ID: 413040
Cookbook: browseurl.jbs
Time: 06:47:45
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

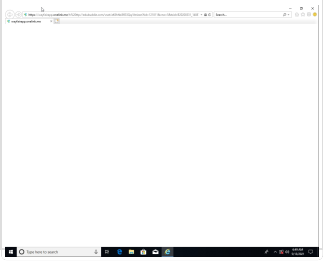
Analysis Report https://wayfairapp.onelink.me/24208021…

Overview

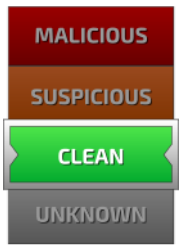
General Information

Sample URL:	https://wayfairapp.onelink.me/2420802157?pid=Email&c=Triggered&af_sub5=AppE...i8933Qq%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5
Analysis ID:	413040
Infos:	

Most interesting Screenshot:



Detection

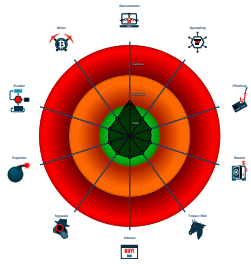


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5836 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5888 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5836 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

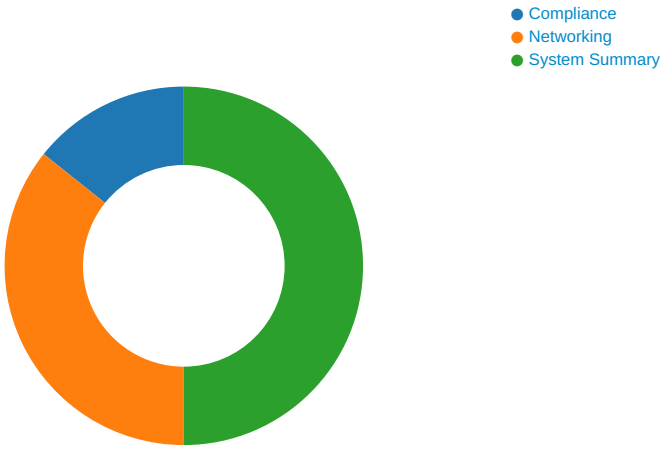
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



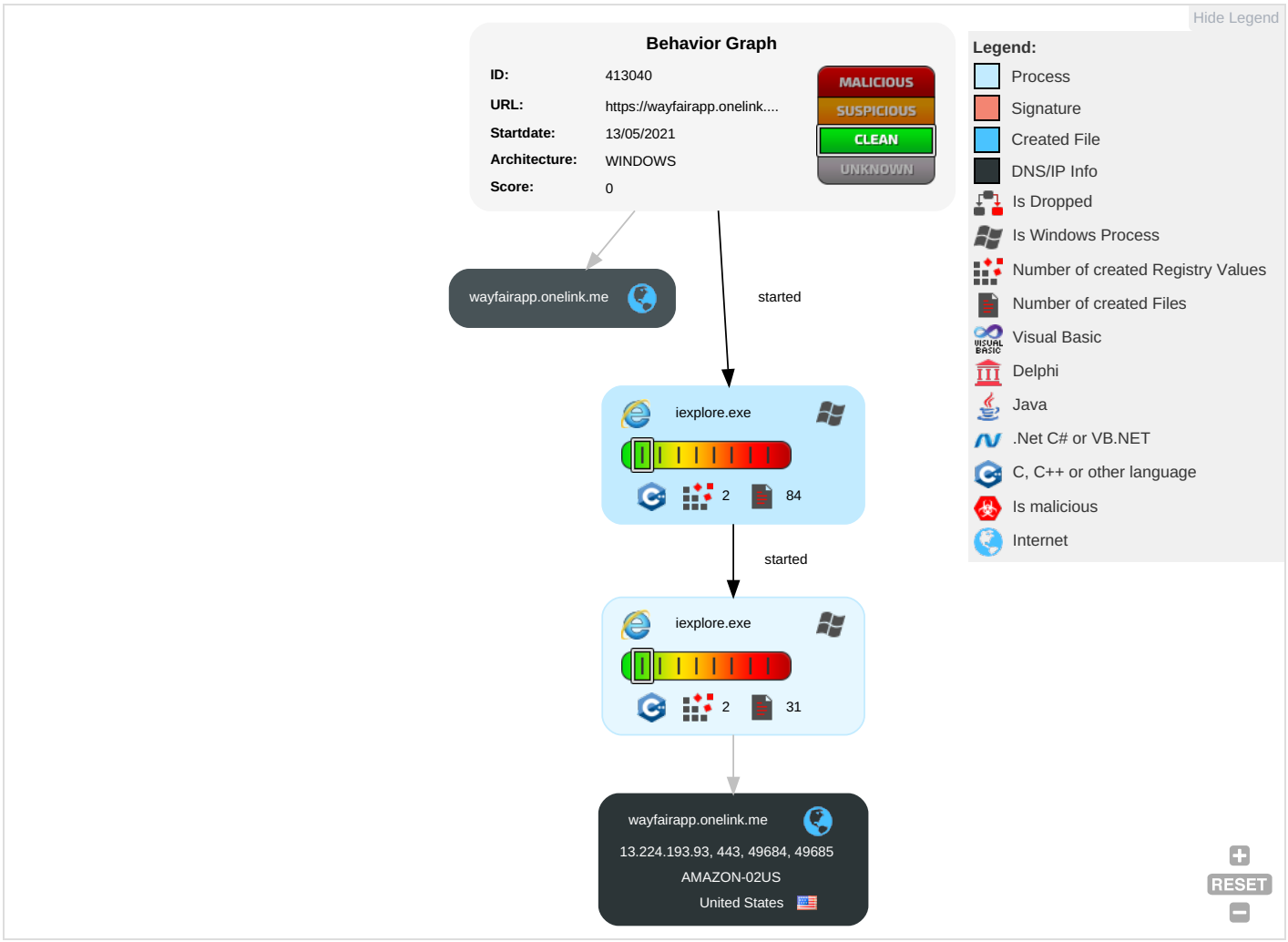
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
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	Devic Lockc
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	Delet Devic Data

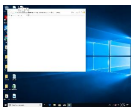
Behavior Graph

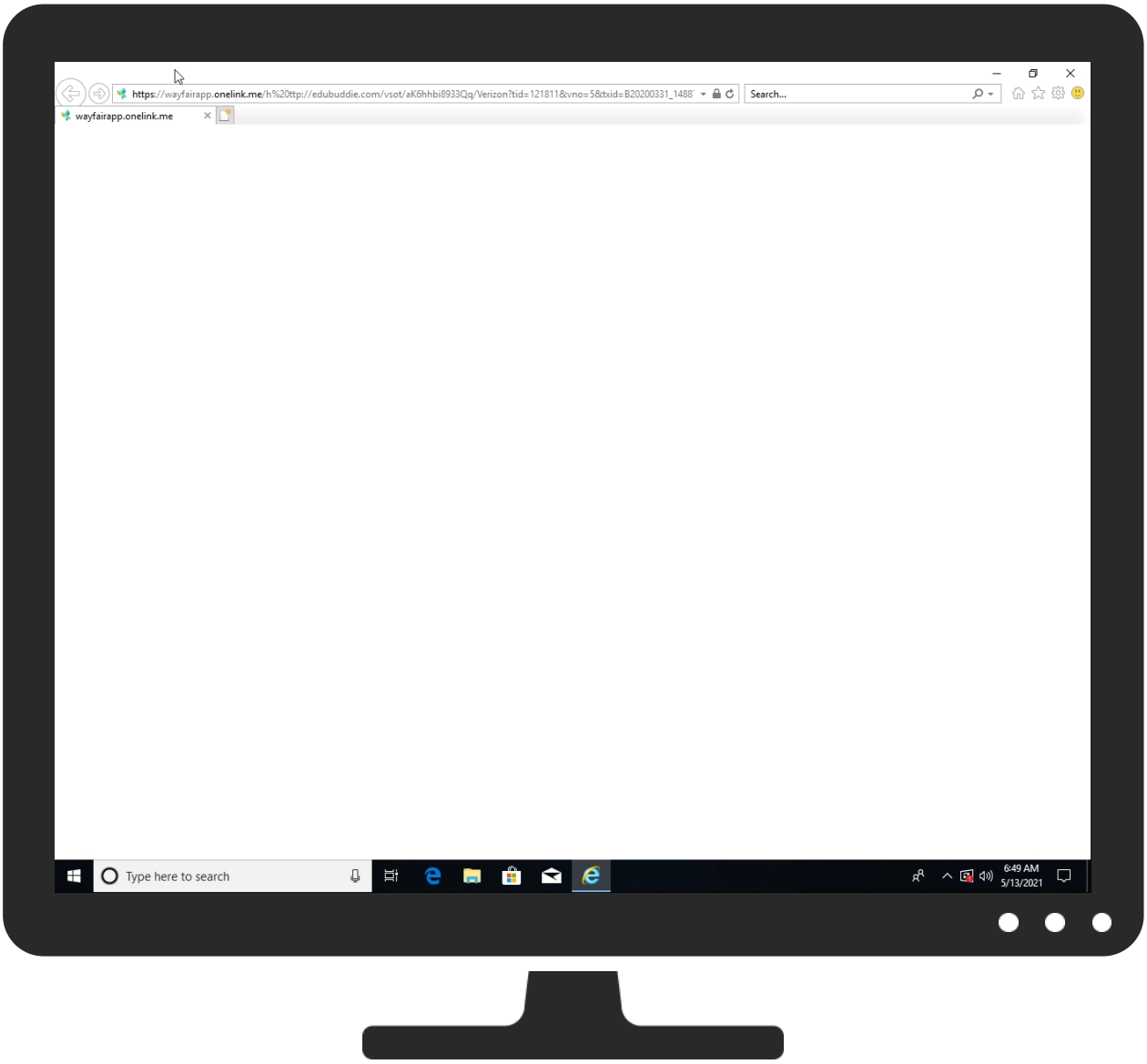


Screenshots

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://wayfairapp.onelink.me/2420802157?pid=Email&c=Triggered&af_sub5=AppEmailCA&af_dp=wayfairapp%3A%2F%2Fhome&af_web_dp=h%20ttp%3A%2F%2Fedubuddie.com/vsot/aK6hhbi8933Qq%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5<id=0	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wayfairapp.onelink.me	13.224.193.93	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://wayfairapp.onelink.me/h%20ttp://edubuddie.com/vsot/aK6hhbi8933Qq/Verizon?tid=121811&vno=5&txid=B20200331_1488798683&lid=18207&c=Triggered&pid=Email<id=0&af_sub5=AppEmailCA	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://https://wayfairapp.onelink.me/h%20ttp://edubuddie.com/vsot/aK6hhbi8933Qq/Verizon?tid=121811&vno=5&tx	~DF58651D31E836AEEB.TMP.1.dr, {F550CFD1-B3F1-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://https://wayfairapp.onelink.me/favicon.ico	imagestore.dat.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.193.93	wayfairapp.onelink.me	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413040
Start date:	13.05.2021
Start time:	06:47:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://wayfairapp.onelink.me/2420802157?pid=Email&c=Triggered&af_sub5=AppEmailCA&af_dp=wayfairapp%3A%2F%2Fhome&af_web_dp=h ttp%3A%2F%2Fedubuddie.com/vsot/aK6hhbi8933Qq%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5<id=0
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/17@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI

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:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F550CFCF-B3F1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8512180119540458
Encrypted:	false
SSDEEP:	48:Iwf0GcprCGwpL71G/ap87f6uGIpc7f6IaYGvnZpv7f6IalgGoJqp97f6IalzhGoF:rfoZqZl2TW4xt47f4gxM4iK404of4U8X
MD5:	628FEB61A9D423C3BD85440CD1D5A38C
SHA1:	77F9B67F543BA48D832ED158D1435F03ADCCE1AB
SHA-256:	97FFFF14A651DD2A31CA6A822D548C4334CA9D182DBA4043C21204AE0B18705E
SHA-512:	419C9816DAC4C6F25BCE83BCF4E182CBA4CE0420223C16A029BE2375AE9BDF8C648A92E74F898DE7122D95AB1B64ADCF1F11BBDEAEC6A7D65B894223FC3E35F5
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F550CFD1-B3F1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24472
Entropy (8bit):	1.691879243811193
Encrypted:	false
SSDEEP:	48:IwfGcpr6GwpaOG4pQlGrapbS+tGQpBSGHHpcHTGUp8/GzYpmE0GopQOgaJNvtT+u:r1ZiQu6VBSCjp2RWNMtSqttTMg
MD5:	DEAF001D72F101835B45984701FA3D52
SHA1:	6951FEF9B9E5B698ECFC300566B6CD08FC24AD20
SHA-256:	E467241E9B89B1C5FCB2B6F5E745162C11D8B6E1786988EDE2216C66D8F1FCD8
SHA-512:	CA929151FD54BCBCB19E6E499493A25A222771C6C9863AC0E9EE2851BBDF4DED53783EABAC7BF1A93A4F14407F71D04CDCED6F44D3AC267232E94EAE4BE01650
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F550CFD2-B3F1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.563049490150249
Encrypted:	false
SSDEEP:	48:Iw/Gcpr6GwpagG4pQUGrapbSu9GQpK9G7HpRHTGIpG:rVZiQA6iBSuHAcT1A
MD5:	E2EB97D8AF8436450E58A8F159596F17
SHA1:	F62BB30FBDD70C2CE25A88AC25663D4FA7815DBB

