ID: 392887
Cookbook: browseurl.jbs
Time: 23:44:25
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

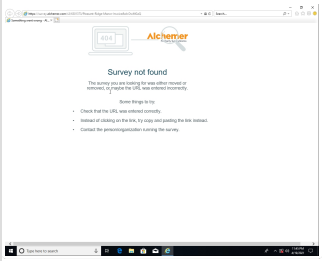
Analysis Report https://survey.alchemer.com/s3/630137…

Overview

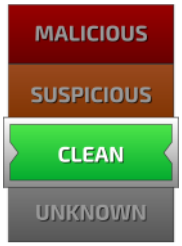
General Information

Sample URL:	http://https://survey.alchemer.com/s3/6301373/Pleasant-Ridge-Manor-Invoice&d=DwMGaQ
Analysis ID:	392887
Infos:	

Most interesting Screenshot:



Detection

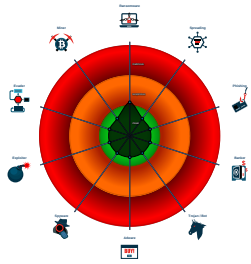


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3828 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4564 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3828 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

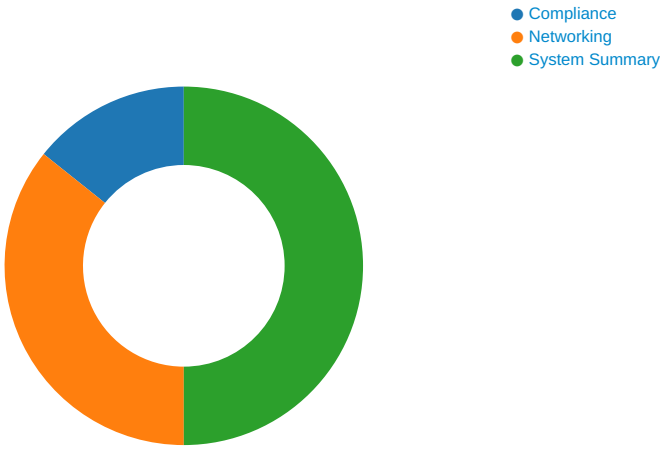
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



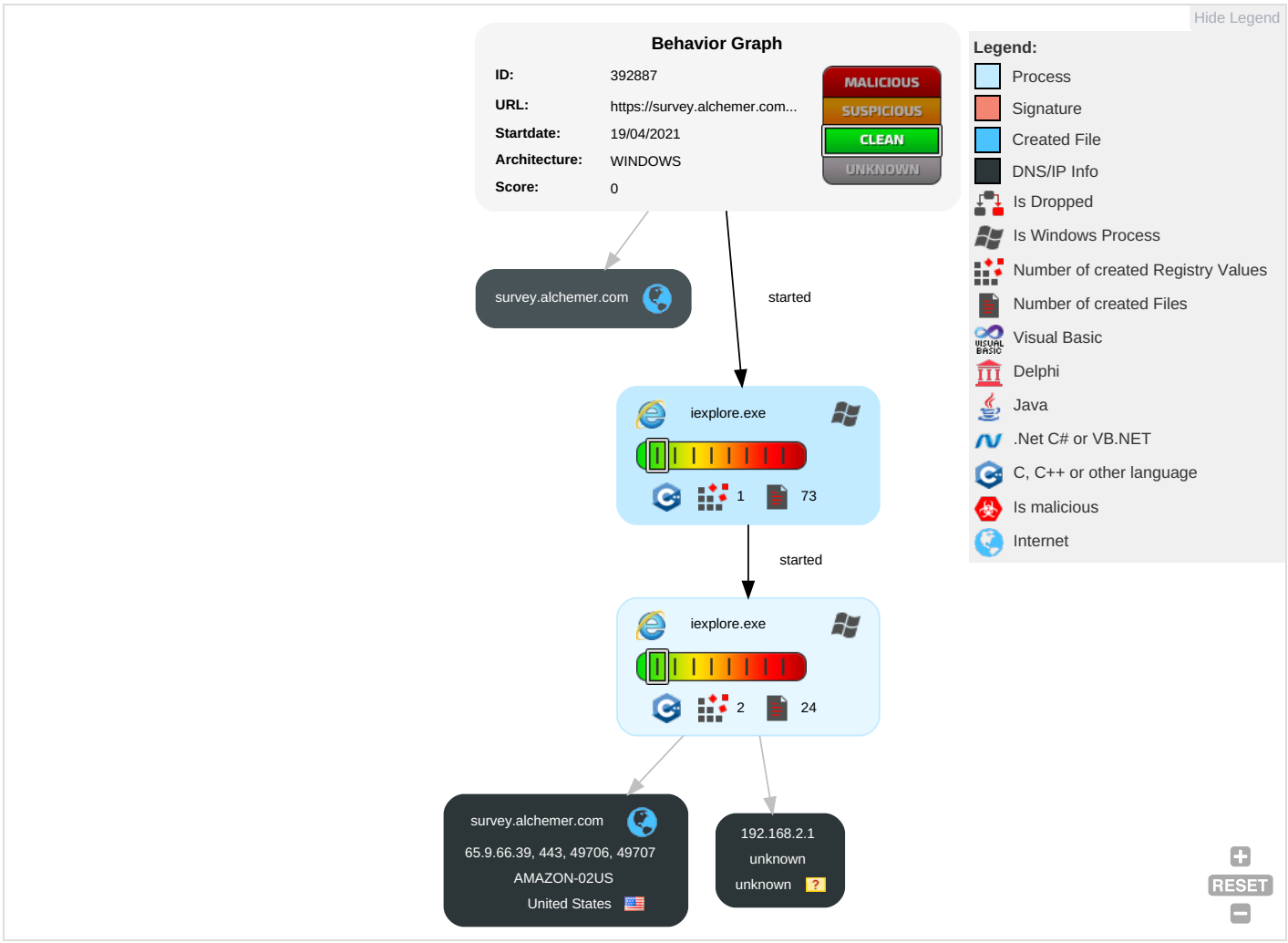
Click to jump to signature section

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

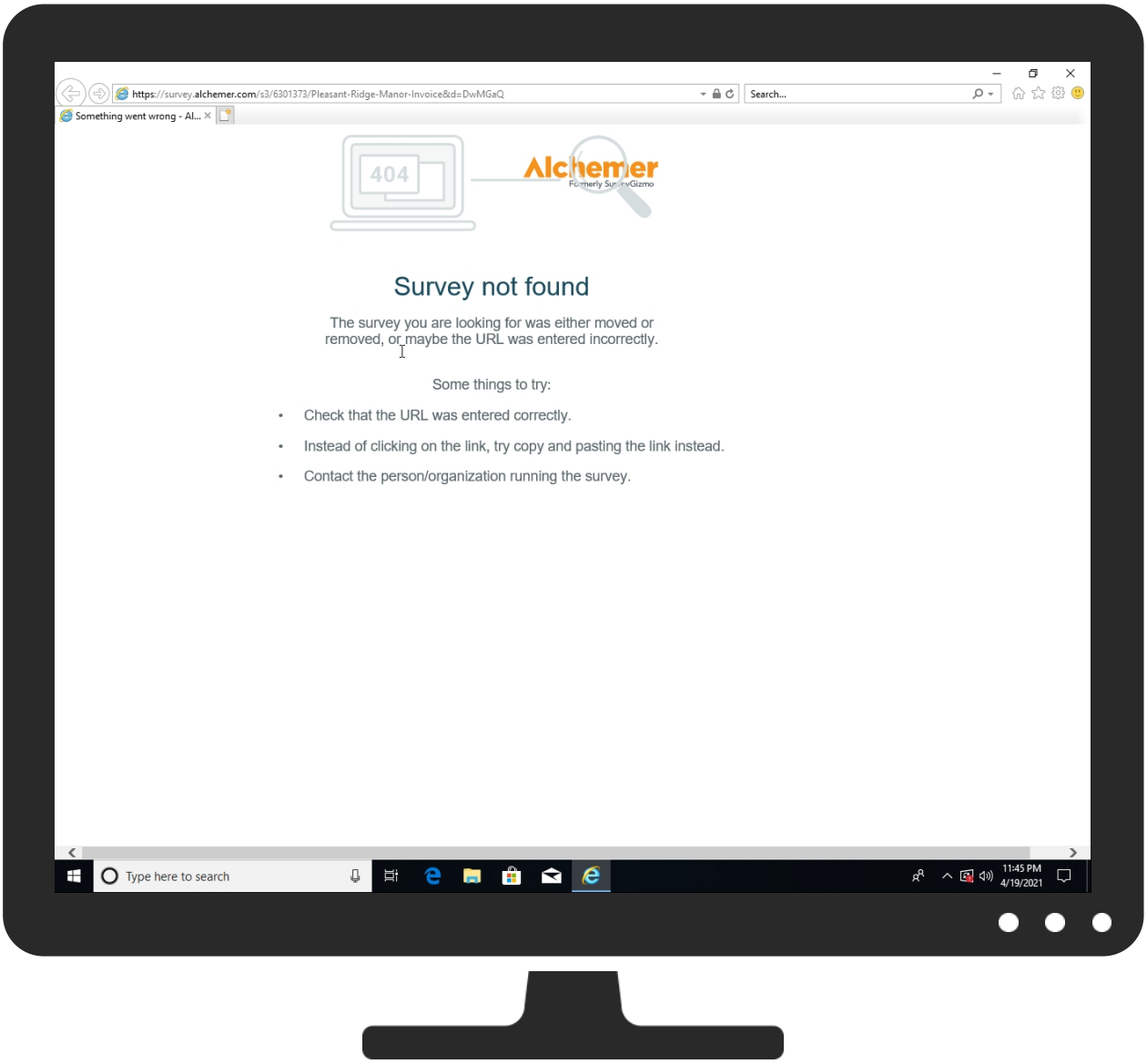
Behavior Graph



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://survey.alchemer.com/s3/6301373/Pleasant-Ridge-Manor-Invoice&d=DwMGaQ	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
survey.alchemer.com	2%	Virustotal		Browse

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	
http://https://survey.alchemer.com/s3/6301373/Pleasant-Ridge-Manor-Invoice&d=DwMGaQRoot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
survey.alchemer.com	65.9.66.39	true	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://survey.alchemer.com/s3/6301373/Pleasant-Ridge-Manor-Invoice&d=DwMGaQ	false		unknown

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://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://https://survey.alchemer.com/s3/6301373/Pleasant-Ridge-Manor-Invoice&d=DwMGaQRoot	{F885A27F-A1A3-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://survey.alchemer.com/s3/6301373/Pleasant-Ridge-Manor-Invoice&d=DwMGaQ	~DF8E0AD787EDA4F2B4.TMP.1.dr	false		unknown
http://www.youtube.com/	msapplication.xml7.1.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.9.66.39	survey.alchemer.com	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392887
Start date:	19.04.2021
Start time:	23:44:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://survey.alchemer.com/s3/6301373/Pleasant-Ridge-Manor-Invoice&d=DwMGaQ
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:	19
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@3/15@2/2
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.82.210.154, 52.147.198.201, 13.88.21.125, 92.122.145.220, 88.221.62.148, 184.30.20.56, 104.43.139.144, 152.199.19.161, 92.122.213.194, 92.122.213.247, 104.42.151.234, 104.43.193.48, 93.184.221.240, 2.20.142.210, 2.20.142.209, 51.103.5.159, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, cs11.wpc.v0cdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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.{F885A27D-A1A3-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.854532828295978
Encrypted:	false
SSDEEP:	192:rVZiZF2/WetSif1aAzMXoBpODSsfLadjX:rb+cOe7MASBE
MD5:	5C4374ABCFC1905D6C37B6C6624C92A9
SHA1:	D2507D261BE4C932C789F62B48DA460FDBF30F21
SHA-256:	3F7F66393A7ACA79FD8C420A764EDB93EE007B5FDD8EE3CB294DD415BED6313E
SHA-512:	FEB278E55C540B148C4E50FB29D1CA0A1798D568190488F8E1E002FC9075292B380FE091E40E9EA85ECF39391D63B1E6BAB6C581F9D75069000593368C9FB526
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\{F885A27F-A1A3-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24264
Entropy (8bit):	1.650059934301595
Encrypted:	false
SSDEEP:	48:Iw7GcprSGwpa+G4pQKGrapbS4hGQpBeGHHpcwiTGUp8jGzYpmOGGop9MLqxC5EtS:rhZaQ+68BS0jt29W5M5TzxCqDg
MD5:	491C3920D00174178E9B3B99FCB1D311
SHA1:	6D95AF672983814FEBD756E36DD6B2ACB1E82D56
SHA-256:	C9705285DF26B483DCF0E30D6376F7B276F7BDE7C3B5F9C26F890C5DF3C83C81
SHA-512:	B0262F06F9BF8D766195AAE21199458179ADDAC115A76F89F01E3B7A974723C709955382E1211F1BC3986E49C834616B6C7746F586C324FB9CA89E27A71B5E31
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\{F885A280-A1A3-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5660647538824346
Encrypted:	false
SSDEEP:	48:IwIGcpr1GwpaKG4pQOGrapbS8GQpK3G7HpRgTGIpG:r8ZfQq6ABSUAWT0A
MD5:	ABE40B8366CA9C554089B6668B5FCD17

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F885A280-A1A3-11EB-90E6-ECF4BB82F7E0}.dat	
SHA1:	AD5796B9DF70247648BEBE39C73D946991E6F7D8
SHA-256:	EF42AD4C8C3F1CA42CC5DEC89E777FBCE609E51AFED8D5A57822215D20DE41A5
SHA-512:	5A78DAA08737D7CB158E982146C2DA3D437D576646447A0C92B4D7B811528C3E4B887B34BE005E9D64E368CBDB99DCEB60F948D06CA4D8309978416786383E7
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):	660
Entropy (8bit):	5.070206590454977
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE87f4nWimI002EtM3MHdNMNxOE87f4nWimI00OYVbkEtMb:2d6NxOh4SZHKd6NxOh4SZ7xb
MD5:	57587C83114530BB7BFDEA0BF4D9E764
SHA1:	33C607A7B13B5A67814F7E55D41373D14FC81BFF
SHA-256:	9AD1B4E0EFE363A26FA1C7C8F14E3A629D4B5F8A6E06447CA47A3E770B477226
SHA-512:	1AEA568EBE913892059F70A3EFE072088B1EDECAB7F33A1C40A8A282A924BAF0E6A922F08387C63300DBE675D1270A5F5A76A1FA368E5649717B6FCAB5DB544 6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xce7166bb,0x01d735b0</date> accdate>0xce7166bb,0x01d735b0</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>0xce7166bb,0x01d735b0</date><accdate>0 xce7166bb,0x01d735b0</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):	657
Entropy (8bit):	5.096458212085735
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kyAw0Aws4nWimI002EtM3MHdNMNxe2kyAwis4nWimI00OYkak6EtMb:2d6NxrCEj4SZHKd6NxrCI4SZ7Ja7b
MD5:	726C8BB41E384C343B5625EFFC5D64A5
SHA1:	5349E327C34FC8CA10B1B3DDCE9749EBC3C5A263
SHA-256:	1C701D20221C926B8980A2B8086E7C5E0B2EEA4C0DA2334C72057C333C4188C5
SHA-512:	93FAEFE5A00FA428E8FDDD72E4DBB32DC6020AA72E3AD5BDDE1B7D4806B627543BD547773C10BABF9100127A00A811D63BC159C91704AD2F34FB641B67162B EF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xce6a3f9f,0x01d735b0</date><a ccdate>0xce6a3f9f,0x01d735b0</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>0xce6a3f9f,0x01d735b0</date><a ccdate>0xce6ca1f6,0x01d735b0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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):	666
Entropy (8bit):	5.086318464256087
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL87f4nWimI002EtM3MHdNMNxvL87f4nWimI00OYmZEtMb:2d6Nxv64SZHKd6Nxv64SZ7Zb
MD5:	23CBE17838CC1527879BA2DF5EA36227
SHA1:	05FD16D7E8E35A9E2CE55895E548721BB6D3FEA4
SHA-256:	BD9DB837A2ECC2A577423462E76E6DC04E4E7DE961F1099449A0ABF9A412720D
SHA-512:	73E58A2C3C86140FC28A778245D22F36F3554D9CC217ABA0BC19E65EA27CDEC39B8F870F97A752B552E360778E81FE4FEA7ECF2957BF379F8A7AEF6DD0E7CD B3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xce7166bb,0x01d735b0</date><accdate>0xce7166bb,0x01d735b0</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>0xce7166bb,0x01d735b0</date><accdate>0xce7166bb,0x01d735b0</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):	651
Entropy (8bit):	5.088885169481866
Encrypted:	false
SSDEEP:	12:TMHdNMNxiG4s4nWimI002EtM3MHdNMNxiG4s4nWimI00OYd5EtMb:2d6Nxl4SZHKd6Nxl4SZ7qjb
MD5:	807C8C94F6AAC270354F8EB9194C8BB5
SHA1:	467A79544A2D6BD1F7CDD2DD9F6EDAC54278BF1E
SHA-256:	F35B05D1F8F199DD748341C4AF080123B5BFFBB59D329654484C5D448F916FE7
SHA-512:	F1701E2B634CE89A7B7C1808CB61AADFD0A46C5221595524F05234429998F3829BF8DEAEB74428324792E30E60677AD8AB535CC1B7DE6303967D17D5AB96E4FA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xce6f045f,0x01d735b0</date><accdate>0xce6f045f,0x01d735b0</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>0xce6f045f,0x01d735b0</date><accdate>0xce6f045f,0x01d735b0</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:	modified
Size (bytes):	660
Entropy (8bit):	5.085260750820761
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwc4nWimI002EtM3MHdNMNxhGwc4nWimI00OY8K075EtMb:2d6NxQz4SZHKd6NxQz4SZ7RKajb
MD5:	3D950D0120D46BF81EE9A9320F89694D
SHA1:	F0693B9838C2E676A446F79B55B03139AC45750C
SHA-256:	EC76377D7399BB750F6BA99F199E0B52A1F2B488CE252FA9A24C4621E85EDE15
SHA-512:	104E31C048242BD092E070E86DC37D5D6FEBB4421028584ED3FE7BC42AE9E6DB67A61860E5D2008ACC9656BCAAE9B72D97A4358F3C5FCFDD90F67683AF4618C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xce73c91b,0x01d735b0</date><accdate>0xce73c91b,0x01d735b0</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>0xce73c91b,0x01d735b0</date><accdate>0xce73c91b,0x01d735b0</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):	657
Entropy (8bit):	5.073551589222396
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n87f4nWimI002EtM3MHdNMNx0n87f4nWimI00OYxEtMb:2d6Nx0m4SZHKd6Nx0m4SZ7+b
MD5:	4F730B906C08FF246922827224E0F0C1
SHA1:	7CB8347D88B0A3B97904C675476671087420D745
SHA-256:	602AC5F972C69D0DFCDFC894C8D499CBBA43AB0988560922B7F06C63EC69E82B
SHA-512:	1E7FBF767E87E9B213B4F2C13D244C827361F8FFEB8B86713D93400F59A4A7496389F47238890DDAA95FBF03BACC835980C5C1262A28CD301DCA508E90BB00E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xce7166bb,0x01d735b0</date><accdate>0xce7166bb,0x01d735b0</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>0xce7166bb,0x01d735b0</date><accdate>0xce7166bb,0x01d735b0</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):	660
Entropy (8bit):	5.117948477196494
Encrypted:	false
SSDEEP:	12:TMHdNMNxxG4s4nWimI002EtM3MHdNMNxxGef4nWimI00OY6Kq5EtMb:2d6NxC4SZHKd6NxP4SZ7Xb
MD5:	D46443F95D681A60AF48C98C2AAF0F93
SHA1:	81457EF9D694090A6EA7BDA258E0DF68266CD552
SHA-256:	CB5FDB63E7A1C7A5FEB71B8C82E2F71A0ECD1429E23CDF4CC930226B3F5E01F3
SHA-512:	183831BFA7C404EEC7D79CB9AB5D0973C6F277A228CD4A3D740D833155D5C44F205608358830A2934AC6C04E35E9F72782296EA314EC5BF72AAB684F86210229
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xce6f045f,0x01d735b0</date><accdate>0xce6f045f,0x01d735b0</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>0xce6f045f,0x01d735b0</date><accdate>0xce7166bb,0x01d735b0</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):	663
Entropy (8bit):	5.083349786224597
Encrypted:	false
SSDEEP:	12:TMHdNMNxcG4s4nWimI002EtM3MHdNMNxcG4s4nWimI00OYVEtMb:2d6NxT4SZHKd6NxT4SZ7Gb
MD5:	ED43B52F405B88F71A83023E9E6C9407
SHA1:	EF164206AAF7D8A49E0A35BFB688008049C58A8E
SHA-256:	663F10A4FB39A887E47A3C47C11DDFE8282BB2A5B0913FB29E290DC21082E0D2
SHA-512:	DD72C41AECCAF852501BD669BC923D441477530E636E4E5D8AE4F51D1E97C760125CE100BB3C3B2D62AD77F2187796530758B745AD53E699123C2F160E6C0D2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xce6f045f,0x01d735b0</date><accdate>0xce6f045f,0x01d735b0</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>0xce6f045f,0x01d735b0</date><accdate>0xce6f045f,0x01d735b0</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):	657
Entropy (8bit):	5.07458572869714
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnG4s4nWimI002EtM3MHdNMNxfnG4s4nWimI00OYe5EtMb:2d6Nxk4SZHKd6Nxk4SZ7Fjb
MD5:	17E0D5866A1CFF003BDD2FC64C17CD4E
SHA1:	ED7975004432A6071E0A3A46A10CB7291A60B08E
SHA-256:	843DA6449E97F543E54500AECFDB23FCF6B8772E1E720F04AA649EA2CC28A806
SHA-512:	3D63B0207D51B9FC6358CC8F09232C39257A44615DB222B830A6E5F8C80DB5EC9D7B499CF901906B4F0D5B4F8313DA043CE038A3A3E2ABD6A2B0AF373C593DB
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xce6f045f,0x01d735b0</date><accdate>0xce6f045f,0x01d735b0</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>0xce6f045f,0x01d735b0</date><accdate>0xce6f045f,0x01d735b0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Temp\~DF0BCD7C5818A0B206.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.333310092014618
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAq2QLC5LL:kBqoxxJhHWSVSEabga
MD5:	B327A32F7051367D6DC07DC8E723BA87
SHA1:	9AAC7B349929409647C61237B74F88D023FAFD4D
SHA-256:	CDBCD6EEAE9114E27B460150474E3AA6EBAD7E26B3F9215396EDD09DBC63E617
SHA-512:	75FE9DD859667F756775CF594E4BB2BD547B9098D787F0269B7947E88640A19ED5357AAC2A9294B756C24BE57A30E6AD3166A0E2DDD0DEA04235ED48A4FE06F B
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF8E0AD787EDA4F2B4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34457
Entropy (8bit):	0.3675381825843353
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw89lws9l269l2a9l/Ox:kBqoxKAuvScS+/hDqOIOvMLqxC5EV
MD5:	88CB4880D9672024658BE02B6E19B646
SHA1:	6990B850037E849A54C70690DA5975F457000FE3
SHA-256:	862191D0CF8BED8A92AF2871AAECDEFB37379A18381E504C222C154C61F85A76
SHA-512:	B1CADE69FCF78CB06B331367E00218FE83CDAA0A86879E6630118619FCEAC93F7093E680FFFA84D67EF03F8494C72AAA9394AF502351D19A62B9145F3DA2320(
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

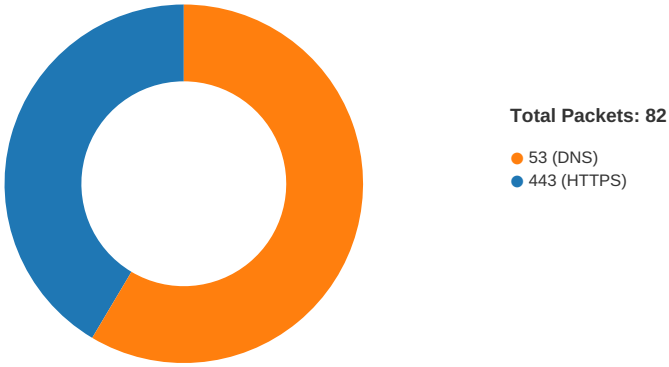
C:\Users\user\AppData\Local\Temp\~DFEAF6CAF48898AE43.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4795981866112163
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fR99l8fRd9lTqpEcvkEB:c9lLh9lLh9lIn9lIn9lo99lod9lWGcv5
MD5:	42D5CA310E27F3B406DB2791BB3CCB9B
SHA1:	5556D7E78AD9D072732050FA72AE51B728A373C2
SHA-256:	FDA4D5F547B2CD003B8B07FB8825E7E8BDEFA4478D5CA8BDEE413E7F67583667
SHA-512:	A83C281D08D937C89B723110A2864C7174906DE7515EEAA1AE787AFF7BD33D52A6F9AB63612AA51150F9D5FC22225A669BCF7A5899BCFE22EF134BC6F7AA2EA C
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



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:45:20.847219944 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.848359108 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.887654066 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.887778997 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.888612032 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.888721943 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.918777943 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.919646978 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.959882975 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.959914923 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.959935904 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.960004091 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.960035086 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.960093021 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.960133076 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.962377071 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.963764906 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.963888884 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.964895010 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.964915037 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.964931011 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.964977980 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.965007067 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:20.969873905 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:20.970057964 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.007283926 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.007463932 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.015511036 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.015697956 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.015763044 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.050195932 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.050232887 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.050359964 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.050448895 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.050504923 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.050517082 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.050549030 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.050575972 CEST	49706	443	192.168.2.7	65.9.66.39

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:45:21.050625086 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.050641060 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.051299095 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.051388979 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.059101105 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.059128046 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.059138060 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.059149027 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.059166908 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.059328079 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.059948921 CEST	49707	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.092631102 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.093023062 CEST	443	49707	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.766638994 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.766690016 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.766701937 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.766716003 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.766840935 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.766911030 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.767613888 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.767636061 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.767729998 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.769836903 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.769927025 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.769949913 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.770000935 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.771356106 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.771377087 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.771392107 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.771408081 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.771430016 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.771491051 CEST	49706	443	192.168.2.7	65.9.66.39
Apr 19, 2021 23:45:21.772371054 CEST	443	49706	65.9.66.39	192.168.2.7
Apr 19, 2021 23:45:21.772566080 CEST	49706	443	192.168.2.7	65.9.66.39

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:45:08.471589088 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:08.506696939 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:08.528453112 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:08.556704044 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:09.193085909 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:09.252954006 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:10.027254105 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:10.092958927 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:11.328155041 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:11.389488935 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:19.630738974 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:19.703265905 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:20.776648998 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:20.836245060 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:33.170978069 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:33.257570982 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:37.274559975 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:37.337120056 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:43.913954973 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:43.962657928 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:45.450220108 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:45.499125004 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:46.701692104 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:46.765083075 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:47.900787115 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:47.949790955 CEST	53	54008	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:45:48.792279005 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:48.841793060 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:48.889157057 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:48.941237926 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:49.639739990 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:49.702073097 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:49.965929031 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:50.014612913 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:50.420878887 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:50.478089094 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:50.645673037 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:50.709244967 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:51.411859035 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:51.470429897 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:51.501554012 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:51.550278902 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:51.669842958 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:51.731637001 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:52.427043915 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:52.475692034 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:52.758057117 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:52.817476034 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:53.678503990 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:53.692101955 CEST	49958	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:53.740642071 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:53.741951942 CEST	53	49958	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:54.442832947 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:54.502597094 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:54.619801998 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:54.668929100 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:55.549997091 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:55.607047081 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:55.796374083 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:55.855170965 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:57.591469049 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:57.640379906 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:57.693270922 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:57.755362988 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:58.517097950 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:58.566724062 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:58.808238029 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:45:58.859757900 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 19, 2021 23:45:59.983366013 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:00.031862020 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:00.897392035 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:00.950052977 CEST	53	56680	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:02.062344074 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:02.110940933 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:03.313710928 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:03.365257978 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:03.681902885 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:03.738914967 CEST	53	49247	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:03.837685108 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:03.896152020 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:04.258946896 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:04.310358047 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:04.423583031 CEST	63744	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:04.480581045 CEST	53	63744	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:05.416429996 CEST	61457	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:05.465842009 CEST	53	61457	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:05.554311037 CEST	58367	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:05.602859020 CEST	53	58367	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:07.828012943 CEST	60599	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:07.891033888 CEST	53	60599	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:46:14.748433113 CEST	59571	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:14.822138071 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:14.835839987 CEST	53	59571	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:14.889255047 CEST	53	52689	8.8.8.8	192.168.2.7
Apr 19, 2021 23:46:15.403913975 CEST	50290	53	192.168.2.7	8.8.8.8
Apr 19, 2021 23:46:15.461313009 CEST	53	50290	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 19, 2021 23:45:20.776648998 CEST	192.168.2.7	8.8.8.8	0xaff4	Standard query (0)	survey.alchemer.com	A (IP address)	IN (0x0001)
Apr 19, 2021 23:45:37.274559975 CEST	192.168.2.7	8.8.8.8	0x7a08	Standard query (0)	survey.alchemer.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 19, 2021 23:45:20.836245060 CEST	8.8.8.8	192.168.2.7	0xaff4	No error (0)	survey.alchemer.com		65.9.66.39	A (IP address)	IN (0x0001)
Apr 19, 2021 23:45:20.836245060 CEST	8.8.8.8	192.168.2.7	0xaff4	No error (0)	survey.alchemer.com		65.9.66.73	A (IP address)	IN (0x0001)
Apr 19, 2021 23:45:20.836245060 CEST	8.8.8.8	192.168.2.7	0xaff4	No error (0)	survey.alchemer.com		65.9.66.68	A (IP address)	IN (0x0001)
Apr 19, 2021 23:45:20.836245060 CEST	8.8.8.8	192.168.2.7	0xaff4	No error (0)	survey.alchemer.com		65.9.66.119	A (IP address)	IN (0x0001)
Apr 19, 2021 23:45:37.337120056 CEST	8.8.8.8	192.168.2.7	0x7a08	No error (0)	survey.alchemer.com		65.9.66.119	A (IP address)	IN (0x0001)
Apr 19, 2021 23:45:37.337120056 CEST	8.8.8.8	192.168.2.7	0x7a08	No error (0)	survey.alchemer.com		65.9.66.68	A (IP address)	IN (0x0001)
Apr 19, 2021 23:45:37.337120056 CEST	8.8.8.8	192.168.2.7	0x7a08	No error (0)	survey.alchemer.com		65.9.66.73	A (IP address)	IN (0x0001)
Apr 19, 2021 23:45:37.337120056 CEST	8.8.8.8	192.168.2.7	0x7a08	No error (0)	survey.alchemer.com		65.9.66.39	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 19, 2021 23:45:20.963764906 CEST	65.9.66.39	443	192.168.2.7	49706	CN=*.alchemer.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	Tue Jul 28 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	Sat Aug 28 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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
Apr 19, 2021 23:45:20.969873905 CEST	65.9.66.39	443	192.168.2.7	49707	CN=*.alchemer.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	Tue Jul 28 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	Sat Aug 28 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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 3828 Parent PID: 792

General

Start time:	23:45:19
Start date:	19/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff630020000
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	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: 4564 Parent PID: 3828

General

Start time:	23:45:19

Start date:	19/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3828 CREDAT:17410 /prefetch:2
Imagebase:	0x3f0000
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	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly