ID: 881
Cookbook: browseurl.jbs
Time: 13:17:40
Date: 24/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

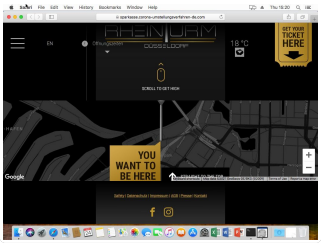
macOS Analysis Report https://sparkasse.corona-umste…

Overview

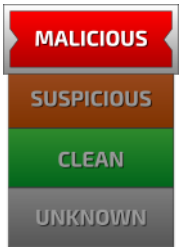
General Information

Sample URL:	http://https://sparkasse.corona-umstellungsverfahren-de.com/ALC81OPACG
Analysis ID:	881
Infos:	

Most interesting Screenshot:



Detection

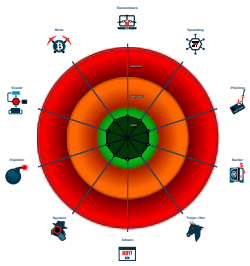


Score:	48
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Opens the Safari browser app

Classification



General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	881
Start date:	24.06.2021
Start time:	13:17:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://sparkasse.corona-umstellungsverfahren-de.com/ALC81OPACG
Analysis system description:	Virtual Machine, High Sierra (Office 2016 v16.16, Java 11.0.2+9, Adobe Reader 2019.010.20099)
Analysis Mode:	default
Detection:	MAL
Classification:	mal48.mac@0/7@15/0
Warnings:	Show All

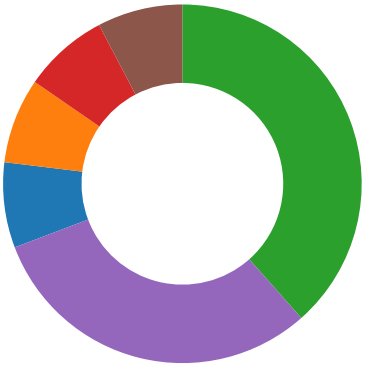
Process Tree

- **System is macvm-highsierra**
- xpcproxy New Fork (PID: 528, Parent: 1)
  - Safari (MD5: 8e18be737fe87f19fe7a97b4821e2005) Arguments: /Applications/Safari.app/Contents/MacOS/Safari
- **cleanup**

Yara Overview

No yara matches

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Persistence and Installation Behavior
- Language, Device and Operating System Detection

Click to jump to signature section

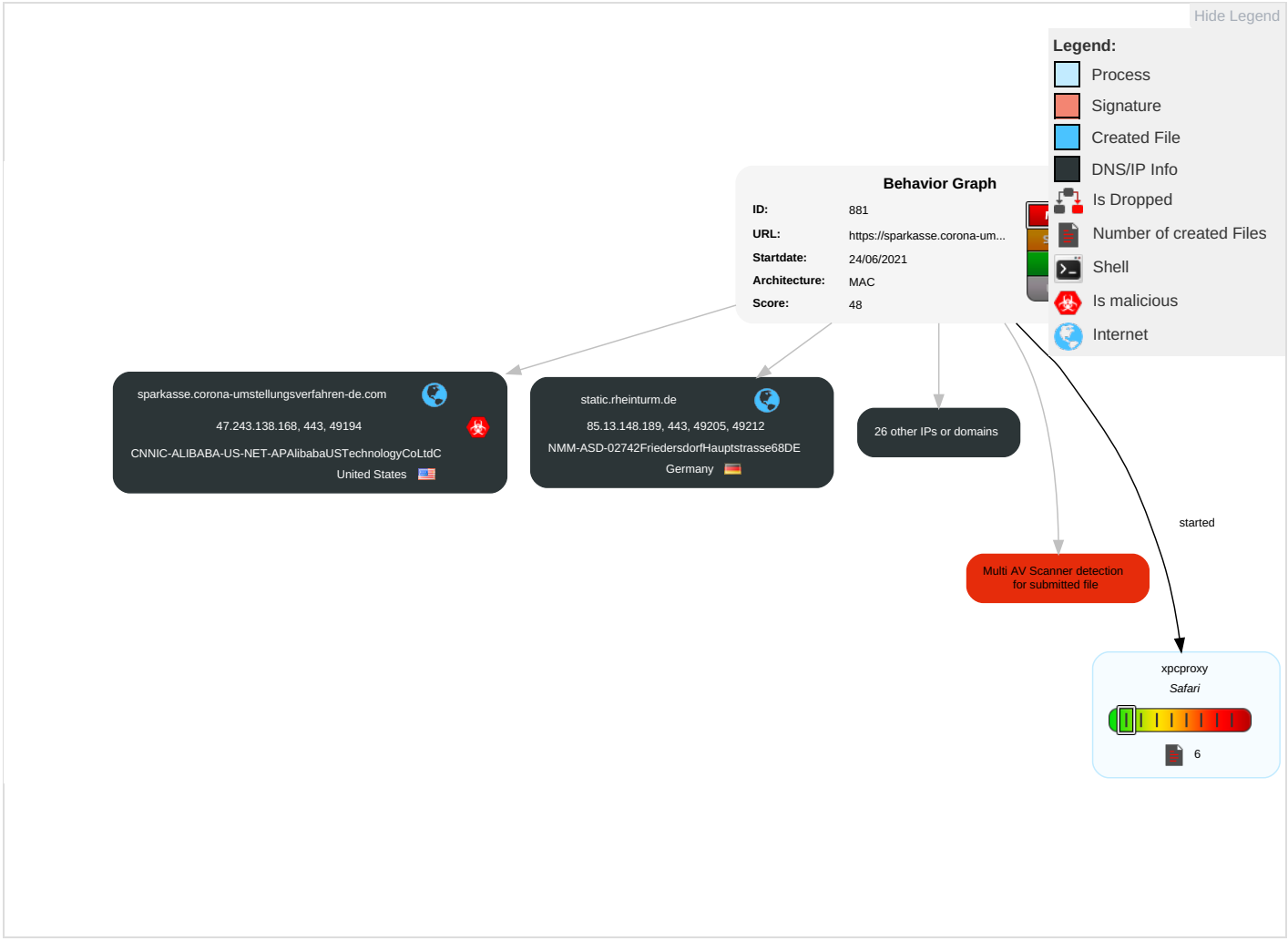
AV Detection:

Multi AV Scanner detection for submitted file

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	Impac
Valid Accounts	Windows Management Instrumentation	Plist Modification 1	Plist Modification 1	Direct Volume Access	OS Credential Dumping	System Information Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	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	Devic Locko
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 Devic Data

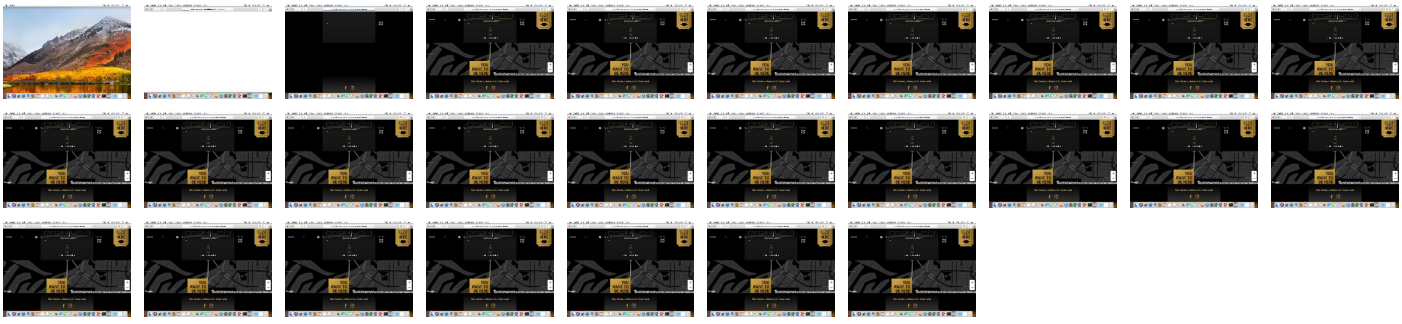
Behavior Graph



Screenshots

Thumbnails

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



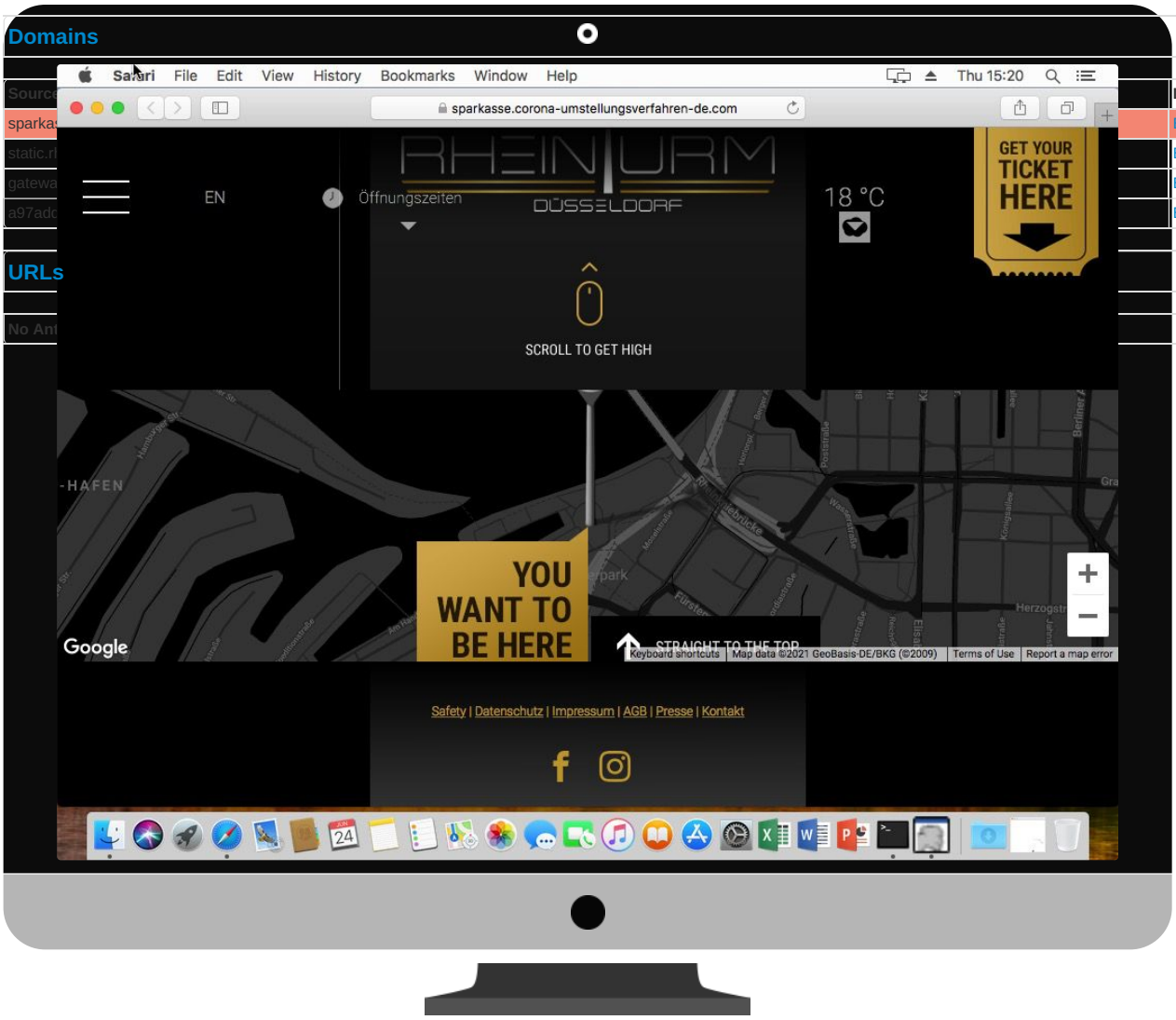
Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://sparkasse.corona-umstellungsverfahren-de.com/ALC81OPACG	9%	Virustotal		Browse
http://https://sparkasse.corona-umstellungsverfahren-de.com/ALC81OPACG	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches



Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sparkasse.corona-umstellungsverfahren-de.com	47.243.138.168	true	true	• 8%, Virustotal, Browse	unknown
dart.l.doubleclick.net	172.217.16.102	true	false		high
pagead46.l.doubleclick.net	142.250.181.226	true	false		high
static.rheinturm.de	85.13.148.189	true	false	• 0%, Virustotal, Browse	unknown
stats.l.doubleclick.net	142.250.27.154	true	false		high
gateway.fe.apple-dns.net	17.248.145.74	true	false	• 0%, Virustotal, Browse	unknown
a97adde81b00f2ca4.awsglobalaccelerator.com	13.248.242.197	true	false	• 0%, Virustotal, Browse	unknown
cm.g.doubleclick.net	172.217.20.2	true	false		high
pixelglobal.sojern.com	107.178.244.119	true	false		high
ib.anycast.adnxs.com	185.33.221.90	true	false		high
kubernetes-loadbalancer.triptease.io	35.186.195.233	true	false		unknown
static.triptease.io	unknown	unknown	false		unknown
pixel.sojern.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
onboard.triptease.io	unknown	unknown	false		unknown
adservice.google.de	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
beacon.sojern.com	unknown	unknown	false		high
x1.c.lencr.org	unknown	unknown	false		unknown
api.triptease.io	unknown	unknown	false		unknown
ib.adnxs.com	unknown	unknown	false		high
r3.o.lencr.org	unknown	unknown	false		unknown
match.adsrvr.org	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.33.221.90	ib.anycast.adnxs.com	Netherlands		29990	ASN-APPNEXUS	false
107.178.244.119	pixelglobal.sojern.com	United States		15169	GOOGLEUS	false
13.248.242.197	a97adde81b00f2ca4.awsglobalaccelerator.com	United States		16509	AMAZON-02US	false
17.253.55.204	unknown	United States		6185	APPLE-AUSTINUS	false
17.248.145.74	gateway.fe.apple-dns.net	United States		714	APPLE-ENGINEERINGUS	false
104.76.200.212	unknown	United States		3462	HINETDataCommunicationBusinessGroupTW	false
85.13.148.189	static.rheinturm.de	Germany		34788	NMM-ASD-02742FriedersdorfHauptstrasse68DE	false
47.243.138.168	sparkasse.corona-umstellungsverfahren-de.com	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
172.217.16.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.27.154	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
17.171.27.65	unknown	United States		714	APPLE-ENGINEERINGUS	false
35.186.195.233	kubernetes-loadbalancer.triptease.io	United States		15169	GOOGLEUS	false
172.217.20.2	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/Users/berri/Library/Safari/.dat.nosync0210.8kfcUv	
Process:	/Applications/Safari.app/Contents/MacOS/Safari
File Type:	Apple binary property list
Category:	dropped
Size (bytes):	1746
Entropy (8bit):	7.2504763805227075
Encrypted:	false

/Users/berri/Library/Safari/.dat.nosync0210.8kfcUv	
SSDEEP:	24:/MVp+dVGmEH3oFqBo4cT9DHoTAqg9f9SoQ78WqcS+9aNMMOjSQj/4zQLcT0BzVvb:E3NmrecoTlg9fYwi4TkH/xL5DcRJg
MD5:	F1B94C817755ACE420A7FB7631151174
SHA1:	FE9F7D72F241B92200297B8779D4841A6E377D3E
SHA-256:	E50786DBB43BBF91EDC23F3968BF172C32BC3B66C69CCBEF7C3B36197F40A768
SHA-512:	AE4452E25E8480E0357E3EBD5A5F409AB6532A4BC9338CD1E858947C6F7DD3DE7937412BCFB750310FF8B27181444AD578944EF9DED7C1DAEDB1A5959BFD40E
Malicious:	false
Reputation:	low
Preview:	bplist00.....^SessionVersion^SessionWindowsS1.0.....9_..SelectedTabIndex\TabBarHiddenZDateClosed_..FavoritesBarHidden]IsPopupWindow_. PrefersReadingListSidebarVisible\Miniaturized_..WindowStateVersionZWindowUUID_..WindowContentRectYTabStates_..IsPrivateWindow_..SelectedPinnedTabIndex...3A.B^..E....S2.0_.$0CF9D3F8-C031-4694-8366-FC506FE1E754_..{{0, 52}, {1024, 693}}.... !."#.$%&'()*.,-...0123456.\IsDisposable\SessionState_..AncestorTabIdentifiers_..SessionStateIsEncryptedXTabIndex]LastVisitTimeWTabUUIDVTabURL]TabIdentifierXTabTitle_..ProcessIdentifierWIsMuted.O........}.9.$0....H..-.~NO.....:...._.c.....XS..@vPNTE.....{Z..K..A..Eb....zC..*.....""....34.....s..W..C.N..j.r.O.....:.....O..S.)..E....][..zgbt....H...?..J.X..M..}..4..|K.a-..z.%6.j.....Ll`.(oe^.mj."..H.k...q..y.G....Q%.f.-.*.x..:g.3Zd....F...^.6.iZ)....'.VN..N...!.X..E.....!..e....|p....P.:....E p..V.IPS.B.F..9M"%.....P.....\qcx...[.....a.V.m...GX~..kS.....h.. ._...

/Users/berri/Library/Safari/.dat.nosync0210.bKXvUw	
Process:	/Applications/Safari.app/Contents/MacOS/Safari
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1012
Entropy (8bit):	5.286991847916908
Encrypted:	false
SSDEEP:	24:2dfyiwHuG5Ku3hu65juqVrTrmuGoTxR1F1xW:cfyP5Z/5PrUon1F1xW
MD5:	0C29425555C7FF0CA114B1FD0DC39C50
SHA1:	D7D808E8BE92462F4C3CEBA66734F0E9BB26ACDD
SHA-256:	52826AFEEC974BB7BACB85BDC01DC4F23BF917D65E04773D7CAD393F7866F3FD
SHA-512:	D9C8364A85F4B4A96CAAC1409F32F9D6B2F8AE19201E0ABD2D449A3EEDADD471E99E44BC92DEB5D8FB60287DA64A88E61B45F759E7B9A383A9BBE5F5FD242F95
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">.<plist version="1.0">.<dict>..<key>SingleDeviceSaveChangesThrottlingPolicy</key>..<string>1:1440</string>..<key>MultipleDeviceSaveChangesThrottlingPolicy</key>..<string>50:1 | 10:2 | 10:5 | 10:30 | 9:40 | 1:510</string>..<key>SingleDeviceFetchChangesThrottlingPolicy</key>..<string>11:15 | 1:1275</string>..<key>MultipleDeviceFetchChangesThrottlingPolicy</key>..<string>50:1 | 50:3 | 20:4 | 20:5 | 20:15 | 20:18 | 20:20</string>..<key>SyncCircleSizeRetrievalThrottlingPolicy</key>..<string>1:1440</string>..<key>MaximumRequestLimitCharacterCount</key>..<integer>100000</integer>..<key>SyncWindow</key>..<real>1209600</real>..<key>HistoryModificationIdleDelayBeforeSyncAttemptKey</key>..<integer>90</integer>..<key>HistoryRemovalIdleDelayBeforeSyncAttempt</key>..<integer>6</integer>..<key>SaveChangesBeforeTerminationTimeout</key>..<integer>1</integer>.</dic

/Users/berri/Library/Safari/Favicon Cache/favicons/.dat.nosync0210.t7NkvP	
Process:	/Applications/Safari.app/Contents/MacOS/Safari
File Type:	MS Windows icon resource - 6 icons, 256x256 withPNG image data, 256 x 256, 8-bit/color RGB, non-interlaced, 32 bits/pixel, 128x128, 32 bits/pixel
Category:	dropped
Size (bytes):	104432
Entropy (8bit):	4.144635779349267
Encrypted:	false
SSDEEP:	384:foO4vY8acUdOxNu1cG+87BPCi7uoO17Lhx13FKFK4TQ4lL7R30yr+DCCCCCCCCCw:fHb8/xY1cV1rAQ4lLxIrCgT7it
MD5:	C38CA5B1EF20C89B52E393D842861586
SHA1:	7071CDC3F0CADF38D598FC66FFFECDFB7617B8F5
SHA-256:	DCECA13D3E8348F4628F4151D05B31A83757F5ED550D5DB9997B5B3B4A38FD4B
SHA-512:	E4F866841A1DFB829DBBCF5F3AFDB090F0B23B2F59A58C56FE244D5F80E7C41D89130FEF9578BE0BE69FAA8DB1634B3A5F2AAEA0877F04F91EC6A7685879FF10
Malicious:	false
Reputation:	low
Preview:	....f..... .(.....@@.... .(B.....00.... ..%..8].. .... .h.....PNG.....IHDR.....?1...IIDATx...r#.....<H"cDj..:.....7V/.wz...F8.o'..I.B..b...9.x...@..]{!.. ...n.....%..>....*.J..O.....h . ....&.....s..]..]., .;&..4.J.....h . .....ZKM..O...u.....q..q..W.F...?.$..h`....D....@.@4.....qp.V{...u.....p83.1l..T....h . .....A..RXL.....A.....h . ....&..R.&X6.....h . .....A.ra.....`k..Qd.?.%.....h . .....A..\.si:_.0....]....!5O_.".^%..r.....*A.....h.....1..3.....jm#..g.c..U.....D....@.@4..W....:.A..g."..... .....h ..W.KfN.$l.;..i..\...s.....j...P...b../...c.....x.1(.X*.9.....h . ...ea}t6.....=ok...Mj.....$.h4...]....@..`1.Rjs.I._.....c..C....w.~8_'..999.....B.e@.....h . ...ea1([.m8.^]]..z..h4.C.... ...i...hT..C.V.f..l..1q!...D....@.@4.....d...G.|.....aQ/._.....a..@I ..d...z...s.4.M6.....A..4...-.t..h . .....b.=~.....>

/dev/null	
Process:	/Applications/Safari.app/Contents/MacOS/Safari
File Type:	ASCII text
Category:	dropped
Size (bytes):	61
Entropy (8bit):	4.786894099680635
Encrypted:	false
SSDEEP:	3:tUI52wcLJLXd5HWOv:mO2p1jd52A

/dev/null	
MD5:	DC10074F8C99C0D488FBBAF3B38C87D1
SHA1:	7B7090DCCC48BD1A30868B65865BF14997A5860B
SHA-256:	DF41FA20D04461218689127C1857BBE4213ABF48AA1862DB720591471E998278
SHA-512:	7CA53D9661C24695F044F775EAB29BA6DB08DF93214C7E62A19658CEFE1E766156BEE13AD25D94A45729D5213AE9084BE8B010CAEF27EC9564BDADAB3C465F5
Malicious:	false
Reputation:	low
Preview:	2021-06-24 15:18:29.042 Safari[528:4417] ApplePersistence=NO.

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/0/SafariFamily/Safari/.dat.nosync0210.Is8mxg	
Process:	/Applications/Safari.app/Contents/MacOS/Safari
File Type:	Apple binary property list
Category:	dropped
Size (bytes):	76
Entropy (8bit):	3.9370658315190226
Encrypted:	false
SSDEEP:	3:N1n6qMvRGNMTAnd/t1tH:N1nleRaMTAltH
MD5:	CDC65B5F112547EAFAE0F16F9C149426
SHA1:	AEAF9908A5B6FF3E2F7B738ABF5FE9E79108BA01
SHA-256:	1C6D085D871A855CE4A3902BAB4B9B92631B8EE8F0B7F6536768A2AAF427B45C
SHA-512:	E8B0E4CE6A760A718A19976D3CFE9063F04FB4BF179947AECA84E94C83F21459FB9DC0FFABEA8F633BD2D0BA94FE1E15D8C97E9604FDE8BD0DEA961EB83BDDB7
Malicious:	false
Reputation:	low
Preview:	bplist00..._..ExtensionArchivesExtracted...(.....)

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/C/mds/mdsDirectory.db_	
Process:	/Applications/Safari.app/Contents/MacOS/Safari
File Type:	Mac OS X Keychain File
Category:	dropped
Size (bytes):	48908
Entropy (8bit):	3.533948990143748
Encrypted:	false
SSDEEP:	384:xSMdGleGklG7FF3theSMVXBD0tgcNrGBOmBfbouR6/chQOnGqwc2U+v+h/:8MdGleOGmBouRwchQOnGqwc2U+v+h/
MD5:	09070E01FA6ED1973D94FAD50C35E3ED
SHA1:	7546663E66F9889EE3365A7A0BE372300C6022CA
SHA-256:	2E6EC437A97DD88F9067B2E99AC64789670D9B9C1FC50B2856E392E66163211F
SHA-512:	621399FF832F1A8352E5E9A54984B878C7D3432156D9CF9986A1A5B75662E92D9A00FA1BA6714D679286BB49E71916F72655AADA2B99880A2806FAFC6F86E7F3
Malicious:	false
Reputation:	low
Preview:	kych.....`...X...p..S0..SX..Th..T...T...[...^h.....L...X.....T.....d.....t.....t.....<.....P.....0.....$...p.....l.....X.....@.....!...%.....CSSM_DL_DB_SCHEMA_INFO.....D.....!...%.....CSSM_DL_DB_SCHEMA_ATTRIBUTES...D.....!...%.....CSSM_DL_DB_SCHEMA_INDEXES.....H.....!...%..... CSSM_DL_DB_SCHEMA_PARSING_MODULE...D.....!...%@.....MDS_CDSADIR_CSSM_RECORDTYPE....D.....!...%@.....MDS_CDSADIR_KRMM_RECORDTYPE....D.....!...%@.....MDS_CDSADIR_EMM_RECORDTYPE.....L.....!...%@....."MDS_CDSADIR_EMM_PRIMARY_RECORDTYPE.....H.....!...%@.....MDS_CDSADIR_COMMON_RECORDTYPE.....L.....!...%@....."MDS_CDSADIR_CSP_PRIMARY_RECORDTYPE.....P.....!...%@.....%MDS_CDSADIR_CSP_CAPABILITY_R

/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/C/mds/mdsObject.db_	
Process:	/Applications/Safari.app/Contents/MacOS/Safari
File Type:	Mac OS X Keychain File
Category:	dropped
Size (bytes):	4404
Entropy (8bit):	3.5113078915037033
Encrypted:	false
SSDEEP:	48:m6Xsh+CLjL3Pe3T5FFKfEuyu+iYxGv4sS:3X6LjLfe3wEuyu9YxGQX
MD5:	D487F899A14AE98519B46D51BC810F1B
SHA1:	64877ECFBE47ED66EED545B2449BBE8B22B775D0
SHA-256:	4835899C464487946E281D535381D4CAB8BC90EC08CD00A6A0ECB97854E9321D
SHA-512:	EB4FABD61B4FD2B9EF3C9E93793CA5F11353A1F81EA4DA22E0F79ED45D89180B77469B9E5DCD5350AE650B31DE9018743DA7716EFA7B5CDDFC3FA7A13C47640
Malicious:	false
Reputation:	low

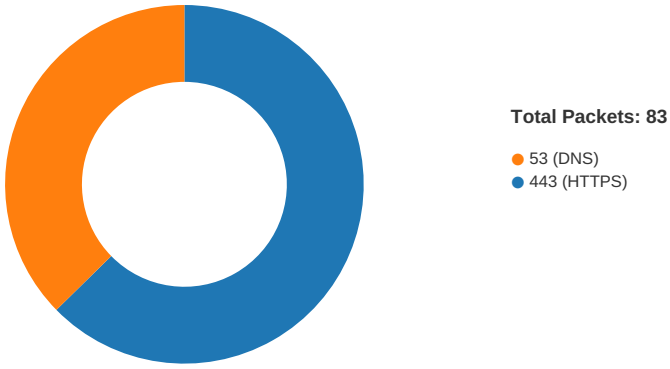
/private/var/folders/ql/8wfqxrtx52n95h35b6cz4nyw0000gn/C/mds/mdsObject.db_	
Preview:	kych.....d.....0.....0...p.....@...@.....!...%.....CSSM_DL_DB_SCHEMA_INFO.....D.....!...%..... CSSM_DL_DB_SCHEMA_ATTRIBUTES...D.....!...%.....CSSM_DL_DB_SCHEMA_INDEXES.....H.....!...%..... CSSM_DL_DB_SCHEMA_PARSING_MODULE...@.....!...%@.....MDS_OBJECT_RECORDTYPE.....h..... ..`..... ...@.....-...1...5...9...=@.....X..... ...P..... ...p.....l.....d.....P.....H.....,.....h.....P.....1...5...9...=.....M.....RelationID.....P.....1...5...9...=.....M .....RelationName.....P.....1...5...9...=.....M.....RelationID.....P.....1...5...9...=.....M.....AttributeID.....X....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 24, 2021 13:18:31.547223091 CEST	192.168.11.11	1.1.1.1	0xc40a	Standard query (0)	sparkasse.corona-umstellungsverfahren-de.com	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:33.031886101 CEST	192.168.11.11	1.1.1.1	0x9e1d	Standard query (0)	r3.o.lencr.org	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:33.034948111 CEST	192.168.11.11	1.1.1.1	0xad2d	Standard query (0)	x1.c.lencr.org	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:35.066656113 CEST	192.168.11.11	1.1.1.1	0x66fc	Standard query (0)	static.rheinturm.de	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:35.068680048 CEST	192.168.11.11	1.1.1.1	0xbe25	Standard query (0)	static.triptease.io	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:35.447813034 CEST	192.168.11.11	1.1.1.1	0x5025	Standard query (0)	beacon.sojern.com	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:35.452259064 CEST	192.168.11.11	1.1.1.1	0xc5b0	Standard query (0)	onboard.triptease.io	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:35.786597013 CEST	192.168.11.11	1.1.1.1	0x9855	Standard query (0)	api.triptease.io	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.000657082 CEST	192.168.11.11	1.1.1.1	0xeda6	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.002609015 CEST	192.168.11.11	1.1.1.1	0x5e8c	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.002768993 CEST	192.168.11.11	1.1.1.1	0xf8fe	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 24, 2021 13:18:36.004607916 CEST	192.168.11.11	1.1.1.1	0xc85b	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.432132959 CEST	192.168.11.11	1.1.1.1	0xdd8b	Standard query (0)	pixel.sojern.com	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.609052896 CEST	192.168.11.11	1.1.1.1	0x7a73	Standard query (0)	adservice.google.de	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:37.584100008 CEST	192.168.11.11	1.1.1.1	0x6d4	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 24, 2021 13:18:31.976254940 CEST	1.1.1.1	192.168.11.11	0xc40a	No error (0)	sparkasse.corona-umstellungsverfahren-de.com		47.243.138.168	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:31.991909027 CEST	1.1.1.1	192.168.11.11	0x30a1	No error (0)	gateway.fe.apple-dns.net		17.248.145.74	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:31.991909027 CEST	1.1.1.1	192.168.11.11	0x30a1	No error (0)	gateway.fe.apple-dns.net		17.248.145.147	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:31.991909027 CEST	1.1.1.1	192.168.11.11	0x30a1	No error (0)	gateway.fe.apple-dns.net		17.248.145.139	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:31.991909027 CEST	1.1.1.1	192.168.11.11	0x30a1	No error (0)	gateway.fe.apple-dns.net		17.248.145.143	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:31.991909027 CEST	1.1.1.1	192.168.11.11	0x30a1	No error (0)	gateway.fe.apple-dns.net		17.248.145.144	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:31.991909027 CEST	1.1.1.1	192.168.11.11	0x30a1	No error (0)	gateway.fe.apple-dns.net		17.248.145.202	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:31.991909027 CEST	1.1.1.1	192.168.11.11	0x30a1	No error (0)	gateway.fe.apple-dns.net		17.248.145.146	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:31.991909027 CEST	1.1.1.1	192.168.11.11	0x30a1	No error (0)	gateway.fe.apple-dns.net		17.248.145.164	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:33.040370941 CEST	1.1.1.1	192.168.11.11	0x9e1d	No error (0)	r3.o.lencr.org	o.lencr.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:33.043989897 CEST	1.1.1.1	192.168.11.11	0xad2d	No error (0)	x1.c.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:35.098663092 CEST	1.1.1.1	192.168.11.11	0x66fc	No error (0)	static.rheinturm.de		85.13.148.189	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:35.114051104 CEST	1.1.1.1	192.168.11.11	0xbe25	No error (0)	static.triptease.io	q.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:35.458962917 CEST	1.1.1.1	192.168.11.11	0x5025	No error (0)	beacon.sojern.com	pixelglobal.sojern.com		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:35.458962917 CEST	1.1.1.1	192.168.11.11	0x5025	No error (0)	pixelglobal.sojern.com		107.178.244.119	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:35.461179972 CEST	1.1.1.1	192.168.11.11	0xc5b0	No error (0)	onboard.triptease.io	onboard.triptease.io.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:35.797981977 CEST	1.1.1.1	192.168.11.11	0x9855	No error (0)	api.triptease.io	kubernetes-loadbalancer.triptease.io		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:35.797981977 CEST	1.1.1.1	192.168.11.11	0x9855	No error (0)	kubernetes-loadbalancer.triptease.io		35.186.195.233	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.009327888 CEST	1.1.1.1	192.168.11.11	0xeda6	No error (0)	cm.g.doubleclick.net		172.217.20.2	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.010739088 CEST	1.1.1.1	192.168.11.11	0x5e8c	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:36.010739088 CEST	1.1.1.1	192.168.11.11	0x5e8c	No error (0)	dart.l.doubleclick.net		172.217.16.102	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 24, 2021 13:18:36.011209011 CEST	1.1.1.1	192.168.11.11	0xf8fe	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:36.011209011 CEST	1.1.1.1	192.168.11.11	0xf8fe	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:36.011209011 CEST	1.1.1.1	192.168.11.11	0xf8fe	No error (0)	ib.anycast .adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.011209011 CEST	1.1.1.1	192.168.11.11	0xf8fe	No error (0)	ib.anycast .adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.011209011 CEST	1.1.1.1	192.168.11.11	0xf8fe	No error (0)	ib.anycast .adnxs.com		185.33.221.14	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.011209011 CEST	1.1.1.1	192.168.11.11	0xf8fe	No error (0)	ib.anycast .adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.011209011 CEST	1.1.1.1	192.168.11.11	0xf8fe	No error (0)	ib.anycast .adnxs.com		185.33.223.178	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.011209011 CEST	1.1.1.1	192.168.11.11	0xf8fe	No error (0)	ib.anycast .adnxs.com		185.33.221.88	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.011209011 CEST	1.1.1.1	192.168.11.11	0xf8fe	No error (0)	ib.anycast .adnxs.com		185.33.221.13	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.011209011 CEST	1.1.1.1	192.168.11.11	0xf8fe	No error (0)	ib.anycast .adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.012895107 CEST	1.1.1.1	192.168.11.11	0xc85b	No error (0)	match.adsrvr.org	match-aga.adsrvr.org		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:36.012895107 CEST	1.1.1.1	192.168.11.11	0xc85b	No error (0)	match-aga. adsrvr.org	a97adde81b00f2ca4.awsglobalaccelerator.com		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:36.012895107 CEST	1.1.1.1	192.168.11.11	0xc85b	No error (0)	a97adde81b 00f2ca4.aw sglobalacc elerator.com		13.248.242.197	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.012895107 CEST	1.1.1.1	192.168.11.11	0xc85b	No error (0)	a97adde81b 00f2ca4.aw sglobalacc elerator.com		76.223.111.131	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.441044092 CEST	1.1.1.1	192.168.11.11	0xdd8b	No error (0)	pixel.sojern.com	pixelglobal.sojern.com		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:36.441044092 CEST	1.1.1.1	192.168.11.11	0xdd8b	No error (0)	pixelgloba l.sojern.com		107.178.244.119	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:36.617521048 CEST	1.1.1.1	192.168.11.11	0x7a73	No error (0)	adservice. google.de	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:36.617521048 CEST	1.1.1.1	192.168.11.11	0x7a73	No error (0)	pagead46.l .doubleclick.net		142.250.181.226	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:37.592453957 CEST	1.1.1.1	192.168.11.11	0x6d4	No error (0)	stats.g.do ubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 24, 2021 13:18:37.592453957 CEST	1.1.1.1	192.168.11.11	0x6d4	No error (0)	stats.l.do ubleclick.net		142.250.27.154	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:37.592453957 CEST	1.1.1.1	192.168.11.11	0x6d4	No error (0)	stats.l.do ubleclick.net		142.250.27.157	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:37.592453957 CEST	1.1.1.1	192.168.11.11	0x6d4	No error (0)	stats.l.do ubleclick.net		142.250.27.156	A (IP address)	IN (0x0001)
Jun 24, 2021 13:18:37.592453957 CEST	1.1.1.1	192.168.11.11	0x6d4	No error (0)	stats.l.do ubleclick.net		142.250.27.155	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
Jun 24, 2021 13:18:32.012967110 CEST	17.248.145.74	443	192.168.11.11	49195	C=US, ST=California, O=Apple Inc., CN=gateway.icloud.com C=US, O=Apple Inc., OU=Certification Authority, CN=Apple IST CA 2 - G1 C=US, O=Apple Inc., OU=Certification Authority, CN=Apple IST CA 2 - G1	C=US, O=Apple Inc., OU=Certification Authority, CN=Apple IST CA 2 - G1 CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE CN=GeoTrust Global CA, O=GeoTrust Inc., C=US	Mon Jul 20 19:41:36 CEST 2020 Wed Dec 12 13:00:00 CET 2018 Mon Jun 16 17:42:02 CEST 2014	Thu Aug 19 19:51:00 CEST 2021 Wed May 07 14:00:00 CEST 2025 Fri May 20 17:42:02 CEST 2022	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2
					C=US, O=Apple Inc., OU=Certification Authority, CN=Apple IST CA 2 - G1	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Dec 12 13:00:00 CET 2018	Wed May 07 14:00:00 CEST 2025		
					C=US, O=Apple Inc., OU=Certification Authority, CN=Apple IST CA 2 - G1	CN=GeoTrust Global CA, O=GeoTrust Inc., C=US	Mon Jun 16 17:42:02 CEST 2014	Fri May 20 17:42:02 CEST 2022		
Jun 24, 2021 13:18:33.003151894 CEST	47.243.138.168	443	192.168.11.11	49194	CN=sparkasse.corona-umstellungsverfahren-de.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jun 08 12:01:51 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Sep 06 12:01:51 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10-21,29-23-24,0	92306a1faec06f00b17da7dd2a607d69
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 24, 2021 13:18:35.150533915 CEST	85.13.148.189	443	192.168.11.11	49205	CN=static.rheinturm.de CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 22 03:11:36 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Aug 20 03:11:36 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 24, 2021 13:18:35.497191906 CEST	107.178.244.119	443	192.168.11.11	49209	CN=*.sojern.com, O="Sojern, Inc.", L=Omaha, ST=Nebraska, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Dec 07 01:00:00 CET 2020	Tue Dec 21 00:59:59 CET 2021	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jun 24, 2021 13:18:35.802954912 CEST	85.13.148.189	443	192.168.11.11	49212	CN=static.rheinturm.de CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 22 03:11:36 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Aug 20 03:11:36 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 24, 2021 13:18:35.820970058 CEST	35.186.195.233	443	192.168.11.11	49213	CN=*.triptease.io, OU=Triptease Ltd, O=Triptease Ltd, STREET="Devonshire House, 60 Goswell Road", L=London, ST=London, OID.2.5.4.17=EC1M 7AD, C=GB CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Thu Apr 16 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Mon Feb 01 01:00:00 CET 2010	Sun May 08 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Tue Jan 19 00:59:59 CET 2038	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		
Jun 24, 2021 13:18:36.067429066 CEST	185.33.221.90	443	192.168.11.11	49216	CN=*.adnxs.com, O=Xandr Inc., L=New York, ST=New York, C=US CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 05 01:00:00 CET 2021 Mon Nov 06 13:24:09 CET 2017	Sun Feb 20 00:59:59 CET 2022 Sat Nov 06 13:24:09 CET 2027	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:24:09 CET 2017	Sat Nov 06 13:24:09 CET 2027		
Jun 24, 2021 13:18:36.088251114 CEST	172.217.20.2	443	192.168.11.11	49214	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 24 03:34:17 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 16 03:34:16 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 24, 2021 13:18:36.090882063 CEST	172.217.16.102	443	192.168.11.11	49215	CN=*.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 24 03:32:07 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Aug 16 03:32:06 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jun 24, 2021 13:18:36.094093084 CEST	13.248.242.197	443	192.168.11.11	49217	CN=*.adsrvr.org CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3 CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Mar 18 23:45:32 CET 2021 Tue Jul 28 02:00:00 CEST 2020 Wed Mar 18 11:00:00 CET 2009	Wed Apr 20 00:45:32 CEST 2022 Sun Mar 18 01:00:00 CET 2029 Sun Mar 18 11:00:00 CET 2029	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2
					CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
					CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Mar 18 11:00:00 CET 2009	Sun Mar 18 11:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 24, 2021 13:18:36.478436947 CEST	107.178.244.119	443	192.168.11.11	49221	CN=*.sojern.com, O="Sojern, Inc.", L=Omaha, ST=Nebraska, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Tue Dec 21 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jun 24, 2021 13:18:37.640086889 CEST	142.250.27.154	443	192.168.11.11	49223	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon May 24 03:34:09 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 16 03:34:08 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49188-49187-49162-49161-52393-49200-49199-49192-49191-49172-49171-52392-157-156-61-60-53-47,65281-0-23-13-5-13172-18-16-11-10,29-23-24,0	3e4e87dda5a3162306609b7e330441d2
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

System Behavior

Analysis Process: xpcproxy PID: 528 Parent PID: 1

General

Start time:	13:18:28
Start date:	24/06/2021
Path:	/usr/libexec/xpcproxy
Arguments:	n/a
File size:	43488 bytes
MD5 hash:	d1bb9a4899f0af921e8188218b20d744

File Activities

File Read

Directory Created

Analysis Process: Safari PID: 528 Parent PID: 1

General

Start time:	13:18:28
Start date:	24/06/2021
Path:	/Applications/Safari.app/Contents/MacOS/Safari
Arguments:	/Applications/Safari.app/Contents/MacOS/Safari
File size:	20896 bytes
MD5 hash:	8e18be737fe87f19fe7a97b4821e2005

File Activities

File Created

File Deleted

File Read

File Written

File Moved

Directory Enumerated

Directory Attributes Enumerated Bulk

Directory Created

Permission Modified