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F550CFD2-B3F1-11EB-90E4-ECF4BB862DED}.dat	
SHA-256:	31D2F8247BEA2F40B492AB5F3B52B1FC44A354752135A81F2878C42BA646AD21
SHA-512:	604BCA0D6C9AF1483A46674090E143435531B1BC9035D3404CA6BDB8B26ECE7D522E385172AF152767C37CB6B84531170AC84B4E17206836DBBE2E7E11060359
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.0840312005888455
Encrypted:	false
SSDEEP:	12:TMHdNMNxOECOfnWimI002EtM3MHdNMNxOECiKfnWimI00ObVbkEtMb:2d6NxOXOfSZHKd6NxOXrSZ76b
MD5:	4AABFD74208D86C0847B19B2E1B2916F
SHA1:	C736451EA0978ED05CFE2D1B14B97F32BE55008A
SHA-256:	AA9B5277144B9C61C3B22832157F8DE4EAEE09C7BC0C1C405F4841EC1D035520
SHA-512:	718264E0ABB8219431C516E30337227A3849E140667347B7A808F10F48FEB97D92EA9D37C86D19F5DC41C2242255012EFD095966AFE5077A95435611A1747666
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xcadd36b4,0x01d747fe</date><accdate>0xcadd36b4,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xcadd36b4,0x01d747fe</date><accdate>0xcadf98e6,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.078809430750294
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kGOyOfnWimI002EtM3MHdNMNxe2kGOyOfnWimI00Obkak6EtMb:2d6NxrqHfSZHKd6NxrqHfSZ7Aa7b
MD5:	7EBEC858BB5438F84536306CE1E0EE6C
SHA1:	2A9FBE6CCD3AE4FBB4630D68DEB2562A3BE7D4D5
SHA-256:	65A805F6F515A52841B17BA0C1F27E5833B7F53A1B7AF70073D6C84B0A0BA8A8
SHA-512:	484C3AEAAEC8D9CE38839905DD006EEEF305D5F00CFBE14083EF4C8E39F54323EF0F5C32227446E18836981CF435E9B497BCC63EF0AA787CE7291EE00624066
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xcad60fd4,0x01d747fe</date><accdate>0xcad60fd4,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xcad60fd4,0x01d747fe</date><accdate>0xcad60fd4,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.099436144903412
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLWKiKfnWimI002EtM3MHdNMNxvLWKiKfnWimI00ObmZEtMb:2d6NxvXSZHKd6NxvXSZ7mb
MD5:	799B191F993A905133F02E8D1F414B63
SHA1:	34B7FCA4C743A40AED9B428C3390CE0C72CF18E7
SHA-256:	6FE1F4305C17CD9ACC405AEC1A5256177564FCD9A3421192FC154FC377C7F42C
SHA-512:	1ECE211CF7F29178BFE3F26759E92D1883F67ABFBF85870CC3DA4A4B68CBFE3206076B3418F060D3D21291180EB7D57AFB2BC6D9B288B168C3D442E12C32E89
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xcadf98e6,0x01d747fe</date><accdate>0xcadf98e6,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xcadf98e6,0x01d747fe</date><accdate>0xcadf98e6,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.075167418904998
Encrypted:	false
SSDEEP:	12:TMHdNMNxiQUfnWimI002EtM3MHdNMNxiQUfnWimI00Obd5EtMb:2d6Nx6SZHKd6Nx6SZ7Jjb
MD5:	D99B30F7BAAA52A463AF96D78BD341E1
SHA1:	7BC1FA9B8C51CCDE0053C277A449D768683CA72A
SHA-256:	BF1C8029F0BB2DDFFF880BE6F65E98C5BB26A9857783F4E21D96C02EFDC2F51A
SHA-512:	0FBDECE92699FE9229218FD51B371D25A242F38A67CB7C0266E6949C378B697CB2C3ABAA9F7801018A1B25097F00BBCAED6D11E1FC30F40D9DA329AA47C1265
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xcadad446,0x01d747fe</date><accdate>0xcadad446,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xcadad446,0x01d747fe</date><accdate>0xcadad446,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.116218683260203
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwWKiKfnWimI002EtM3MHdNMNxhGwWKiKfnWimI00Ob8K075EtMb:2d6NxQ+SZHKd6NxQ+SZ7YKajb
MD5:	00278A67E93810E533865B08CB6F9037
SHA1:	DCFCBFF9E89C789DD5A9D0042AF0BA1C4D5E0E69
SHA-256:	48B01E0C71CD36E6C3785BE53FD312E7E0BA50DAC086EC8301E2F04571FC62EE
SHA-512:	A0EC5889DD3B599885AD584A705ADFC2660EA0A5F4C54CD24FAD872B578580318B0E0E7C3EF898E08513D888C1F9A4E5C45942E5E4BAC7CFB054D4BCB6D9A418
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xcadf98e6,0x01d747fe</date><accdate>0xcadf98e6,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xcadf98e6,0x01d747fe</date><accdate>0xcadf98e6,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.075650898107231
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nCOfnWimI002EtM3MHdNMNx0nCOfnWimI00ObxEtMb:2d6Nx0COfSZHKd6Nx0COfSZ7nb
MD5:	05F7DBC47263EAAD854C7A269E3539AB
SHA1:	D9EF064FA26FE47D4748C26BE0F674666E31E53C
SHA-256:	CA134F84EF30099ADDD5533B5681A72229AB5306FA65ADCA86999407A7A62781
SHA-512:	71602E878AC870A5BFA5F7E711F845687F4CBF7ABD8DF1B380C7C988400E2AC67B4A09431A21557D0A03FB5C994C8968029579FEAE26A0754F47A7257D39BD3D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xcadd36b4,0x01d747fe</date><accdate>0xcadd36b4,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xcadd36b4,0x01d747fe</date><accdate>0xcadd36b4,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.106051601666198
Encrypted:	false
SSDEEP:	12:TMHdNMNxxQUfnWimI002EtM3MHdNMNxxQOfnWimI00Ob6Kq5EtMb:2d6Nx3SZHKd6NxlfSZ7ob
MD5:	F6D96CA69473D2F9C74C96FECC51C690
SHA1:	F04B51D07173FCF5C49758923412BE840356347D
SHA-256:	D6420A24E94D542866ABCC617BE73375B794AE6A5C275123813668A731996DA8
SHA-512:	0FEA52A1AFAA359B1CC44E00739BE19C6662BF52E3B281AB833CBFD434244C3CCD084DFF0C330175811F3EE66F96245ECDCB5823B11C6AF1F9348C1DCBA4D2 58
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xcadad446,0x01d747fe</date> accdate>0xcadad446,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xcadad446,0x01d747fe</date><accdate>0 xcadd36b4,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.058605945360077
Encrypted:	false
SSDEEP:	12:TMHdNMNxcMm+Im+fnWimI002EtM3MHdNMNxcMm+Im+fnWimI00ObVEtMb:2d6Nx4SZHKd6Nx4SZ7Db
MD5:	8EB7F2AA2764B6A1C94BB7BEBD6AB0DB
SHA1:	6AAC2008452BDE92399C152E37E21077C6B1E208
SHA-256:	36A01B726990730E1A25896B5303F2C4F4F2F6659285638CFAB5E8681427AFA8
SHA-512:	ED230B17C6A2A4BB8255348DA3E5AEBF635375234EA531908D2C81C1DB931BF37DB3D01E910AA65A347D7703CC55FC8AB74CB7DFF9CA5AA4516502F95A80E8 E3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xcad871ef,0x01d747fe</date> <accdate>0xcad871ef,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xcad871ef,0x01d747fe</date><accdate >0xcad871ef,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.061161364152711
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnQUfnWimI002EtM3MHdNMNxfnQUfnWimI00Obe5EtMb:2d6NxlSZHKd6NxlSZ7ijb
MD5:	A0595AB440AC91C32EEF83F2C9BC669E
SHA1:	57D7EF83B7FA78297971FBBB0B3AFFA74FF29139
SHA-256:	3DA8D2FD9F3742256A0E1F5E971302399C7BD0B5B812A3B836A1B9A9DCC3679E
SHA-512:	BBA63C901BE52FBCDAFFD703FBFDC08550944C519E878FE7DBD90CCBCAF074053E3C192C786814AEECE6EB3BC03210B3B9CD10F0DE1DA4237ABD837969072 523
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xcadad446,0x01d747fe</date><a ccdate>0xcadad446,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xcadad446,0x01d747fe</date><accdate>0xc adad446,0x01d747fe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Size (bytes):	7264
Entropy (8bit):	7.936087329294195
Encrypted:	false
SSDEEP:	192:wAzHaIz1bToOSzDjBZmgehpIoFM+2ef3W945CP:Hz6IdTohDtgHXm+jU/P
MD5:	89AF961629EE1E49785094AF7370B328
SHA1:	CB33E528B90C30D32E742E10185953B1C82EB4EE
SHA-256:	7271F1204637449D3ADE76A48403F16D3B7E090F5C30002D87751ABA10EFBBDF
SHA-512:	5B2062F0D2C57CC91367AECA5594DBC0FD0DC5F656F6556025302F1D48CB7B3EE29EE35ED4D52CAB73FC9B371459C483DCC9E52BD6AF9BDBA53634805E08AD7
Malicious:	false
Reputation:	low
Preview:	).h.t.t.p.s.:./.w.a.y.f.a.i.r.a.p.p...o.n.e.l.i.n.k...m.e./.f.a.v.i.c.o.n...i.c.o.....PNG.....IHDR.....>a.....sBIT....|.d.....pHYs.....B(.x....tEXtSoftware.www.inkscape.org..<....eIDATx..y.$U.....Z.....^.i.g...=...a.f..A.....6....2c.....7.t+0= ..."..vAD.aDh.....*+3".y.DD..uwUfe?3.....w.=...7EU.}aZ..Z.....9:.hst.....!@..ku.~.p.....o.E./..G..s.lnu.v..I.....#'H.U.0..j06G..}.[...3.....Z....,..z,...w.C...+Z.]A.....]V...y.]Fp..xn.....O.....t.X..b...O..s.=..+(.(Na..!g...o.:.`.X.~.....X.e...7(..&$P.9./.<.vh.....}.....X..P.o.....8M..4i....|C....-....`7 .....,_.....;....*....w.m/w...S.C....h.?.X.....T.S._%....9...._..O...v.+..~y ..{.F..h&...R....=...>,k..Z..).!..`.....Xr.T.>U...H..t..ZrF.....``X.a.HO.-+.<;.78.....?..q.3.(.s.Q../>.k..L.....[.3....t/.L.....8..a!}..[D8...;Zy?..C.)p.=.]...9`E.A.:o_k4?....U...!..r.&..76...L.R0./=.G...U...P.Z.:..R..2_!V.....(,Z..;.G...`...Xy.a=..TR.q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	7144
Entropy (8bit):	7.952897954730649
Encrypted:	false
SSDEEP:	192:7AzHaIz1bToOSzDjBZmgehpIoFM+2ef3W945CI:cz6IdTohDtgHXm+jU/I
MD5:	935E549F78D4869919DE63FEDFB6CC2F
SHA1:	119EBEA10A83F8F79736AF274195DECC8CF545FD
SHA-256:	35B0EBD3A369DB1384E012E2770AEE7E4EEDC1E1B9D5F968E2E4BAEBDF02E06B
SHA-512:	84FDE326321AAABFC5927CC6EC7F5F0A0691A00DB70B1129C9B801E6EFB72DFFF7B3459C86EEAB20DD4C8B08B179C1862A8310C457009DACD2F0BA1D1F3B530
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....>a.....sBIT....|.d.....pHYs.....B(.x....tEXtSoftware.www.inkscape.org..<....eIDATx..y.$U.....Z.....^.i.g...=...a.f..A.....6....2c.....7.t+0= ..."..vAD.aDh.....*+3".y.DD..uwUfe?3.....w.=...7EU.}aZ..Z.....9:.hst.....!@..ku.~.p.....o.E./..G..s.lnu.v..I.....#'H.U.0..j06G..}.[...3.....Z....,..z,...w.C...+Z.]A.....]V...y.]Fp..xn.....O.....t.X..b...O..s.=..+(.(Na..!g...o.:.`.X.~.....X.e...7(..&$P.9./.<.vh.....}.....X..P.o.....8M..4i....|C....-....`7 .....,_.....;....*....w.m/w...S.C....h.?.X.....T.S._%....9...._..O...v.+..~y ..{.F..h&...R....=...>,k..Z..).!..`.....Xr.T.>U...H..t..ZrF.....``X.a.HO.-+.<;.78.....?..q.3.(.s.Q../>.k..L.....[.3....t/.L.....8..a!}..[D8...;Zy?..C.)p.=.]...9`E.A.:o_k4?....U...!..r.&..76...L.R0./=.G...U...P.Z.:..R..2_!V.....(,Z..;.G...`...Xy.a=..TR.q..J..g.... I.... .|.....{.4|.....c.Iul...V.....q.A.#.e.p@.7.p .=wA.....`..v.

C:\Users\user\AppData\Local\Temp\~DF4ADEF8CDE444C23C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47865376751456606
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo73F9lo7V9lW7f6IalzIaAiyaAgezeq:kBqoI7+7g7f6IalzIaAiyaAgezeq
MD5:	294560C42A25D73D8658DFE6D8AD6711
SHA1:	25097A86A70C2803EF46CFD6DD374EAFC781A9E1
SHA-256:	A7F97B08F2BB9655536D2B1BDFBA256CF74953EFC251AAE5EA897E1DB070EBC8
SHA-512:	AD36B7B35DD04B467B6493D44CF97C3C771053FA5C3A9E26AF6614F04F2B092967221269CE49C4647A12CDD0D1BD02553250198D53E74DDBEBF1D45C8A80A25
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF52B391DAC9B7D700.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A

C:\Users\user\AppData\Local\Temp\~DF52B391DAC9B7D700.TMP	
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF58651D31E836AEEB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34665
Entropy (8bit):	0.40404700735574184
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+V75oEIEuOgaJNvtT+eqs:kBqoxKAuvScS+V75orBqttTt
MD5:	70AA16D16E7368B286BC76018EEED9F8
SHA1:	9B7803D05F1839E500519364EFCED70481F2BDF4
SHA-256:	5F669F8F1FF9C264E50B407604E4844E0A77E07AE1F0B56DD077D56130673A82
SHA-512:	2291CFFE2510602A2174E12F7C9DD153FF5B9F8A450C0472ED40D5588C737EEB2DB78942D3A0F2D3372D6CCEDECFF257F3425F81AD89796E3422AED6C28C9A
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 82

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:48:57.793637991 CEST	49684	443	192.168.2.3	13.224.193.93

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:48:57.793900967 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.834850073 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.834932089 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.834945917 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.834997892 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.842094898 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.842412949 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.847992897 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.848109961 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.849713087 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.849839926 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.884957075 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.884983063 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.885072947 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.885092974 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.885112047 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.885129929 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.885139942 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.885152102 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.885174036 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.885185957 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.885209084 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.885247946 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.885905027 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.887037039 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.887115002 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.894499063 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.894577026 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.937648058 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.940110922 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.947182894 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.947350979 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.947514057 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.979096889 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.979127884 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.979147911 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.979249954 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.980842113 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.981657982 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.981682062 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.981699944 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.981770992 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.981805086 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.982600927 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.988445044 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.988668919 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.988740921 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:57.988986015 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.989018917 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:57.989092112 CEST	49684	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:58.016321898 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.016422033 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:58.020843983 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:58.022389889 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.023737907 CEST	443	49684	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.064194918 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.163208961 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.163330078 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:58.401702881 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:58.444298983 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.537306070 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.537353992 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.537450075 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.537492990 CEST	443	49685	13.224.193.93	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:48:58.537513018 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:58.537566900 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:58.538615942 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.538670063 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.538746119 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:58.538796902 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:48:58.539735079 CEST	443	49685	13.224.193.93	192.168.2.3
May 13, 2021 06:48:58.539836884 CEST	49685	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.429631948 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.472372055 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.472500086 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.478219986 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.483669996 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.483767033 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.519382000 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.519474030 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.519500017 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.519521952 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.519536972 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.519584894 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.521694899 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.521794081 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.530239105 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.573057890 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.573085070 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.573177099 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.577127934 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.618252039 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.685659885 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.685717106 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.685738087 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.685851097 CEST	49693	443	192.168.2.3	13.224.193.93
May 13, 2021 06:49:14.685870886 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.685914040 CEST	443	49693	13.224.193.93	192.168.2.3
May 13, 2021 06:49:14.685925007 CEST	49693	443	192.168.2.3	13.224.193.93

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:48:50.850625992 CEST	54260	53	192.168.2.3	8.8.8.8
May 13, 2021 06:48:50.900738955 CEST	53	54260	8.8.8.8	192.168.2.3
May 13, 2021 06:48:51.785048962 CEST	51904	53	192.168.2.3	8.8.8.8
May 13, 2021 06:48:51.836766005 CEST	53	51904	8.8.8.8	192.168.2.3
May 13, 2021 06:48:52.712727070 CEST	61328	53	192.168.2.3	8.8.8.8
May 13, 2021 06:48:52.761281967 CEST	53	61328	8.8.8.8	192.168.2.3
May 13, 2021 06:48:53.678791046 CEST	54130	53	192.168.2.3	8.8.8.8
May 13, 2021 06:48:53.731203079 CEST	53	54130	8.8.8.8	192.168.2.3
May 13, 2021 06:48:54.925029039 CEST	56961	53	192.168.2.3	8.8.8.8
May 13, 2021 06:48:54.984932899 CEST	53	56961	8.8.8.8	192.168.2.3
May 13, 2021 06:48:56.542867899 CEST	59353	53	192.168.2.3	8.8.8.8
May 13, 2021 06:48:56.599987030 CEST	53	59353	8.8.8.8	192.168.2.3
May 13, 2021 06:48:57.717732906 CEST	52238	53	192.168.2.3	8.8.8.8
May 13, 2021 06:48:57.782128096 CEST	53	52238	8.8.8.8	192.168.2.3
May 13, 2021 06:49:03.864171982 CEST	49873	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:03.915791035 CEST	53	49873	8.8.8.8	192.168.2.3
May 13, 2021 06:49:04.915522099 CEST	53196	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:04.964524031 CEST	53	53196	8.8.8.8	192.168.2.3
May 13, 2021 06:49:06.348589897 CEST	56777	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:06.397373915 CEST	53	56777	8.8.8.8	192.168.2.3
May 13, 2021 06:49:07.266315937 CEST	58643	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:07.315284014 CEST	53	58643	8.8.8.8	192.168.2.3
May 13, 2021 06:49:08.199542999 CEST	60985	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:08.248311996 CEST	53	60985	8.8.8.8	192.168.2.3
May 13, 2021 06:49:09.082907915 CEST	50200	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:49:09.133197069 CEST	53	50200	8.8.8.8	192.168.2.3
May 13, 2021 06:49:10.193173885 CEST	51281	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:10.253154039 CEST	53	51281	8.8.8.8	192.168.2.3
May 13, 2021 06:49:14.369575024 CEST	49199	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:14.426666021 CEST	53	49199	8.8.8.8	192.168.2.3
May 13, 2021 06:49:14.553080082 CEST	50620	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:14.613209963 CEST	53	50620	8.8.8.8	192.168.2.3
May 13, 2021 06:49:15.464420080 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:15.518747091 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 06:49:16.366929054 CEST	60152	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:16.421466112 CEST	53	60152	8.8.8.8	192.168.2.3
May 13, 2021 06:49:17.518594027 CEST	57544	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:17.570329905 CEST	53	57544	8.8.8.8	192.168.2.3
May 13, 2021 06:49:18.865534067 CEST	55984	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:18.917100906 CEST	53	55984	8.8.8.8	192.168.2.3
May 13, 2021 06:49:20.928606033 CEST	64185	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:20.977300882 CEST	53	64185	8.8.8.8	192.168.2.3
May 13, 2021 06:49:21.833398104 CEST	65110	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:21.882286072 CEST	53	65110	8.8.8.8	192.168.2.3
May 13, 2021 06:49:23.145522118 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:23.291203976 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 06:49:26.563096046 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:26.614417076 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 06:49:27.263041019 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:27.320123911 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 06:49:27.590069056 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:27.639148951 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 06:49:28.252136946 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:28.300885916 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 06:49:28.581167936 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:28.631649971 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 06:49:29.267283916 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:29.327899933 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 06:49:30.595799923 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:30.644458055 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 06:49:31.283065081 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:31.340188026 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 06:49:34.611471891 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:34.668358088 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 06:49:35.283421040 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 06:49:35.333653927 CEST	53	60831	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2021 06:48:57.717732906 CEST	192.168.2.3	8.8.8.8	0x8318	Standard query (0)	wayfairapp .onelink.me	A (IP address)	IN (0x0001)
May 13, 2021 06:49:14.369575024 CEST	192.168.2.3	8.8.8.8	0xb32	Standard query (0)	wayfairapp .onelink.me	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 06:48:57.782128096 CEST	8.8.8.8	192.168.2.3	0x8318	No error (0)	wayfairapp .onelink.me		13.224.193.93	A (IP address)	IN (0x0001)
May 13, 2021 06:48:57.782128096 CEST	8.8.8.8	192.168.2.3	0x8318	No error (0)	wayfairapp .onelink.me		13.224.193.53	A (IP address)	IN (0x0001)
May 13, 2021 06:48:57.782128096 CEST	8.8.8.8	192.168.2.3	0x8318	No error (0)	wayfairapp .onelink.me		13.224.193.39	A (IP address)	IN (0x0001)
May 13, 2021 06:48:57.782128096 CEST	8.8.8.8	192.168.2.3	0x8318	No error (0)	wayfairapp .onelink.me		13.224.193.23	A (IP address)	IN (0x0001)
May 13, 2021 06:49:14.426666021 CEST	8.8.8.8	192.168.2.3	0xb32	No error (0)	wayfairapp .onelink.me		13.224.193.93	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 06:49:14.426666021 CEST	8.8.8.8	192.168.2.3	0xb32	No error (0)	wayfairapp .onelink.me		13.224.193.53	A (IP address)	IN (0x0001)
May 13, 2021 06:49:14.426666021 CEST	8.8.8.8	192.168.2.3	0xb32	No error (0)	wayfairapp .onelink.me		13.224.193.39	A (IP address)	IN (0x0001)
May 13, 2021 06:49:14.426666021 CEST	8.8.8.8	192.168.2.3	0xb32	No error (0)	wayfairapp .onelink.me		13.224.193.23	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
May 13, 2021 06:48:57.887037039 CEST	13.224.193.93	443	192.168.2.3	49685	CN=*.onelink.me CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Sep 03 02:00:00 CEST 2020	Sun Oct 03 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 13, 2021 06:48:57.894499063 CEST	13.224.193.93	443	192.168.2.3	49684	CN=*.onelink.me CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Sep 03 02:00:00 CEST 2020	Sun Oct 03 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 13, 2021 06:49:14.521694899 CEST	13.224.193.93	443	192.168.2.3	49693	CN=*.onelink.me CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Sep 03 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun Oct 03 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5836 Parent PID: 792

General

Start time:	06:48:55
Start date:	13/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff72a640000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
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

File Path	Offset	Length	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: iexplore.exe PID: 5888 Parent PID: 5836

General

Start time:	06:48:56
Start date:	13/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5836 CREDAT:17410 /prefetch:2
Imagebase:	0xc70000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly