08-10:08:18.693 1314 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.213122641830331
Encrypted:	false
SSDEEP:	6:m1xWlDjM+q2PWXp+N23iKKdKgXz4rRIFUtpkxWVZmwPkxWwMVkwOWXp+N23iKKdA:oWjM+va5KkgXiuFUtpYu/PYRMV5f5Kkt
MD5:	C837CE138943C10E18D2BFBAA408E780
SHA1:	5331E9F1AE6E2C4E6D89EB99A5025F45EA0AEFED
SHA-256:	8061E3450D8073FA981A580CCFFEF5AD83500C656C80FB16B5416E434E346744
SHA-512:	356D5D466DD4E4A892132E93D32F09E412B445030051DAB82F2959F3C6A176F81C273E30A506EF86725FBC25B0D62A27CF1C737004FA3CFBD5B63E9654CA2BC
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:18.974 f8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/04/08-10:08:18.977 f8c Recovering log #3.2021/04/08-10:08:18.977 f8c 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\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

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):	5.14610193669978
Encrypted:	false
SSDEEP:	6:m1xWT3lN+q2PWXp+N23iKKdKrQMxIFUtpkxWToaFZZmwPkxWTEVkwOWXp+N23iKN:o4VIva5KkCFUtpY4rZ/PY4E5f5KktJ
MD5:	C4A6425DBC863D5F0FFE90F24459C28F
SHA1:	1A69D3985A1275318F0AFAAE6CDC4B525095DBE1
SHA-256:	B2A62021F91A0D46D64D76AE74576D82D3FA29FE805CEE2B16C5FFD063129B0D
SHA-512:	076EACF3E737B293EB22C0C08AE722679FBB487AD395FC936CA204CFCB890C285A229B94D8C99FD22224290CCCF75704E74543C8489025B60BCFDC3037EFFA 1
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:18.845 1738 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/04/08-1 0:08:18.847 1738 Recovering log #3.2021/04/08-10:08:18.848 1738 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
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.18048818955955
Encrypted:	false
SSDEEP:	6:m1xWTq2PWXp+N23iKKdK7Uh2ghZIFUtpkxWRR9ZmwPkxWiTkwOWXp+N23iKKdK7w:oMva5KklhHh2FUtpYoR9/PYZ5f5KkIh9
MD5:	0B0FCC6B58DD265E4B423E49FCE6B1FA
SHA1:	D2094D7D1806D4DF5B3C5291FE76BAC3440E7FE3
SHA-256:	622046EDFB231B2E1FF17876122A6B30C1D0D3C2E089425A8F8D5E9841E0A3C6
SHA-512:	B8CA84329B48007F4FAA69AE8CABC1831193BE94804688FBE93F29D4019161391E0AB78308744B6E28FAD8A063BB6E3627ADB7C9105E1A7604BAE64F0051F69D
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:18.555 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/04/08-10:08:18.556 864 Recovering log #3.2021/04/08-10:08:18.557 864 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Char acteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\84375109-a45c-4963-b994-df044772f908.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):	420
Entropy (8bit):	4.986775197192121
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Kn:YHO8sdBsB6MAsBdLJlyH7E4f3K3X
MD5:	0D1F7A36AD610D2F08709B1EF88F1B09
SHA1:	237E8E7BC7891D987DEA1D2EB1DA9DA511396D11
SHA-256:	5C36B7E531EE8DF00FE937FDE21AF4D1B6606EAD4B5F98D56396DDCEF1C4249A
SHA-512:	37DAD8F9F2008D7B287A03964F0AE41FA4EBED92987B3872E022758857131971BC486638D0339774E80DF01A669B68DB4729D48E49EC5DE714F27ADF20B247AC
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
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\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):	5.235886317923056
Encrypted:	false
SSDEEP:	6:m1xWmdw+q2PWXp+N23iKKdKusNpV/2jMGIFUtpkxWv6ZZmwPkxWv6NVkwOWXp+Nh:op1va5KkFFUtpYP/PYd5f5KkOJ
MD5:	B9DB04EFB61C5B161A6535055281E413
SHA1:	0943025EA02AE0256B0110BD8721DCE1DABC0B42
SHA-256:	472039294D53038E24C554D395CEC464168A81D06D84A6A7178DBEFDAB3F6659
SHA-512:	E292A880CC858A4528A7120983DD99FAF4488DD5EF379E1D94A0FB23815C47715E8B839A7771FEF842A82191DB169DF0525F20B63074D69926DAA7A709D75DAC
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:18.908 1738 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Local Storage\leveldb/MANIFEST-000001.2021/04/08-10:08:18.910 1738 Recovering log #3.2021/04/08-10:08:18.910 1738 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):	5.282649137876078
Encrypted:	false
SSDEEP:	6:m1xWgdyyq2PWXp+N23iKKdKusNpqz4rRIFUtpkxWZwz1ZmwPkxWpjRkwOWXp+N23:oNBva5KkmiuFUtpYh1/PY4F5f5Kkm2J
MD5:	CF2DDCDF4169CE458A52C565C79AF18C
SHA1:	B6384566146869013661 9A7BC9CCC6C3DE6C0EDD
SHA-256:	E5E47834F8F01D81AEB7CDA30C47A21CA76627D195FDC411B90653E0FC55ED71
SHA-512:	630AEB9499EA0B9C0B7ADEFB4F6CF47ED74E140A4C638605C97799D09D66197DB160A477C887E9BBB86F734730CE73C750DC4B617AB18C077B2E7D0AF2DB61 B8
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:18.968 1314 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl \def\Platform Notifications/MANIFEST-000001.2021/04/08-10:08:18.970 1314 Recovering log #3.2021/04/08-10:08:18.971 1314 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):	415
Entropy (8bit):	5.275733723148281
Encrypted:	false
SSDEEP:	12:oUr6+va5KkMFUtpYUgX/PYUp3V5f5KkTJ:oAa5KkUgWJ42f5Kkl
MD5:	390462E6F89A44FF033992C98A15AAA0
SHA1:	E8EE1411C94C88B7D160C8FFA7A5FC4B13C30618
SHA-256:	75886F8BBB1E6BFD6768A3C4115E94BC6FF576BCD03E1B75FCD171421BF14B37
SHA-512:	E033C70B0BBC4F12318FAF99D3D798697F029AFEF8A32B3EAE7AD75087740C5D5BCD51EAA7E2ED752E6389A769E598734945FD1EDA3285F18F67CF2CCFB90B1
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:35.724 fdc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/04/08-10:08:35.726 fdc Recovering log #3.2021/04/08-10:08:35.727 fdc 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\gfdkimpbcpahaombhbimeihdjnejgicl\def\a0220e3f-3006-4336-9d7e-ad7540a095e2.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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","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\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):	427
Entropy (8bit):	5.193938918876533
Encrypted:	false
SSDEEP:	12:oUvNva5KkkGHArBFUtpYU+/PYUa5f5KkkGHAryJ:okRa5KkkGgPgWYLf5KkkGga
MD5:	BFCC62B693CA556F2B53DF6D05ED28CF
SHA1:	828440449F6981B69BC8EF8C1C265BFF585C06C6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
SHA-256:	E87E7A24111ECA7B5614ED411E4810CE1761B479C6E1002DEF75F0A40113D61F
SHA-512:	3B67A874EFAB408CB8921216B1486D77846850BC0118C6CC4F34D51EB347E09E1A3DF17D7D6C890ECC36D1695E6996826CA69E3806D61ECEB6EF2843D27C8C B
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:39.793 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Local Storage\leveldb/MANIFEST-000001.2021/04/08-10:08:39.799 988 Recovering log #3.2021/04/08-10:08:39.801 988 Reusing old log C:\Users\user\AppD ata\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):	5.18643752761188
Encrypted:	false
SSDEEP:	12:oUZva5KkkGHArqiuFUtpYU//PYUAF5f5KkkGHArq2J:oca5KkkGgCgWfzf5KkkGg7
MD5:	96B72F614C2F75DBFBC3645AD47C6CE0
SHA1:	3A7EC7A8648584644480AA7CE04B831341129F6B
SHA-256:	5176D64E7A1F3665C232573522B01AFCF91C20DAD4C5ABC7E5D7A744AAE771C2
SHA-512:	14ABF922C82460374DFDE3773E69B991EC45F1B352A076613E86910C0D84937DB0054330D5B27E836A9FD47EB2D61F77FD453BA34A284C766B1C6B7C18EBE825
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:39.803 1408 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/04/08-10:08:39.811 1408 Recovering log #3.2021/04/08-10:08:39.814 1408 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):	415
Entropy (8bit):	5.180367609641229
Encrypted:	false
SSDEEP:	12:osova5KkkGHArAFUtpY5/PYm5f5KkkGHArfJ:oRa5KkkGgkgWiwf5KkkGgV
MD5:	EF6A04DD51CE227A9A932DDDAA05E2AD
SHA1:	1AC2A0782456437061DCD0EBEBB9D11C67C046C4
SHA-256:	1F2B6961274E23340B54FFAF6A30655C8AD0B88F41B138D4ADDC51876E49AC4B
SHA-512:	3827E076AD49FC4E411E43BA9B146EE04984B12E14B4E6EC44A4EDF36421C0F2E2D5241241A9BCCED3B3040FB67909ED1DD45D1854E4F4448EB373829389DD3
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:55.202 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/04/08-10:08:55.203 988 Recovering log #3.2021/04/08-10:08:55.204 988 Reusing old log C:\Users\user\AppData\Lo cal\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\b72bc0c5-c02c-495a-a99a-fa202cbaeab4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\b72bc0c5-c02c-495a-a99a-fa202cbaeab4.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","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):	321
Entropy (8bit):	5.239405562951163
Encrypted:	false
SSDEEP:	6:m1xWC0q2PWXp+N23iKKdKpIFUtpkxWzZmwPkxWfkwOWXp+N23iKKdKa/WLJ:okva5KkmFUtpYI/PYi5f5KkaUJ
MD5:	6EC0C8D38EAD2E81811A3CC60B562103
SHA1:	0E892B2D00CA772B17C949FA2BF34AC8BC90A119
SHA-256:	281697801F91543D8DA0DA4F3B38DEFF13D5DD1D8E579148589F3EB73D55021E
SHA-512:	EE9D43FC35BF741F6B6951A53D92D1136335CFE262822A8EBE2CE3AB50B5610852B63C3F826440BE800B5EDE94F54FDDA1A30F6A89C820E0BA051C797966C22
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:18.586 864 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/04/08-10:08:18.590 864 Recovering log #3.2021/04/08-10:08:18.592 864 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):	5.316102911231103
Encrypted:	false
SSDEEP:	12:oYcva5KkkOrsFUtpYYX/PYYM5f5KkkOrzJ:oYma5Kk+gWY4YWf5Kkn
MD5:	6A83B845B49F9775CCD715A5228D08E7
SHA1:	B657BB923259A3D5D56EA24CAE087BD6A166E56D
SHA-256:	6843FF0B68E144F95F1E689FEC6BF629E4A908C32D9ED9EF3413DC923BB9C7D0
SHA-512:	4BF4E7513017D0EFCA98DF1FFA4E92B73DC271F4ACDD65441EBB8ED24C3FDACF4C17285965659C259F89552821D7D80B77BF485EE90FE4592D03480FB25E127

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:41.742 16d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/04/08-10:08:41.744 16d0 Recovering log #3.2021/04/08-10:08:41.745 16d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	3.7720552088742014
Encrypted:	false
SSDEEP:	3:J2kbEsYwa:JJosYF
MD5:	9F8AF4FF1C1A88E5FD810D667629A236
SHA1:	23B1DA86D62E99E72C5D36F052195A94ABCABFA8
SHA-256:	7074819D11ACC5F050592A6FC7A61DD622D1C6B30A8D6C2D448A0442D8704DD1
SHA-512:	704C7CCAE1C5C8731580F5E291A299F1ED14EF7F152B1C012313491E9E78CC7AB25B3DEF34EF040662DFF981B34094903C5EED144C7D1448D2A9B0B8A9CE575
Malicious:	false
Reputation:	low
Preview:	....m...(.....vA(.}...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ad14f2ea-0e31-4fe5-a91a-c4f665951272.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):	5.577393327018188
Encrypted:	false
SSDEEP:	384:OkutLLl3DX51kXqKf/pUZNCgVLH2HfDfrU/DXil94w:ULl751kXqKf/pUZNCgVLH2HfjrU/A9n
MD5:	2339A4BF04AC94DC186631B7C4CF72BC
SHA1:	18DE5AEE5C2C068C9038A4A37F9A1DAAD1AF3201
SHA-256:	34DC9623615B98A532D005800223CEAEE16C7C6A0355B14E00F7DA8DE8713FC0
SHA-512:	B236D13EBB31180167D7748D52ACD315939074B35DEB5577A14434D1F05EBFA0CB1AE7973564BF066A4FA671507B92AA5D2916F97C9642DA49446F3E40BFB2AA
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":"13262375298581755","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bbaf7a03-81b8-4350-81af-5993d03a5972.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871755235889535
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMZ:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhS
MD5:	AE133C52F86E27CD225F807F1DDB33A3
SHA1:	A0EB1D7B7D41F31993C975A8B5F27954F90B6DF8
SHA-256:	A795DA84B0B14FD651959C4E712B297CA76E50FAF03E18469336F5FB1BE5420A
SHA-512:	098D9CC2B0436B77AE03D9289C2DBF2316B0F0145C7AEE81F8F19A26964AB7F975F941CD2A9E14783E600602A195ED60A059B0EFEFFCEEC2BD0C5923E09663E3
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\bd017ff7-5bff-43b9-9ed5-374ac8d33435.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.535971662052096
Encrypted:	false
SSDEEP:	384:OkutWLl3DX51kXqKf/pUZNCgVLH2HfDfrU5HG5nTX0ij94h:fLl751kXqKf/pUZNCgVLH2HfjrUdG5na
MD5:	9EA885479C34ABD9DF4459413CC9C658
SHA1:	A0677D22BE532CC6FF58515FF615D3ABCA717CF6
SHA-256:	9D7251E88BF700BC2222B407C730AF5BA98BEA198479BB1DE63D71046406685C
SHA-512:	6E622C893C13B9441179D4A6B177695E970234FCBA8C2E08B8322EE26C46C98CC1F2FEB36924497F4BD9C8A94C45CF4BE2C16128BACED9B0CDABC73732BE59 6
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13262375298581755","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c8fb386c-d396-41a7-942d-0e3119cdcaef.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:	modified
Size (bytes):	22596
Entropy (8bit):	5.535796493907417
Encrypted:	false
SSDEEP:	384:OkutWLl3DX51kXqKf/pUZNCgVLH2HfDfrU5HG6nTX0iHD948:fLl751kXqKf/pUZNCgVLH2HfjrUdG6nL
MD5:	6F74A29333144F36E9092C62F83710E8
SHA1:	69BD369EC6CE9E4C884295411772FB31C7220193
SHA-256:	708CF3CE4FE0753AC0040182A575EA44C4B125058D543E0528C81C9A3BD1D7C3
SHA-512:	15E00F7C7D9B4546E80CA36470AA3E1D15AD6E0C9642D57EA944085021945D5B7353748C5D437D195E8051BB6F75B4AB23F6BB169A5C68ECDD925942A8C19C6
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13262375298581755","location":5,"manifest":{"a pp":{"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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cb2337b1-1338-4710-a76a-4edad96811e5.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):	5642
Entropy (8bit):	5.188022618828191
Encrypted:	false
SSDEEP:	96:n09aPXfBQlfKcVLwok0JCKL82ks1hbOTQVuwn:n0afClfKcF4KdksL
MD5:	91591A453CFC08908AFE24CCFDFD9F73
SHA1:	CEDEFEA298AFF8202BC70836EB99A13F0E339EB4
SHA-256:	30F2B4820202F9B55D7994A8135C8A7630D38CC543614EE10460F5ED8DBCB05E
SHA-512:	9C26C4AAF4D928BC5EF23CD776AA121753FCC727E55E92C591B15E0448B2F28FE3D58FB241F07561A6C2C76F3E5E54753545D792E96A9695D1F4A53B6906077
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262375298899543","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcom e_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":1 0,"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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.420471906088783
Encrypted:	false
SSDEEP:	3:tUKO3IUfU0VoN2WZmwv3s3IUfUxSesAR1V8ss3IUfUxS2U9bsAR1WGv:m1xU0oNJZmwPkxUxSesA7VvkxUxS2MsQ
MD5:	883F41F6D689806FFD24FEEA2F05EF43
SHA1:	538072C1E1501E88F078111CC13EE3C62DE94329
SHA-256:	A1FBFF5F0DFCC059E88F04C654F835BC6B6D53FD05999992EC123FDE48383C15
SHA-512:	8547D95AFB611528C7C8FE86B9F5C95C4C22B4F1DC4AF066B021FFC33DE97B9CE5815980B986804C32497F49F8AC5885D7157E04ACE3858488F075F34F9A557C
Malicious:	false
Reputation:	low
Preview:	2021/04/08-10:08:36.180 1660 Recovering log #3.2021/04/08-10:08:36.476 1660 Delete type=0 #3.2021/04/08-10:08:36.477 1660 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ea0047d6-e71a-4207-9593-8616b4d921ee.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):	5046
Entropy (8bit):	4.981079290022728
Encrypted:	false
SSDEEP:	96:n09aoXfpcVLwok0JCKL82ks1hbOTQVuwn:n0hfpcF4KdksL
MD5:	7AB2F20E68BCA3741A8C79801ED0C57B
SHA1:	ABCBC433DA58460D0D5CD8822C79B8FEBE89611D
SHA-256:	FC1A1E0F81C636746B1D6CB3AC70BB79C200AFA03923624887C8FA9C3CEADF2E
SHA-512:	D7DCA60A0F1539C50A00644DBBD3F1FE219E29D7535E9EEAC196E50A4AB50F88BF007D3E77358DAE9B78D1D2FB9D1A5E0E714D04E7BFAF6D8D2B2DD1B0A70 B65
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ea0047d6-e71a-4207-9593-8616b4d921ee.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13262375298899543","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"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","

C:\Users\user\AppData\Local\Google\Chrome\User Data\c120168b-fafb-4a67-9f29-1e2bd55b72a2.tmp	
Encrypted:	false
SSDEEP:	384:Ljl+K0rVUUDKtNmrjv6C3ZiYRH8FG9kr/cK8xxQwkTrrOmnsvsOeytOocOND1+3T:PCFJyItJ9OebQ6cwfT+OKoi6J0
MD5:	4D2E91290933C0FA8758BB5718183663
SHA1:	B1F7A05D68D75FD6B61961D62D84EE13D136BE66
SHA-256:	4D919938B8779EEF75044B49C673128762E50339AC1357476FBE2535C7170CA8
SHA-512:	F648F21FBA86940149C05DFF19038218BB4BC7CE38EEE14B1B9940541F173FEB739758CFB0608EC39A93B00E2F574F93D57323E796E4A8ECCA60CA6524F88449
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...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....68.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\fed3a7e5-4107-4194-8caf-2a2751cd808e.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):	164171
Entropy (8bit):	6.0820784437111985
Encrypted:	false
SSDEEP:	3072:3V0ZM4iTMFp3l+7LSx8sogeEFcbXafIB0u1GOJmA3iuRM:lEgMTo7Jsog1aqfIlUOoSiuRM
MD5:	E65D726986914ED0EE859E2982EEF4B8
SHA1:	DE3C8ED6989664A17375A7A4D7E9CC3683A91B1C
SHA-256:	55AB7AD68FD33CB96BDFE5073FABA047E5E538CAF38080B5A4EEF5C66B01FC43
SHA-512:	449EE68279DADDDDC7C205490D741E7BCD55EA010410F48775F2430DCF0FD0A1FAE0864BEF14CCD14D599BD0EEE67A93E1344D014C13B824662528C73C7402B
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.617901701706121e+12,"network":1.617869303e+12,"ticks":100689872.0,"uncertainty":4306838.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016582411"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\1b680ca0-146b-4332-b694-c9cea11bc65b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L]....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..I.6r[yU...%..f.....N..V.....<+.....I..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\e902c43e-0305-41b6-84cf-9edf4335097a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob

C:\Users\user\AppData\Local\Temp\e902c43e-0305-41b6-84cf-9edf4335097a.tmp	
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\fbc8b9bd-cfb5-400c-b322-ec232ca25e91.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\Temp\fc4aeb2a-86a5-4f47-98c8-fb1963a81b08.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\Temp\scoped_dir2336_1287574166\1b680ca0-146b-4332-b694-c9cea11bc65b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\1b680ca0-146b-4332-b694-c9cea11bc65b.tmp	
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...I5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."I...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\en\messages.json	
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\es_419\messages.json	
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The tr ansaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavail able": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEA D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA7555
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... ."... },.. "app_name": {.. "message": "Chrome ... ."... },.. "craw_app_unavailable": {.. "messa ge": "..... .. .."... },.. "craw_connect_to_network": {.. "message": "..... ...."... },.. "iap_unavailable": {.. "message": "..-.. ...."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "..... Chrome ... ."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D0 6E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\hu\messages.json	
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "craw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\ja\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome ....."... },.. "app_name": {.. "message": "Chrome ....."... },.. "craw_app_unavailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "....."... },.. "iap_unavailable": {.. "message": "....."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Chrome ....."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome . ... .."... },.. "app_name": {.. "message": "Chrome . ... .."... },.. "craw_app_unavailable": {.. "message": ".. .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....."... },.. "iap_unavailable": {.. "message": ".. .. ..".. },.. "jwt_retrieve_failed": {.. " message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Chrome. ....."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344 4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema"... },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema"... },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima."... },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo."... },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome.."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\lv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQkkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma"... },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.ma"... },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama."... },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu."... },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami."... },.. "jwt_retrieve_failed": {.. "message": "The transacti on could not be completed."... },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome."... }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\nb\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\nb\messages.json	
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCE
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app_unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap_unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\nl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A A7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\pl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfiIu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOfIC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B7 77
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be com pleted.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\pt_BR\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\pt_BR\messages.json	
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw _app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.".. },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede.".. },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\pt_PT\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTnPlOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F 4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\ro\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.61125938671415
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344HIx2Z+dgrVPlZO8ZpU34qT7hI3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "cr aw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be c ompleted.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\ru\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSl3ZGG7OJHZMSl3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjT03On:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F6 2
Malicious:	false
Reputation:	low

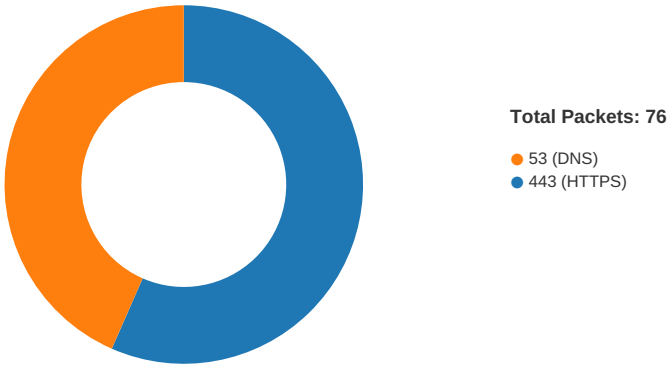
C:\Users\user\AppData\Local\Temp\scoped_dir2336_1287574166\CRX_INSTALL_locales\ru\messages.json	
Preview:	{.. "app_description": {.. "message": "..... ....-..... Chrome".. },.. "app_name": {.. "message": "..... ....-..... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... .....".. },.. "craw_connect_to_network": {.. "message": "..... . .....".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... . Chrome.".. }..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:08:22.315323114 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.316248894 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.421571016 CEST	49709	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.470318079 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.470355988 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.470396996 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.470424891 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.470690966 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.470823050 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.570646048 CEST	443	49709	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.570828915 CEST	49709	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.571154118 CEST	49709	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.619498014 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.622483969 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.622522116 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.622534990 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.622641087 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.622726917 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.626348019 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.626389980 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.626405001 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.626547098 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.646461010 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.647105932 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.647197962 CEST	49705	443	192.168.2.3	103.21.58.181

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:08:22.647422075 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.647711992 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.721227884 CEST	443	49709	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.724025011 CEST	443	49709	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.724047899 CEST	443	49709	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.724061966 CEST	443	49709	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.724107981 CEST	49709	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.725589991 CEST	49709	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.794375896 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.794401884 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.794440985 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.794467926 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.795032024 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.795495987 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.798245907 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.798270941 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.798286915 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.798361063 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.798372984 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.798399925 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.798418045 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.798428059 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.798446894 CEST	443	49705	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.798451900 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.798465967 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.798485994 CEST	49705	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.837500095 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.875415087 CEST	443	49709	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.875442982 CEST	443	49709	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.875458002 CEST	443	49709	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:22.875524044 CEST	49709	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.892363071 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:22.942938089 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:23.717690945 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:23.717720985 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:23.717734098 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:23.717746973 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:23.717765093 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:23.717778921 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:23.717799902 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:23.717827082 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:23.733277082 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:23.882312059 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.446834087 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.446865082 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.446881056 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.446897030 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.446913004 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.446926117 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.446988106 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.447014093 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.537102938 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.538085938 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.538542032 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.539083958 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.539673090 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.540297031 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.540880919 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.684098959 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.684638023 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.685059071 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.685762882 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.686213017 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.687299013 CEST	443	49706	103.21.58.181	192.168.2.3

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:08:24.687973022 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.717905998 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.717932940 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.717946053 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.718000889 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.718019009 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.718034983 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.718033075 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.718051910 CEST	443	49706	103.21.58.181	192.168.2.3
Apr 8, 2021 10:08:24.718077898 CEST	49706	443	192.168.2.3	103.21.58.181
Apr 8, 2021 10:08:24.718100071 CEST	49706	443	192.168.2.3	103.21.58.181

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:08:11.537069082 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:11.551064014 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:12.315946102 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:12.336019039 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:13.221196890 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:13.234899998 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:13.880230904 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:13.893785954 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:21.336711884 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:21.349543095 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:21.806910038 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:21.821154118 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:21.903975964 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:21.924366951 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:21.926006079 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:21.937093019 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:21.947033882 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:22.290848970 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:22.311413050 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:22.320426941 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:22.375641108 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:22.389286995 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:22.781095982 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:22.794420958 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:23.599658012 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:23.615225077 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:23.625294924 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:23.652951002 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:24.540605068 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:24.559180975 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:26.748467922 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:26.765187025 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:26.983849049 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:27.004741907 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:31.031009912 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:31.043966055 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:39.379239082 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:39.406517982 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:41.896400928 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:41.925446987 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:47.120913029 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:47.140219927 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:57.882488966 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:57.895155907 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 10:08:59.179157972 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:08:59.193105936 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 10:09:02.534876108 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:09:02.549170971 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 10:09:03.229640961 CEST	61292	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:09:03.243238926 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 8, 2021 10:09:04.754703999 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:09:04.770364046 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 8, 2021 10:09:05.635170937 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:09:05.647999048 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 10:09:06.323162079 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:09:06.337584019 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 10:09:06.659651041 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:09:06.680979967 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 10:09:08.455435991 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:09:08.467735052 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 10:09:09.288908005 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:09:09.304968119 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 8, 2021 10:09:09.771478891 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:09:09.792877913 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 8, 2021 10:09:10.074965954 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 8, 2021 10:09:10.089092970 CEST	53	59420	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 10:08:21.926006079 CEST	192.168.2.3	8.8.8.8	0x39bb	Standard query (0)	sunmatrixsolar.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:08:24.540605068 CEST	192.168.2.3	8.8.8.8	0xff56	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:08:26.748467922 CEST	192.168.2.3	8.8.8.8	0xa49c	Standard query (0)	sunmatrixsolar.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:08:26.983849049 CEST	192.168.2.3	8.8.8.8	0xbe8a	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:08:39.379239082 CEST	192.168.2.3	8.8.8.8	0xda93	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 10:08:22.311413050 CEST	8.8.8.8	192.168.2.3	0x39bb	No error (0)	sunmatrixsolar.com		103.21.58.181	A (IP address)	IN (0x0001)
Apr 8, 2021 10:08:24.559180975 CEST	8.8.8.8	192.168.2.3	0xff56	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:08:26.765187025 CEST	8.8.8.8	192.168.2.3	0xa49c	No error (0)	sunmatrixsolar.com		103.21.58.181	A (IP address)	IN (0x0001)
Apr 8, 2021 10:08:27.004741907 CEST	8.8.8.8	192.168.2.3	0xbe8a	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:08:39.406517982 CEST	8.8.8.8	192.168.2.3	0xda93	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:08:39.406517982 CEST	8.8.8.8	192.168.2.3	0xda93	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)

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
Apr 8, 2021 10:08:27.106542110 CEST	103.21.58.181	443	192.168.2.3	49723	CN=cpcalendars.sunmatrixsolar.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Feb 13 14:34:34 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri May 14 15:34:34 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 8, 2021 10:08:27.300177097 CEST	103.21.58.181	443	192.168.2.3	49725	CN=cpcalendars.sunmatrixsolar.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Feb 13 14:34:34 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri May 14 15:34:34 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 2336 Parent PID: 968

General

Start time:	10:08:17
Start date:	08/04/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://sunmatrixsolar.com/TO/tomboard@paragon-cc.co.uk'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes

Copyright Joe Security LLC 2021

MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 6020 Parent PID: 2336

General

Start time:	10:08:19
Start date:	08/04/2021
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=1572,16681490481336671047,18098486573724332923,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1704 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly