ID: 358595
Cookbook: browseurl.jbs
Time: 22:04:38
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

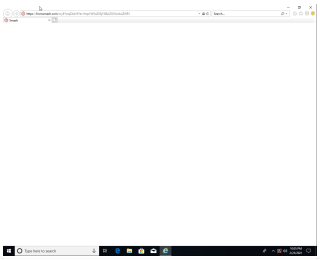
Analysis Report https://fromsmash.com/rcyEYwqZAd-ft…

Overview

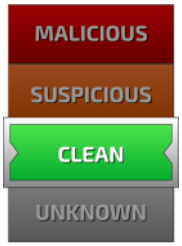
General Information

Sample URL:	http://https://fromsmash.com/rcyEYwqZAd-ft?e=YnJpYW5uZS5jYXBAZGV2cnkuZWR1
Analysis ID:	358595
Infos:	

Most interesting Screenshot:



Detection

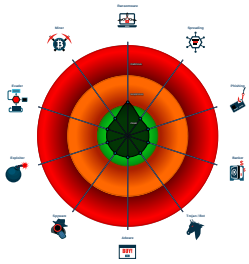


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5620 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5816 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5620 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

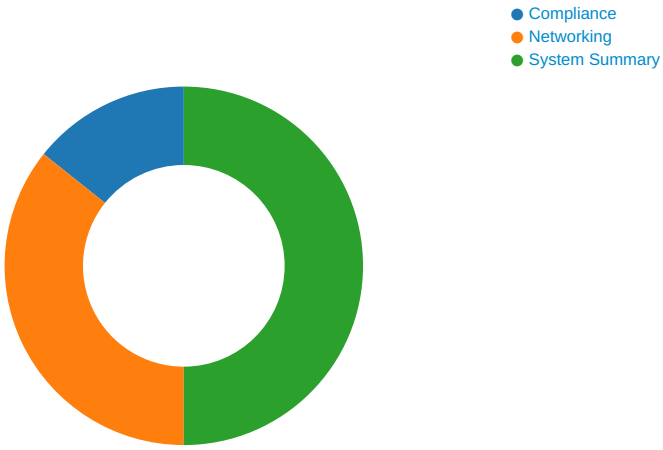
Yara Overview

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.

Compliance:

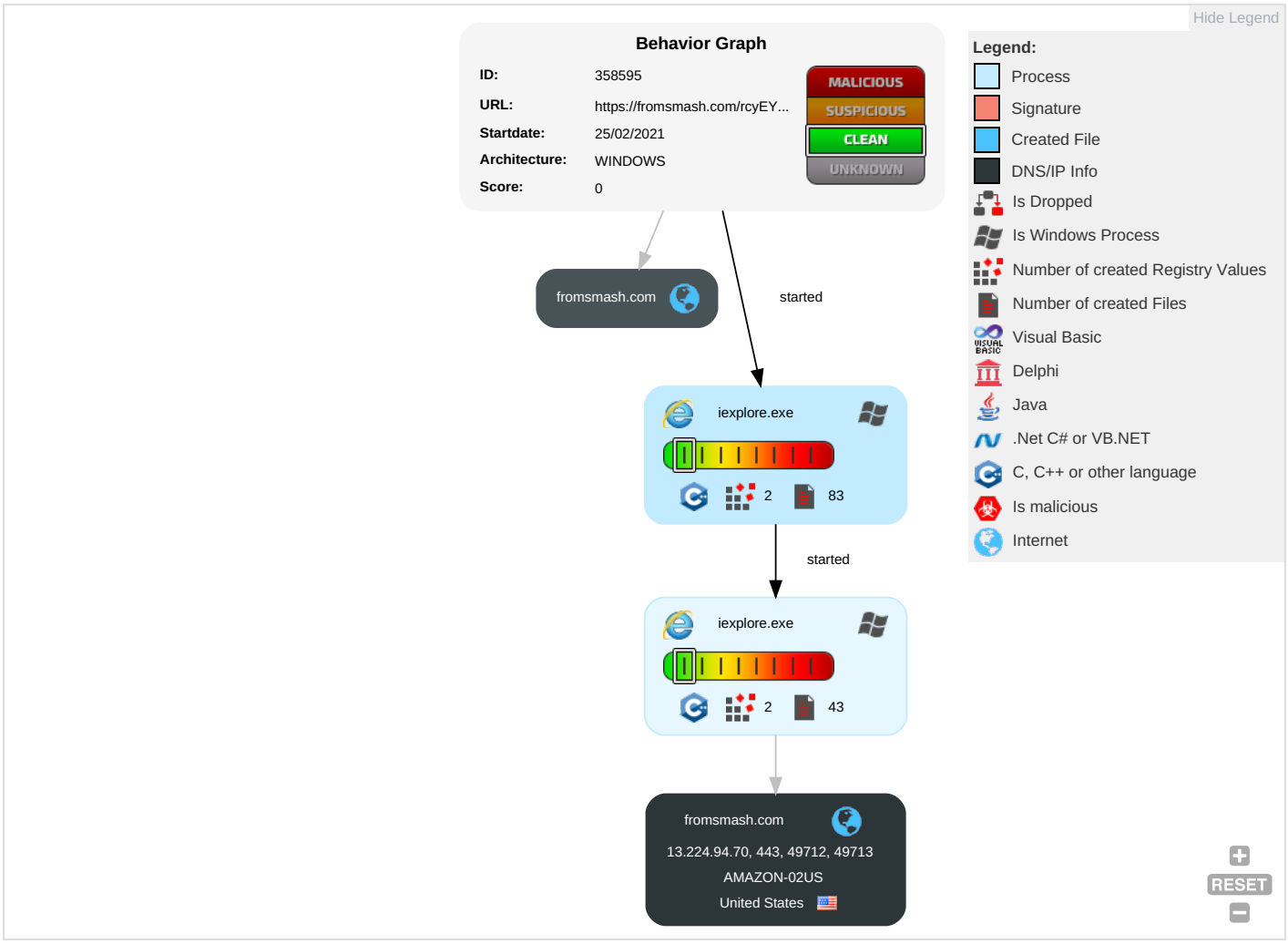
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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

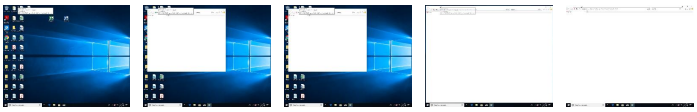
Behavior Graph

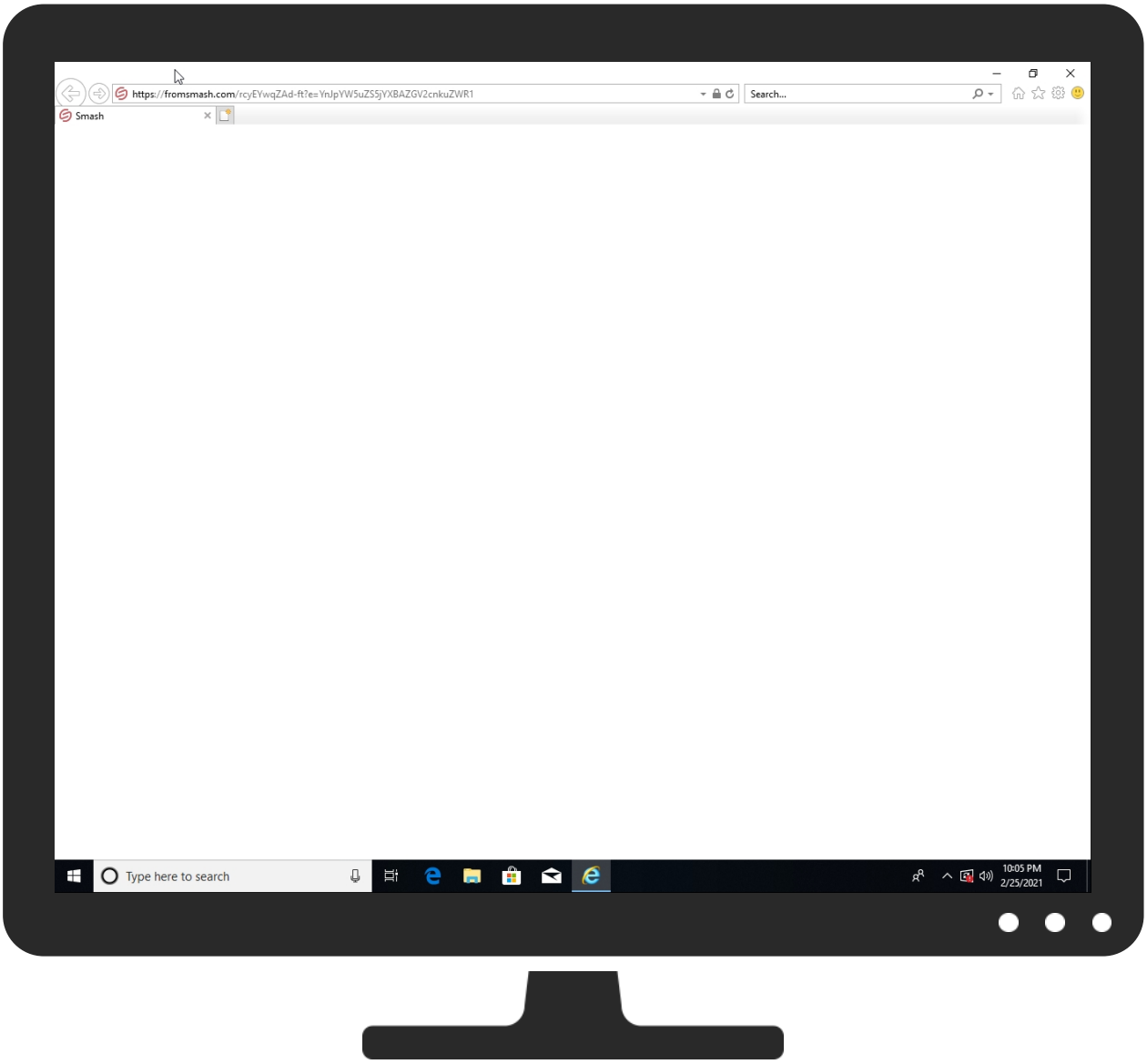


Screenshots

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://fromsmash.com/rcyEYwqZAd-ft?e=YnJpYW5uZS5jYXBAZGV2cnkuZWR1	0%	Virustotal		Browse
http://https://fromsmash.com/rcyEYwqZAd-ft?e=YnJpYW5uZS5jYXBAZGV2cnkuZWR1	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	
http://www.wikipedia.com/	0%	URL Reputation	safe	

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fromsmash.com	13.224.94.70	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://fromsmash.com/rcyEYwqZAd-ft?e=YnJpYW5uZS5jYXBAZGV2cnkuZWR1	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://fromsmash.com/rcyEYwqZAd-ft?e=YnJpYW5uZS5jYXBAZGV2cnkuZWR1	~DFC680C543889275C2.TMP.1.dr	false		high
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://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://https://fromsmash.com/assets/img/smash-logo/png/icono-no-chip-red.png	imagestore.dat.3.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://https://www.youtube.com/player_api	rcyEYwqZAd-ft[1].htm.3.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
http://https://fromsmash.com/rcyEYwqZAd-ft?e=YnJpYW5uZS5jYXBAZGV2cnkuZWR1Root	{9D388144-77F8-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.94.70	unknown	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358595
Start date:	25.02.2021
Start time:	22:04:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://fromsmash.com/rcyEYwqZAd-ft?e=YnJpYW5uZS5jYXBAZGV2cnkuZWR1
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:	16
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@3/26@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.42.151.234, 104.43.139.144, 13.64.90.137, 88.221.62.148, 52.255.188.83, 216.58.208.170, 216.58.198.3, 168.61.161.212, 51.11.168.160, 184.30.20.56, 152.199.19.161 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, arc.msn.com.nsatc.net, fs.microsoft.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net

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.{9D388142-77F8-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8561966175300448
Encrypted:	false
SSDEEP:	192:rOZFTZ02yWNtlcf1zv3ZMHffnQFt/yfpvSJX:raTjx3lit3iHffQFt/wVSx
MD5:	E55D311F75176A8BEA364C045B335D9C
SHA1:	DAC17DF16411B2888626D86C2BB83F41D9ADE410
SHA-256:	66D35E53234798A37786D93E79BAC5B929D3980664C9FCEBA2018836805C6B0E
SHA-512:	E63EDBAD8E1BFFCB6B7D58B4B18A597815B6B6797372A3352E3648F8C8C484638F09DA8D5F788015174896F62BE3C8E49E0847B8D757D9284056518632C2F437
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\{9D388144-77F8-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24244
Entropy (8bit):	1.64363678749567
Encrypted:	false
SSDEEP:	48:IwDGcpruZGwpasG4pQ4GrapbSJGQpBCGHHpcrTGUp8cgGzYpm7p7GopT1RF1fUsW:r5ZuTQs6GBSDjZ2FWcUMtdnZg

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D388144-77F8-11EB-90E4-ECF4BB862DED}.dat	
MD5:	1781A95AD64057990D4C0091DD77018D
SHA1:	8024926E26E9C8DF133750B23BC61B9D6B6DCDBE
SHA-256:	52A5162C22000176B1606275F85DBD28EA8A93E334038A8948F3B1BE0AAAC9A5
SHA-512:	6695A1D356CDFF583ECE0CADED1F6DB691607A38AA6DAF39DC7BBBC414FA277076DD4F0966779DEE51F8837912E928188172276FC355BA37538013E536F290A
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\{9D388145-77F8-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5638546132380575
Encrypted:	false
SSDEEP:	48:IwBGcpr4ZGwpa5G4pQxGrapbSOGQpKVG7HpRiTGIpG:r3Z4TQb6BBSGAET2A
MD5:	11E9AA00E36335F0E7A0DD531AC7861E
SHA1:	9EC01DEAF02EA18CD10444CFB564B6119EAFD177
SHA-256:	20FD0F977D220ED7052D4E514C1A8D9BA5614C20DCD14C4231C35F0702C5D42C
SHA-512:	2D23589A7614BA5553E39BC5A768B3F988683DDB493C0C848554493CBBB042B955F63A30C2D45FBC95912E4744FCE7728CBB4BB142DC0C287AE86C0A9C420C9
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):	5.07232994145172
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEIKJnWimI002EtM3MHdNMNxOEIKJnWimI00ObVbkEtMb:2d6NxOESZHKd6NxOESZ76b
MD5:	0008A3F98DB20F82F794FF5FDADFF8AC
SHA1:	BBAD368788D7BF0ABBAAFE8256F78D9ECD7A1665
SHA-256:	91457D0E7E04E5A563D6A0048920D2D29B13D76006FBA8D8550E2C7987A2BD7F
SHA-512:	DD83CE4224C72F4A4820B81D551AFC8DB2FA9F3B426D80C98985B5E140E9E73DDE4FDD6B8A7CC82ED38E1A4B15424EBE23D07D73F60E3411E339C382823221B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x73d8c985,0x01d70c05</date><accdate>0x73d8c985,0x01d70c05</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>0x73d8c985,0x01d70c05</date><accdate>0x73d8c985,0x01d70c05</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):	5.088246605722141
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kX5CN5CJnWimI002EtM3MHdNMNxe2kX5CN5CJnWimI00Obkak6EtMb:2d6Nxre5e52SZHKd6Nxre5e52SZ7Aa7b
MD5:	741A2955B4B445D7ACD121DEBE2AA1B3
SHA1:	709A0A06396BC196AC793D2F98AB179A2BC87349
SHA-256:	29F96CC1131D909C118A1F71D261AF6DADD24B79801BDCE0F77026E0BB8948AD
SHA-512:	B75E249D61589432AE82DCC4CA0B747C96CCEC0D56DE52C96CDEFAC27698BCC60C5DFF6DB0705A874BA2F7C9EDB40387C4ED54E9F467E77B7412310D63DCDD6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x73d404b7,0x01d70c05</date><accdate>0x73d404b7,0x01d70c05</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>0x73d404b7,0x01d70c05</date><accdate>0x73d404b7,0x01d70c05</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):	5.0723119758330215
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLQs2sJnWimI002EtM3MHdNMNxvLQs2sJnWimI00ObmZEtMb:2d6NxvjSZHKd6NxvjSZ7mb
MD5:	BCDE6D9CFFF7B4D1355A301E2C2E8A59
SHA1:	F5C3BF9944C2069B3FC2D2CFFA3014F4ACF8DA83
SHA-256:	37208289876950511A7AF9F11B2F2A4BEC87326FD353C31D5D5DBCF71ED21B6B
SHA-512:	C5AA9BD5BBD89016571A79BEE79E296769E46CA4B822A9E90EE474A3985DAA88F0A26194872060E909CD6DBDC9C1DEF39FF2A78555723CF6A55C04B1EAC9B87A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x73db2bce,0x01d70c05</date><accdate>0x73db2bce,0x01d70c05</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>0x73db2bce,0x01d70c05</date><accdate>0x73db2bce,0x01d70c05</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):	5.094641669690258
Encrypted:	false
SSDEEP:	12:TMHdNMNxi7X89X8JnWimI002EtM3MHdNMNxi7X8KJnWimI00Obd5EtMb:2d6NxMX4XISZHKd6NxMX5SZ7Jjb
MD5:	736B8C39D6F20F76BAE6D19FBC9A1B05
SHA1:	C9D0083DF7DADD0DB6C587BF8799FF71DB5B74B4
SHA-256:	165C57BBAFB89CF1851442A3579F81EABA3D95B0622ED30735360EF370B539E2
SHA-512:	6793823373310BF6E6E1CA97031BC2725F39E8D0387F4DFE1FCD15708ECD8001E294BEA1F41C62C5D9C4F9B0EA60587BADEBFC465AE6D4FCFED6D54F1DEAED6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x73d66733,0x01d70c05</date><accdate>0x73d66733,0x01d70c05</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>0x73d66733,0x01d70c05</date><accdate>0x73d8c985,0x01d70c05</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):	5.081984811207846
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwQs2sJnWimI002EtM3MHdNMNxhGwQs2sJnWimI00Ob8K075EtMb:2d6NxQqSZHKd6NxQqSZ7YKajb
MD5:	2ECDC2054A09EED430FC80C00FBA6C3A
SHA1:	B52E835AFB0F33D1CBC307C0BE6A0F2D98BA5546
SHA-256:	58214691FC61374D589737FF0951EB264DC00122CF088C096E3B53BE06932F89
SHA-512:	54D381135B110809970AF28196E1E20283ED2789D45538EA8B512C0E8ACA463A0584BEC4CA279228AE93D3CF3F6EDF205E6322B7DF378D06FE002E0A9A340C41
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x73db2bce,0x01d70c05</date><accdate>0x73db2bce,0x01d70c05</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>0x73db2bce,0x01d70c05</date><accdate>0x73db2bce,0x01d70c05</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):	5.072967407088777
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nIKJnWimI002EtM3MHdNMNx0nIKJnWimI00ObxEtMb:2d6Nx09SZHKd6Nx09SZ7nb
MD5:	9362862F42719025AB233A9ECE032E3D
SHA1:	6ED5DC6611A2050C4881E38DDB2C3A5CE3643BA6
SHA-256:	3611E9514591AEC238EAC64422084E7228F89CBD6CFED8B91713AD473F399866
SHA-512:	FEB5EBE3C6FEE3B62B35F83068300C053F44D07D6B924910B03D5630945183DFCF4534B49CF10E63F387058322DBEA08078EA36FBD3E94075A2982D9EBFAD305
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x73d8c985,0x01d70c05</date><accdate>0x73d8c985,0x01d70c05</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>0x73d8c985,0x01d70c05</date><accdate>0x73d8c985,0x01d70c05</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):	5.112753642722416
Encrypted:	false
SSDEEP:	12:TMHdNMNxxIKJnWimI002EtM3MHdNMNxxIKJnWimI00Ob6Kq5EtMb:2d6NxXSZHKd6NxXSZ7ob
MD5:	BBCE137B9EC0CD23086E186CF9982B98
SHA1:	528972E8F6550C70DB063EC8CB62EE2A6045CC62
SHA-256:	ECBC5E80DECE3A2ECB680BCE3A83B99D69959973CF7663A88DE89C3571F95B30
SHA-512:	397C46F3A024ABED0BBE30E6D8BE4482006DEF98C08451D6FA6407ED180FA5F33598D89030FB2BE95966A82196CA57B44E02D0DA9A44FBF87A381DD4D1AE2E8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x73d8c985,0x01d70c05</date><accdate>0x73d8c985,0x01d70c05</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>0x73d8c985,0x01d70c05</date><accdate>0x73d8c985,0x01d70c05</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):	5.08720695536865
Encrypted:	false
SSDEEP:	12:TMHdNMNxc7X89X8JnWimI002EtM3MHdNMNxc7X89X8JnWimI00ObVEtMb:2d6NxCX4XISZHKd6NxCX4XISZ7Db
MD5:	668DB328A99F54FDAB4A6A92CE34E47F
SHA1:	E042A0E2E297403F00CF8ABE5F61722FAA5D554F
SHA-256:	41E7CD65D2B958453916449A60CD29001516ADDA466E3D14F8534E417173A342
SHA-512:	75CCB6CD0A5AF975C1BEADBFE36E4BE98D5632032AA728B57C5E1B537D7340549A3185D4255F46FBBE37973B1A82DF9DFC8534650DE32CA537B4F6C660E019A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x73d66733,0x01d70c05</date><accdate>0x73d66733,0x01d70c05</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>0x73d66733,0x01d70c05</date><accdate>0x73d66733,0x01d70c05</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Entropy (8bit):	5.06761763980147
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn7X89X8JnWimI002EtM3MHdNMNxfn7X89X8JnWimI00Obe5EtMb:2d6NxTX4XISZHKd6NxTX4XISZ7ijb
MD5:	FA536C3F4F820B10E6D4574BB1653DF1
SHA1:	F65382358AEB8D156A66C52DA7E6F59E3F2342E6
SHA-256:	F426F43DF797E59AB01D328B92864E5E0E0B6C9582EE807C2850CC199F07F29B
SHA-512:	B750D0C3AA4DF35F5D497B4475C8E70C6CFF5CDDA4E90E931723D9B176F9F86DC1EAE109D5A75377E41C67B7BE981067DCC5EC36C8EE59633A7506638D2EE C4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x73d66733,0x01d70c05</date><a ccdate>0x73d66733,0x01d70c05</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>0x73d66733,0x01d70c05</date><a ccdate>0x73d66733,0x01d70c05</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.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
Size (bytes):	19109
Entropy (8bit):	7.924140999280492
Encrypted:	false
SSDEEP:	384:W7+F4fmZLgrCsy4YXBpN6MU/SAT2B5ahHaWe8k7qph36/eoM2KSl:PwgLtsCp6MU/haBAh6We8fr3JSl
MD5:	3A7A0F9854824308BA9A508108871E27
SHA1:	553AB226C151CC9AF1A1F14527D47FF9B548220C
SHA-256:	46FDDB0B8582D69268E64374E4B6701453A4D787430256CE58E96887F8272195
SHA-512:	3E6996AF94EC78954B1CC17BDACF010D07762476D11F5B3F61DA92AB8FDBDAA3FDB46F85886F8A56BF6BA86D7B3A3BF0EAB03480C21D56D768A004A30D088E 6A
Malicious:	false
Reputation:	low
Preview:	E.h.t.t.p.s.:./.f.r.o.m.s.m.a.s.h...c.o.m./.a.s.s.e.t.s./.i.m.g./.s.m.a.s.h.-.l.o.g.o./.p.n.g./.i.c.o.n.o.-.n.o.-.c.h.i.p.-.r.e.d...p.n.g..I...PNG.....IHDR..... .]....tEXtSoftw are.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk= "Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:Creato rTool="Adobe Photoshop CC 2019 (Macintosh)" xmpMM:InstanceID="xmp.iid:B758C8EFD25511E9996A8C26DEE2D98A" xmpMM:DocumentID="xmp.did:B758C8F0D2 5511E9996A8C26DEE2D98A"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:B758C8EDD25511E9996A8C26DEE2D98A" stRef:documentID="xmp.did: B758C8EED25511E9996A8C26DEE2D98A"/> </rdf:Description> </rdf:RDF> </

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icono-no-chip-red[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 488 x 498, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18933
Entropy (8bit):	7.935662674511279
Encrypted:	false
SSDEEP:	384:yF4fmZLgrCsy4YXBpN6MU/SAT2B5ahHaWe8k7qph36/eoM2KSY:kwgLtsCp6MU/haBAh6We8fr3JSY
MD5:	2B6082CBA10E16C1049B5A870FE6BD21
SHA1:	96D0CC245BD57894894543F6C3E38693FBBF6EC9
SHA-256:	48524145EB1172CE973951FDE2501E2C3181E6C34ACF6524083ED6DA619BC3A2
SHA-512:	A3A19DF0C42D41318B891702F0A1CBCBAD31A9A3D0D6CBEB7FE21ADDE5C7F451BEF1101767FA464EEF5139B89429B5987625F11F7DDCFDCE5B29EB4F1F3BC D42
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fromsmash.com/assets/img/smash-logo/png/icono-no-chip-red.png
Preview:	.PNG.....IHDR..... .]....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpme ta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/08/13-16:40:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax- ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xa p/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2019 (Macintosh)" xmpMM:InstanceID="xmp.iid:B758C8EFD25511E9996A8C26DEE2D98A" xmpMM:DocumentID="xmp.did:B758C8F0D25511E9996A8C26DEE2D98A"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:B758C8EDD25511E9996A8C26 DEE2D98A" stRef:documentID="xmp.did:B758C8EED25511E9996A8C26DEE2D98A"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>..E...FcIDATx... .U...g.Q...PQ.+.T.C.-v..l11Q.Ml1&....).X.....Q...hP...`.".@.....3+..w.{.93.....{.}S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\runtime.970dd264cf5d1fad178c[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3402

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\runtime.970dd264cf5d1fad178c[1].js	
Entropy (8bit):	5.423086516692374
Encrypted:	false
SSDEEP:	96:EzDPLsj4IerVml71O7Fz6OgeYFxcAsa503kjWX6J:ELs0IwA7E7dYrcZC0J6J
MD5:	2B557569E774EC5583E40B2D96E63B28
SHA1:	E5B0C2DEA6CE16FFCD9AC17E98BC6FC05B26D6F9
SHA-256:	FABF0AB33B1F8B465FE8E85F647F804283084A6DADF0926370B9EABF764D777C
SHA-512:	C8B460944EDFE850B8432809B19792525F184B9CAF3F80D3C9A063C3D647042F80430DE20904E993A9170FB9A0A58EE7272BF9A523F0A0F6509E32390EBE25A8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fromsmash.com/runtime.970dd264cf5d1fad178c.js
Preview:	!function(e){function a(a){for(var c,n,o=a[0],d=a[1],b=a[2],i=0,l=[];i<o.length;i++)n=o[i],Object.prototype.hasOwnProperty.call(f,n)&&f[n]&&l.push(f[n][0]),f[n]=0;for(c in d)Object.prototype.hasOwnProperty.call(d,c)&&(e[c]=d[c]);for(u&&u(a);l.length;)l.shift()();return t.push.apply(t,b||[]),r()}function r(){for(var e,a=0;a<t.length;a++){for(var r=t[a],c=!0,o=1;o<r.length;o++)0!==f[r[o]]&&(c=!1);c&&(t.splice(a--,1),e=n(n.s=r[0]))}return e}var c={},f={11:0},t=[];function n(a){if(c[a])return c[a].exports;var r=c[a]={i:a,l:!1,exports:{}};return e[a].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.e=function(e){var a=[],r=f[e];if(0!==r)if(r)a.push(r[2]);else{var c=new Promise((function(a,c){r=f[e]=[a,c]}));a.push(r[2]=c);var t,o=document.createElement("script");o.charset="utf-8",o.timeout=120,n.nc&&o.setAttribute("nonce",n.nc),o.src=function(e){return n.p+""+({0:"common"}[e]||e)+"."+{0:"aa85268e12225fbdfd83",1:"05b66a5f38483263ec2f",2:"e177618a7d8918269894",3:"7b61c89dd25ae0bf5b87",4:"13e9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOlCnqEu92Fr1MmYUtfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20392, version 1.1
Category:	downloaded
Size (bytes):	20392
Entropy (8bit):	7.969803364230641
Encrypted:	false
SSDEEP:	384:Ld21eNqGoVwVsb0PULg3ZaTn09dltEGKMmZvBxvSJ66JQ3GoT4G54:LY1eNqGM8jULg3Z609taBx6J6fT54
MD5:	BB1E4DC6333675D11ADA2E857E7F95D7
SHA1:	3E2625FE48669F4AD48823E8C18E6FB14B74C5A0
SHA-256:	E8586F9DB7C0503A984C944AD2F1F783BF6051AEA2A066BC21FDEDC8FE7FA68A
SHA-512:	7EBCB4E20E323880245FD9900D58FC54086132711A695825134A8F34D9C63A48610454C9F10210CBB1926A65D1FEBEA96176F865910E1A6A9487FF9BDD83D87B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmYUtfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....~..GSUB.....'.....r.OS/2.....O...`v...cmap...X.....W.cvt ...P...Z...Z...=fpgm.....3.....#.gasp.....glyf.....;...k@...hdmx..H....l....%(. head..I....6...6...Rhhea..I@.....$.]..hmtx..I`...y.....=.loca..K.....Mc1.maxp..M.... ... .(..name..M.....\|..9.post..N..... .m.dprep..N.....8...Cx...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x....dK...{....?..F?.\|.~.m...ms.{.Z..;.....U.]7s.....\.=D.=.7...>....x...D..O\|.U:...\|o..3.x.j.r"B...../.)x$.'"j....1LGmaGxQxG....~.:'.A..hd.z,.k..KO.....^.}H|#z_.O.....R..A...9..A..!.(./...".:.Iq1.r..s..r.7r.7s..q.wr....nz..]...2..d4c..c....d....T.1...d....\....,c9k.g..Yv.#O."%..... ...t"uM..%.....j.#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.....(..(...K..{.^..'.....`#./..B.....N+p.m`...].IQ....Drg.M..Kx.^.S.*.....h ..$.k.'Hy.I.ze..4z.-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20268, version 1.1
Category:	downloaded
Size (bytes):	20268
Entropy (8bit):	7.970212610239314
Encrypted:	false
SSDEEP:	384:LyfRPUY1e32pJd75q1DzPjsnouCrZsZtetWFNFfIP0clWvdzNcrm:uJPb1em3dSPjKrZYtWntk0wvdzh
MD5:	60FA3C0614B8FB2F394FA29944C21540
SHA1:	42C8AE79841C592A26633F10EE9A26C75BCF9273
SHA-256:	C1DC87F99C7FF228806117D58F085C6C573057FA237228081802B7D8D3CF7684
SHA-512:	C921362A52F3187224849EB566E297E48842D121E88C33449A5C6C1193FD4842BBD3EF181D770ADE9707011EB6F4078947B8165FAD51C72C17F43B592439FFF4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....O,.....P.....GDEF.....G...d....GPOS.....GSUB.....'.....r.OS/2.....P...`t...cmap...$.....W.cvt .....T...T+...fpgm...p...5....w.`.gasp.....glyf.....;Q..lD..&0hdmx..H....n..... ..head..Hx...6...6.j.zhhea..H.....$....hmtx..H....t.....Xdloca..KD.....BC%.maxp..M0... ... .(..name..MP.....t.U9.post..N ..... .m.dprep..N4.....l.f..x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x.l..h.a.....l.m.6.1+.X....i...y....&...._..63..5....2>...x|D...ct.Kx..H@b.3..l..#u.....L.*.....^.*.4.....rP..{.*.....Q...JT.:Xu>..T./>...oq.....~..@.....lq../.... ..#..".&.8.H$..r...J)..jj...&..f.=.9..N9.....'F..8.4.....m...m...m.m..n..&.X..}....S.|.....n.....PHaE...J*...4..MjJ.*..nW)..rn3'/.....ks5zY5c...Mgg.5..p..rR{c...p..t\.8.c=..p...X.(.....7....=.....!...H .....(.0...(.q.JT?.b..z].'T...m..vNi.....t....:P.R..H....t.....&?.:.j.51+.S.":j.SK'I.^....}S.i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\polyfills.cd99248bc391ba233525[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	176443
Entropy (8bit):	5.369527816898332
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\polyfills.cd99248bc391ba233525[1].js	
SSDEEP:	1536:XGNZhrt0TuTtQQNGo69PYDaCUIAiygObhNAPk99tSf8/4/u3Fz8Ym4Y+6D4P:2NZt+QNGoI/g2APONSu3Fz8YW+6DM
MD5:	E813534C70E59DC8CCBE630F6C6AFE2F
SHA1:	0AF4A9D9134364180641A798C0A29A6A3FE343EF
SHA-256:	2A73193208A6290CD3EFCAFB61F518378109FD0C7884B84A69FEA0C42F9EAA34
SHA-512:	D82FFCA39872165319AF0DCB6CACDA0598ED6AF494A4EE357064D02ED334E6F5DE680686C80FBC4EAADB6A64363BCE31AE6B8BE3BD12580C599AB2D922B3C CB2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fromsmash.com/polyfills.cd99248bc391ba233525.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[17],{"+auO":function(t,e,n){var r=n("XKFU"),i=n("lvtm");r(r.S,"Math",{cbrt:function(t){return i(t=+t)*Math. pow(Math.abs(t),1/3)}})},"+lvF":function(t,e,n){t.exports=n("VTer")("native-function-to-string",Function.toString)},"+oPb":function(t,e,n){"use strict";n("OGtf")("blink",(function(t){return function(){return t(this,"blink","","")}})})},"+rLv":function(t,e,n){var r=n("dyZX").document;t.exports=r&&r.documentElement},"/KAi":function(t,e,n){var r=n("XKF U"),i=n("dyZX").isFinite;r(r.S,"Number",{isFinite:function(t){return"number"==typeof t&&i(t)}})},"/SS/":function(t,e,n){var r=n("XKFU");r(r.S,"Object",{setPrototypeOf:n(" i5dc").set})},"/e88":function(t,e){t.exports="\t\n\v\f\r \xa0\u1680\u180e\u2000\u2001\u2002\u2003\u2004\u2005\u2006\u2007\u2008\u2009\u200a\u202f\u205f\u3000\u2 028\u2029\ufeff"},"0/R4":function(t,e){t.exports=function(t){return"object"==typeof t?null!==t:"function"==typeof t}},"0E+W":function(t,e,n){n("elZq")("Array")}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\main.fc4f93bd9b7e2d23fe01[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2851607
Entropy (8bit):	5.482120224316256
Encrypted:	false
SSDEEP:	49152:XjU5gFxGtEXbGQAP/X5qUJpUN/9ZtWuo6kmUjWDwz/+x+Pl4qBV2WwC:Xj9FcKXbhiUNMuoMxGhC
MD5:	D877E93FF0D83AAB14B76D29AC8B0455
SHA1:	E570DF2006485B3D62F42DC459ECC1835DAF57BB
SHA-256:	1C59C04115F753E419D7F55DFE5E5D5E34CAFD834445DDD41DD8677F4E55CDEB
SHA-512:	497253401CC995C863AA470B8E8D0B933030494677E8A9752E1E3F43754C92EC9110FF948FF3D2E8A093BEAB4CE1298F2A051D468288922C314FC4877FE6FB33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fromsmash.com/main.fc4f93bd9b7e2d23fe01.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[16],{"+62n":function(e,t,n){"use strict";var i={};n.r(i),n.d(i,"updateDomainToCreate",(function(){return o})),n.d(i," loadDomains",(function(){return a})),n.d(i,"loadDomainsSuccess",(function(){return s})),n.d(i,"loadDomainsFailure",(function(){return c})),n.d(i,"createDomain",(function() {return l})),n.d(i,"createDomainSuccess",(function(){return u})),n.d(i,"createDomainFailure",(function(){return d})),n.d(i,"InitiateTeam",(function(){return h})),n.d(i,"InitiateTe amSuccess",(function(){return p})),n.d(i,"InitiateTeamFailure",(function(){return f}));var r=n("yGQT"),o=Object(r.w)("[Domain Signup] Update Domain To Create",Object(r.C) ()),a=Object(r.w)("[Domain Signup] Load Domains"),s=Object(r.w)("[Domain Signup] Load Domains Success"),c=Object(r.w)("[Domain Signup] Load Domains Failure"),l= Object(r.w)("[Domain Signup] Create Domain"),u=Object(r.w)("[Domain Signup] Create Domain Success",Object(r.C)()),d=Object(r.w)("[Domain Signup] Creat

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\polyfills-es5.c44c2e980ce14a55b741[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	261420
Entropy (8bit):	5.380036461420049
Encrypted:	false
SSDEEP:	3072:NcucccrN6KUF4oYbzHRR2qxPXRvhNKgdJME46MBcKT3J+csg:Ncucccr7U+oYfzjHdJ6RBc0+csg
MD5:	6CF3565F495DF06FF289FB04072171C3
SHA1:	C6B970D97AEF5F5ACCDF83C93F6DB4A19D678108
SHA-256:	A8E9D7A21B4C148AC19B2821A73AAAEFF1344FAA980E0960239C2E370CCF1BC7
SHA-512:	4D7B552109996E0F84FF24F0EB0BBD7CFBF7496540ADC15423006B05D4D224BE2B66C209BAAAF7CA91093662424350A3D0BED0BB34847BC1D46D134F84BE069
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fromsmash.com/polyfills-es5.c44c2e980ce14a55b741.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[18],{"+5Eg":function(t,e,n){var r=n("wA6s"),i=n("6XUM"),o=n("M7Xk").onFreeze,a=n("cZY6"),u=n("rG8t"),s=Obje ct.seal;r({target:"Object",stat:!0,forced:u((function(){s(1)})),sham:!a},{seal:function(t){return s&&i(t)?s(o(t)):t}})},"+IJR":function(t,e,n){n("wA6s")({target:"Number",stat:!0},{ isNaN:function(t){return t!=t}})},"+auO":function(t,e,n){var r=n("XKFU"),i=n("lvtm");r(r.S,"Math",{cbrt:function(t){return i(t=+t)*Math.pow(Math.abs(t),1/3)}})},"+lvF":function(t,e ,n){t.exports=n("VTer")("native-function-to-string",Function.toString)},"+oPb":function(t,e,n){"use strict";n("OGtf")("blink",(function(t){return function(){return t(this,"blink","","")}})})},"+rLv":function(t,e,n){var r=n("dyZX").document;t.exports=r&&r.documentElement},"/AsP":function(t,e,n){var r=n("yliL"),i=n("SDMg"),o=r("keys");t.exports=functi on(t){return o[t]||(o[t]=i(t))}},"/KAi":function(t,e,n){var r=n("XKFU"),i=n("dyZX").isFinite;r(r.S,"Number",{isFinite:function(t){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\styles.ee86bb33f6f63d643664[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	107644
Entropy (8bit):	4.964132126436259
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\styles.ee86bb33f6f63d643664[1].css	
SSDEEP:	1536:d2ofGRaaqYJoCOpCsIrzXZYjz5aBVPjzhg0dCrKsF7q19AgIW:nYvzhgo5
MD5:	FF44BB47507936DB25BF1130846FAA3C
SHA1:	274B95244B7F40EF7269248F30493E6AB3B19496
SHA-256:	DE7173180B698E000A6F37B4318DD16B69FA25690D8DE6DECCEA0AF52552D5AD
SHA-512:	4523B6DB39EEDB05BB4F19F1B0C18C6D9F41C57060F3D8DECD41E2F050FBEB99CB4572E3433E0CF6BCBF4B5ED50EDAC1CC51C9AD5ED6CFC204E87D29257C E98F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fromsmash.com/styles.ee86bb33f6f63d643664.css
Preview:	@import url("https://fonts.googleapis.com/css?family=Nunito:400,900|Roboto:400,900&display=swap");@font-face{font-family:Smash;src:url(Smash.a5bfb0d5eb0d37a67c6 e.eot);src:url(Smash.a5bfb0d5eb0d37a67c6e.eot?#iefix) format("embedded-opentype"),url(Smash.13c1611b4def0e5eac31.woff) format("woff"),url(Smash.d469dd e0140e1ecaa1fb.ttf) format("truetype"),url(Smash.db900add929378a7278d.svg#Smash) format("svg");font-weight:400;font-style:normal}[class*=icon-]:before{display:i nline-block;font-family:Smash;font-style:normal;font-weight:400;line-height:1;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.icon-smash_b ack:before{content:"\0041"}.icon-smash_dots:before{content:"\0042"}.icon-smash_icologo_chip:before{content:"\0043"}.icon-smash_remote:before{content:"\0044"}.icon-smash_settings:before{content:"\0045"}.icon-smash_logo_no_chip:before{content:"\0046"}.icon-smash_logo_no_icologo:before{content:"\0047"}.icon-smash_file:bef ore{content:"\0048"}.icon-smash_profil:before{cont

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	796
Entropy (8bit):	5.138661423815696
Encrypted:	false
SSDEEP:	24:5mOY7aFGmOYkaUnNeJ/iOY7aNxDv/iOYkaNxF8:wOEaLObaUN1OEaNtCObaNQ
MD5:	AA8153331068E0863006061C2E2110B0
SHA1:	23886F3072FB461BCF52F9A58AA149B0EA80539A
SHA-256:	15BB609776C20CDDEFF8B0CB012A553201CF73E0543D8C4C9690A7964296F64C
SHA-512:	F78AA324CD237EB4CC8ADC6AA735498D060DB801E09E6F887EA1ED9D335F6BA25B70E215B1904B1558ED672BC8278929AA5D16776C55B50D3564041388DC5E D
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Nunito';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/nunito/v16/XRXV3I6Li01BKofINeaH.woff) format('woff');.}.@font-face {. font-family: 'Nunito';. font-style: normal;. font-weight: 900;. font-display: swap;. src: url(https://fonts.gstatic.com/s/nunito/v16/XRXW3I6Li01 BKofAtsGUYevO.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/r oboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. font-display: swap;. src: url(ht tps://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmYUtfBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\rcyEYwqZAd-ft[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	1118
Entropy (8bit):	5.170782274791417
Encrypted:	false
SSDEEP:	24:0pQsd0X5kIFdsriOC/UVHG4fNI8uHkTtW3fvHXhpGMpLVPMibXM:0KJpk4dZUpf2wTsX3DGILVzTM
MD5:	09656AF18C71CF30966B552DF4C2D3B0
SHA1:	27F001F6F18D68906873A644C3231EDDB5BC2DAC
SHA-256:	59AA423B63AA229F068F919D4EEBE57BE27638E7B32EE01BED4EDAD9DF115D0E
SHA-512:	D8D87852D88E66E68A4BEE3AE6FEAA1EDDE712F269F9E7B86BFB643D3DD719E8C74B1B89C89C636C7DFCB0428D8786322594AF883CDCA93C936DF63A40202I A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fromsmash.com/rcyEYwqZAd-ft?e=YnJpYW5uZS5jYXBAZGV2cnkuZWR1
Preview:	<!doctype html>.<html lang="en" class="notranslate" translate="no">..<head>. <meta charset="utf-8">. <meta http-equiv="X-UA-Compatible" content="IE=edge" />. <title>Smash</title>. <base href="/">. <meta name="google" content="notranslate" />. <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">. <link rel="icon" type="image/x-icon" href="./assets/img/smash-logo/png/icono-no-chip-red.png" />.<link rel="stylesheet" href="styles.ee86bb33f6f63d643664 .css"></head>..<body>. <app-root></app-root>. <script>. function isIE() { return window.navigator.userAgent.match(/(MSIE|Trident)/) }. if (isIE()) {. } else {. var script = document.createElement("script");. script.setAttribute('src', 'https://www.youtube.com/player_api');. document.body.appendChild(script). };. </script>. <script src="runtime.970dd264cf5d1fad178c.js" defer></script><script src="polyfills-es5.c44c2e980ce14a55b741.js" nomodule defer></script><script src="polyfi

C:\Users\user\AppData\Local\Temp\~DFB5C25BBBFC3B97A0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664

C:\Users\user\AppData\Local\Temp\~DFB5C25BBBFC3B97A0.TMP	
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
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\~DFC680C543889275C2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34437
Entropy (8bit):	0.3640348206332695
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwB9lwh9l2/9l2/9l/71:kBqoxKAuvScS+yU+X7l7h1RF1fU9
MD5:	D8CF53133937DC64010B6DBDB15E66CB
SHA1:	11691C5CB05C76AC7F68A6F6CBFEF274A0E89A06
SHA-256:	06CD089F67EDE2D5FB788CE86CE4800312943938BF3B4A78922936EA7E570E5A
SHA-512:	CC9501081C23F347E7010E2F9EC0D9E9F55ED9C130944163069C76379A8F0541BCCAB995B3A52ACA56B129E78084C0FBBFD398DCB66BD0B110930BD9DA9ADE2
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE61E2820AB5BCB8F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48061555513959187
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo1F9lov9lW6xnl:kBqolwO6xnl
MD5:	44AB0D853BC18F04115FF4FC28DD36DA
SHA1:	FF82130757D9C352A436D146838D4DC80AE852F7
SHA-256:	C70A73F84C14131C83F6A628A1404CA46F133AEA0DDD787F48DC2B5BAB4884AB
SHA-512:	8B872EDB2819CB7A9DDF06A4746E094384C88800A49FE15143BAD1C1E2DB6549DFA008E03F640D3D8D297095DACD55E9CD127B85C847B907BD2BD1B1347434C
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

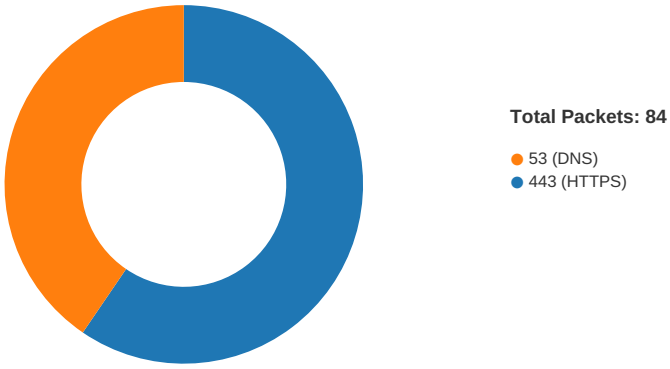
Static File Info

No static file info

Network Behavior

Network Port Distribution

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:05:27.480412960 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.481324911 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.528202057 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.528402090 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.528633118 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.528770924 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.535089970 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.535465002 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.581051111 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.581291914 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.585375071 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.585462093 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.585499048 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.585508108 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.585537910 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.585566044 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.586045027 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.586093903 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.586132050 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.586205959 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.586255074 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.586261988 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.590981007 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.591141939 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.592137098 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.592238903 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.635698080 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.636122942 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.643673897 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.643851995 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.644188881 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.684204102 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.685812950 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.686919928 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.686952114 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.687092066 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.687146902 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.688132048 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.690221071 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.690244913 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.690335035 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.691040039 CET	49712	443	192.168.2.3	13.224.94.70

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:05:27.692238092 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.692266941 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.692292929 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.692595959 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.692749977 CET	49713	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.694336891 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.694439888 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.733994961 CET	443	49713	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.736912012 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.843712091 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.843780994 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.843946934 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.844002008 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.905330896 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.905468941 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.905653000 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.905858994 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.906140089 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.951482058 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.951534986 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.951564074 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.951636076 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.951939106 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.955868959 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.955912113 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.956067085 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.956456900 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.956500053 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.956511974 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.956532955 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.956549883 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.957777023 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.957819939 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.957848072 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.957870007 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.959055901 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.959100008 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.959145069 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.959171057 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.960338116 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.960386992 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.960405111 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.960432053 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.961669922 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.961713076 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.961749077 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.961770058 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.962949038 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.963004112 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.963046074 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.963068008 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.964236975 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.964281082 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.964328051 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.964350939 CET	49712	443	192.168.2.3	13.224.94.70
Feb 25, 2021 22:05:27.965548038 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.965598106 CET	443	49712	13.224.94.70	192.168.2.3
Feb 25, 2021 22:05:27.965617895 CET	49712	443	192.168.2.3	13.224.94.70

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:05:19.276170969 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:19.327660084 CET	53	50620	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:05:20.257031918 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:20.307120085 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:21.233546972 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:21.286159039 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:22.753065109 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:22.801927090 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:23.901102066 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:23.951680899 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:25.136111021 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:25.185199022 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:26.131455898 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:26.195699930 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:26.353842974 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:26.402378082 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:27.400316954 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:27.438325882 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:27.466593981 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:27.491400003 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:28.083802938 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:28.149418116 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:28.395380974 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:28.460160971 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:30.251503944 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:30.303118944 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:37.611218929 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:37.661067009 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:38.802716017 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:38.851627111 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:42.489008904 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:42.541227102 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:44.110189915 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:44.165972948 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:44.565696001 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:44.616399050 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:45.639995098 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:45.688905001 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:52.642822027 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:52.693902016 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:53.669178963 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:53.726963997 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:54.344225883 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:54.397453070 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:54.723613977 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:54.783337116 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:55.560875893 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:55.626926899 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:56.215236902 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:56.267098904 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:56.930385113 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:56.984102011 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:57.252090931 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:57.309736967 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:57.945684910 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:58.010829926 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:58.258843899 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:58.316291094 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 22:05:58.960845947 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:05:59.020849943 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 22:06:00.301647902 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:06:00.354960918 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 22:06:00.976619959 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:06:01.028213024 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 22:06:04.305737019 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:06:04.354469061 CET	53	55435	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:06:04.992588043 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:06:05.045469046 CET	53	50713	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 22:05:27.400316954 CET	192.168.2.3	8.8.8.8	0x7725	Standard query (0)	fromsmash.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:05:44.110189915 CET	192.168.2.3	8.8.8.8	0x68d7	Standard query (0)	fromsmash.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 22:05:27.466593981 CET	8.8.8.8	192.168.2.3	0x7725	No error (0)	fromsmash.com		13.224.94.70	A (IP address)	IN (0x0001)
Feb 25, 2021 22:05:27.466593981 CET	8.8.8.8	192.168.2.3	0x7725	No error (0)	fromsmash.com		13.224.94.6	A (IP address)	IN (0x0001)
Feb 25, 2021 22:05:27.466593981 CET	8.8.8.8	192.168.2.3	0x7725	No error (0)	fromsmash.com		13.224.94.39	A (IP address)	IN (0x0001)
Feb 25, 2021 22:05:27.466593981 CET	8.8.8.8	192.168.2.3	0x7725	No error (0)	fromsmash.com		13.224.94.19	A (IP address)	IN (0x0001)
Feb 25, 2021 22:05:44.165972948 CET	8.8.8.8	192.168.2.3	0x68d7	No error (0)	fromsmash.com		13.224.94.6	A (IP address)	IN (0x0001)
Feb 25, 2021 22:05:44.165972948 CET	8.8.8.8	192.168.2.3	0x68d7	No error (0)	fromsmash.com		13.224.94.19	A (IP address)	IN (0x0001)
Feb 25, 2021 22:05:44.165972948 CET	8.8.8.8	192.168.2.3	0x68d7	No error (0)	fromsmash.com		13.224.94.39	A (IP address)	IN (0x0001)
Feb 25, 2021 22:05:44.165972948 CET	8.8.8.8	192.168.2.3	0x68d7	No error (0)	fromsmash.com		13.224.94.70	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
Feb 25, 2021 22:05:27.590981007 CET	13.224.94.70	443	192.168.2.3	49713	CN=fromsmash.com 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	Sat Dec 26 01:00:00 CET 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	Tue Jan 25 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		
Feb 25, 2021 22:05:27.592137098 CET	13.224.94.70	443	192.168.2.3	49712	CN=fromsmash.com 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	Sat Dec 26 01:00:00 CET 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	Tue Jan 25 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5620 Parent PID: 792

General

Start time:	22:05:24
Start date:	25/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff761b10000
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: 5816 Parent PID: 5620

General

Start time:	22:05:25
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5620 CREDAT:17410 /prefetch:2
Imagebase:	0x1150000
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