ID: 385476
Cookbook: browseurl.jbs
Time: 15:18:17
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

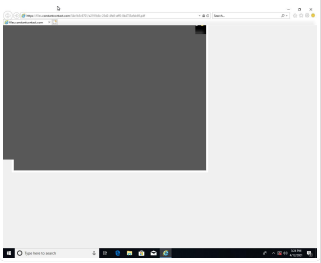
Analysis Report http://r20.rs6.net/tn.jsp?f=001UR9DU5D…

Overview

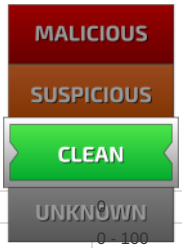
General Information

Sample URL:	r20.rs6.net/tn.jsp?f=001UR9DU5DWULSSQKRSbHmS5tW1BYzJdf5a5nCBJP8j6WTiQVP7-HJ...u6k3Sz7qp1rDA==&ch=t9Qhnt_2hiJ7oXunOWnQpfuylRuTM4kuFHw1DTZGabFSxZ_AG1kZXw==
Analysis ID:	385476
Infos:	

Most interesting Screenshot:



Detection

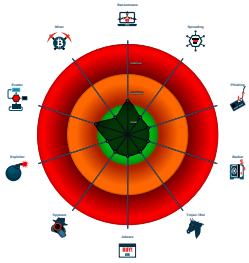


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Contains functionality to access load…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5620 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5904 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5620 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - AcroRd32.exe (PID: 3100 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' /o /eo /l /b /ac /id 5904 MD5: B969CF0C7B2C443A99034881E8C8740A)
      - AcroRd32.exe (PID: 5680 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 /o /eo /l /b /ac /id 5904 MD5: B969CF0C7B2C443A99034881E8C8740A)
- **cleanup**

Malware Configuration

No configs have been found

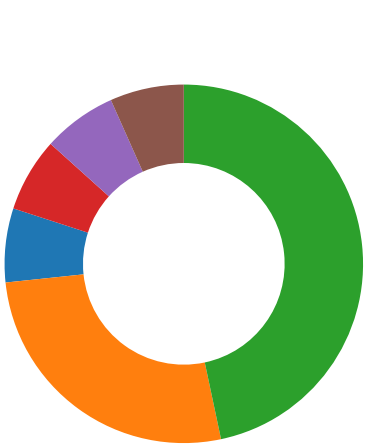
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



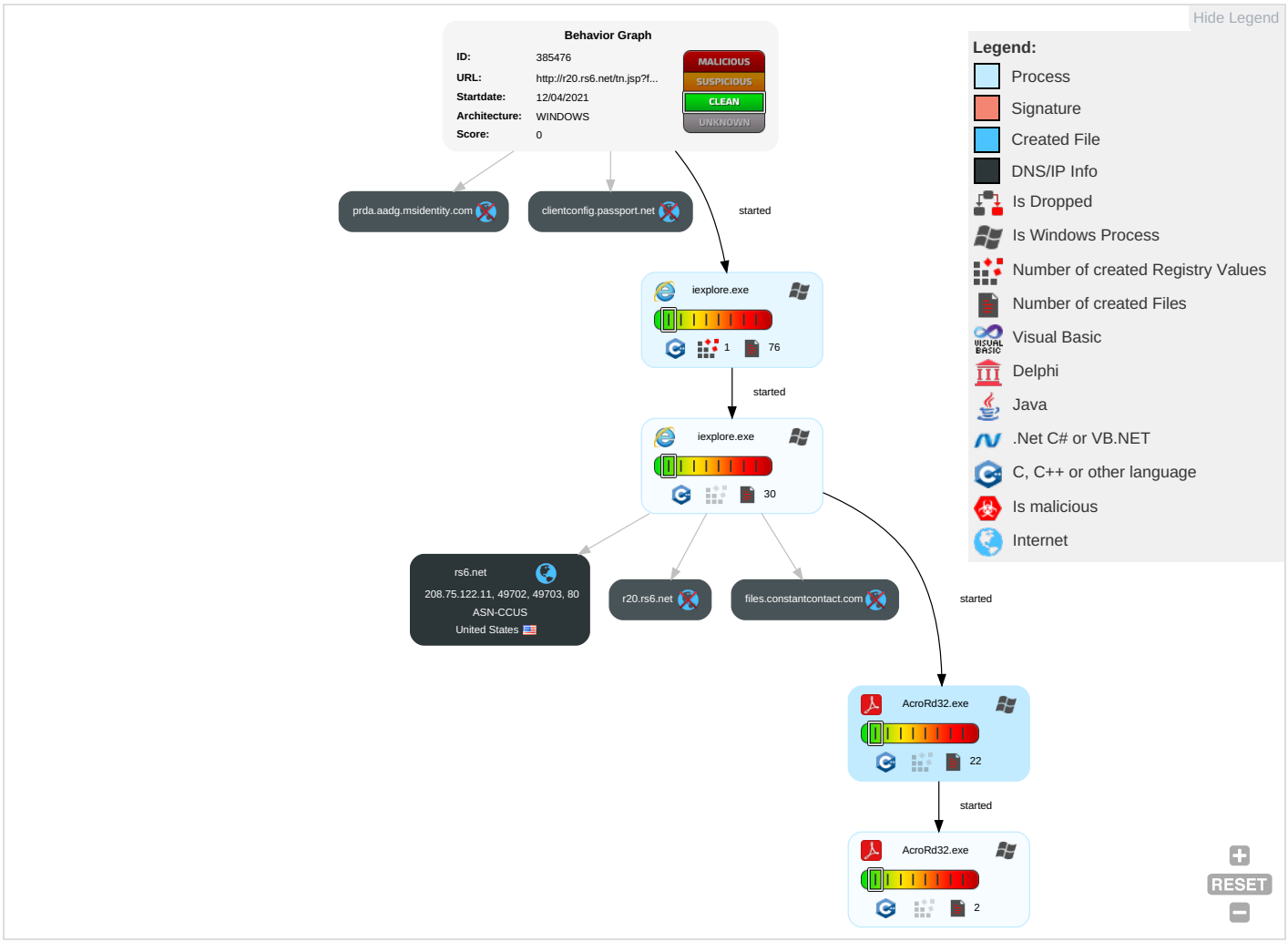
Click to jump to signature section

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 2	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 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 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 2	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	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

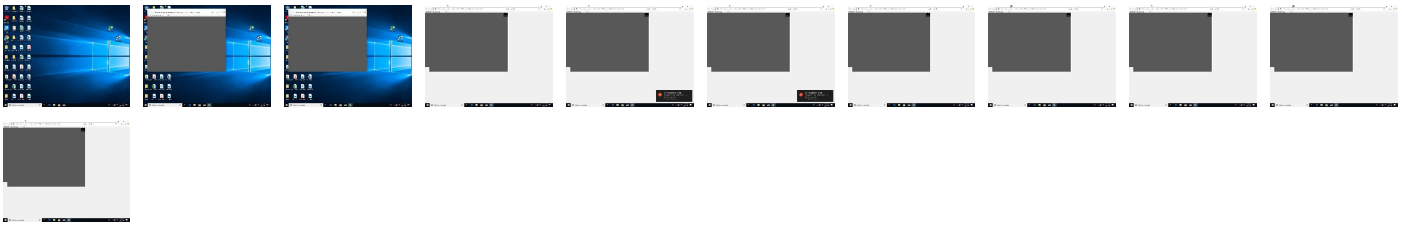
Behavior Graph

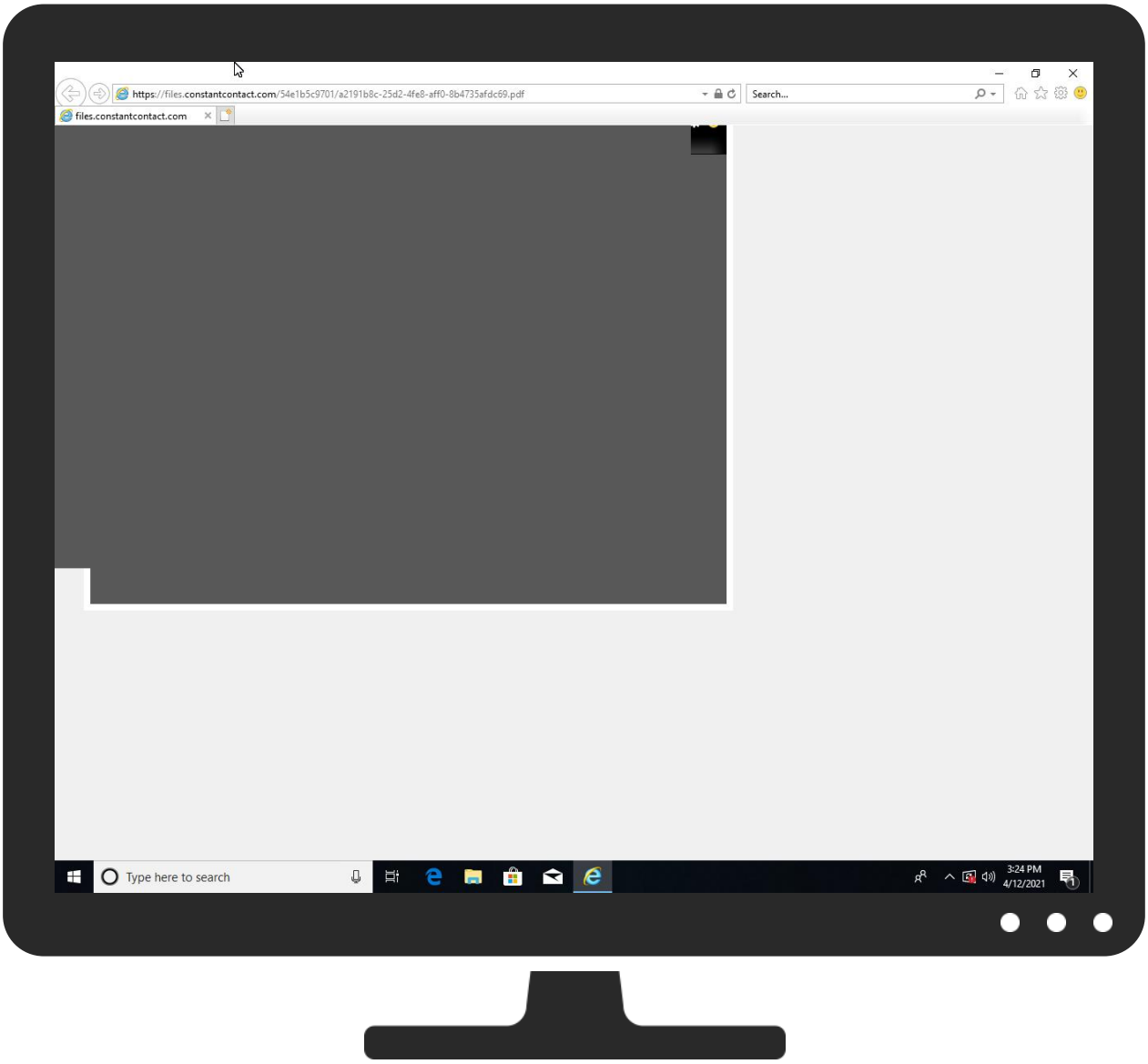


Screenshots

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://r20.rs6.net/tn.jsp?f=001UR9DU5DWULSSQKRSbHmS5tW1BYzJdf5a5nCBJP8j6WTiQVP7-HJVYmCgrw0XB_uf_QV56Haa_M0mobYIQXKQSaOe6Xu-1xTkGHmKJGzfmmZ2amUpZf-ss1HRg0GxKivYopLHGEV8UEW0_6clw3aFuQi_2vwTONr1CLcH72kMluSyn6F3FeMZ-MnNHeyuCyEwaUdYWjqc4gJLjgQuRM_rdz9h3O3GIfxNvpPnSjOOSeM=&c=5vPu-3Qs9yW2IEWn1dtOMdgOR2JdmjhB8RamT_IPEu6k3Sz7qp1rDA==&ch=t9Qhnt_2hiJ7oXunOWnQpfuylRuTM4kuFHw1DTZGabFSxZ_AG1kZXw==	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.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rs6.net	208.75.122.11	true	false		high
clientconfig.passport.net	unknown	unknown	false		unknown
r20.rs6.net	unknown	unknown	false		high
files.constantcontact.com	unknown	unknown	false		high

Contacted URLs

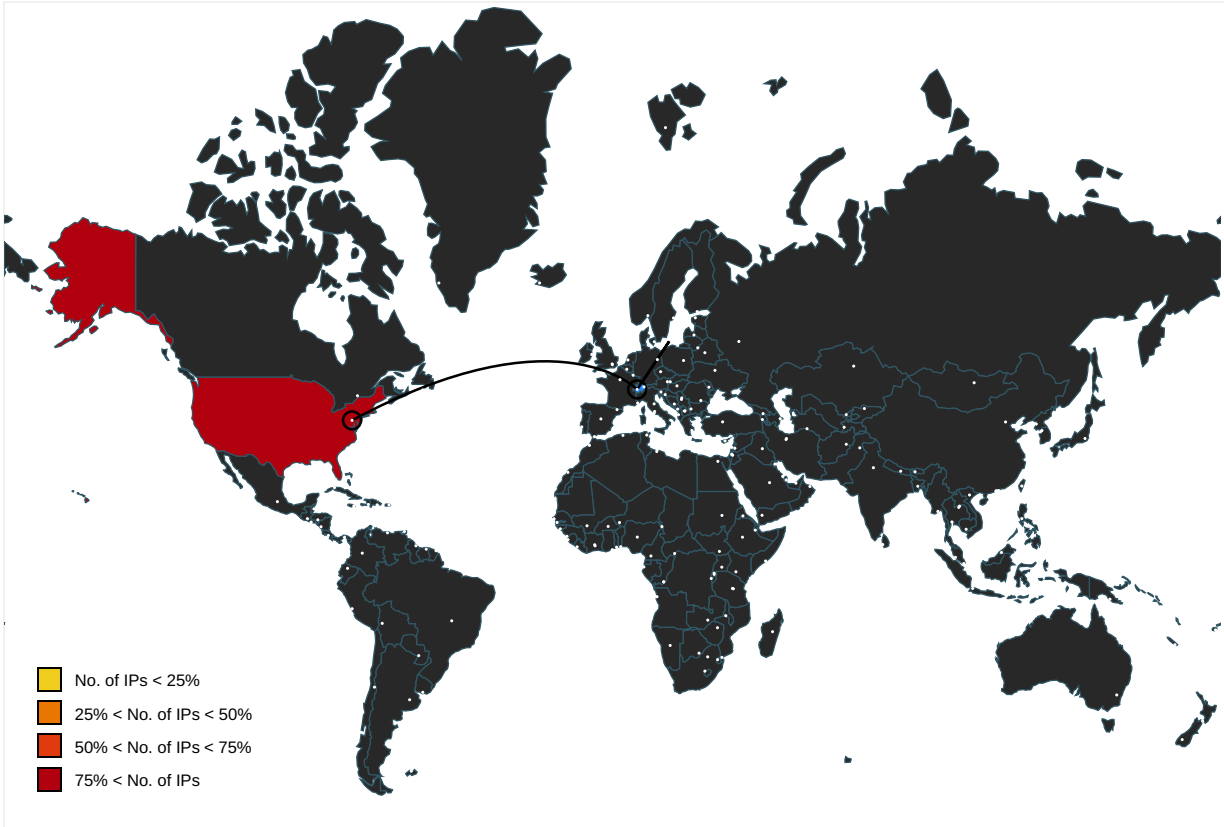
Name	Malicious	Antivirus Detection	Reputation
http://r20.rs6.net/tn.jsp?f=001UR9DU5DWULSSQKRSbHmS5tW1BYzJdf5a5nCBJP8j6WTiQVP7-HJVYmCgrw0XB_uf_QV56Haa_M0mobYIQXKQSaOe6Xu-1xTkGHmKJGzfmmZ2amUpZf-ss1HRg0GxKivYopLHGEV8UEW0_6clw3aFuQi_2vwTONr1CLcH72kMluSyn6F3FeMZ-MnNHeyuCyEwaUdYWjqc4gJLjgQuRM_rdz9h3O3GIfxNvpPnSjOOSeM=&c=5vPu-3Qs9yW2IEWn1dtOMdgOR2JdmjhB8RamT_IPEu6k3Sz7qp1rDA==&ch=t9Qhnt_2hiJ7oXunOWnQpfuylRuTM4kuFHw1DTZGabFSxZ_AG1kZXw==	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://files.constantcontact.com/54e1b5c9701/a2191b8c-25d2-4fe8-aff0-8b4735afdc69.pdfRoot	{168DA7A3-9BDD-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false		high
http://https://files.constantcontact.com/54e1b5c9701/a2191b8c-25d2-4fe8-aff0-8b4735afdc69.pdf	~DF0BE9630EA18F6468.TMP.1.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000005.00000002.1672938210.0000000007430000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.youtube.com/	msapplication.xml7.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000005.00000002.1672938210.0000000007430000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/drm/default	AcroRd32.exe, 00000005.00000002.1672938210.0000000007430000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000005.00000002.1672938210.0000000007430000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000005.00000002.1672938210.0000000007430000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000005.00000002.1672938210.0000000007430000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000005.00000002.1672938210.0000000007430000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000005.00000002.1678278264.0000000008B45000.00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000005.00000002.1672938210.0000000007430000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.75.122.11	rs6.net	United States		40444	ASN-CCUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385476
Start date:	12.04.2021
Start time:	15:18:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://r20.rs6.net/tn.jsp?f=001UR9DU5DWULSSQKRSbHmS5tW1BYzJdf5a5nCBJP8j6WTiQVP7-HJVYmCgrw0XB_uf_QV56Haa_M0mobYIQXKQSaOe6Xu-1xTkGHmKJGzfmmZ2amUpZf-ss1HRg0GxKivYopLHGEV8UEW0_6cIw3aFuQi_2vwTONr1CLcH72kMluSyn6F3FeMZ-MnNHeyuCyEwaUdYWjqc4gJLjgQuRM_rdz9h3O3GIfxNvpPnSjOOSeM=&c=5vPu-3Qs9yW2IEWn1dtOMdgOR2JdmjhB8RamT_IPEu6k3Sz7qp1rDA==&ch=t9Qhnt_2hiJ7oXunOWnQpfuylRuTM4kuFHw1DTZGabFSxZ_AG1kZXw==
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:	40
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@7/16@3/1
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 93.184.220.29, 88.221.62.148, 92.123.150.225, 20.82.210.154, 92.122.145.220, 104.43.139.144, 104.126.36.242, 104.126.36.139, 13.64.90.137, 184.30.24.56, 13.88.21.125, 40.88.32.150, 152.199.19.161, 20.50.102.62, 104.43.193.48, 205.185.216.42, 205.185.216.10, 92.122.213.247, 92.122.213.194, 20.54.26.129, 52.155.217.156, 20.190.159.131, 40.126.31.5, 40.126.31.9, 20.190.159.135, 20.190.159.133, 40.126.31.140, 40.126.31.3, 40.126.31.2, 51.11.168.232, 40.127.240.158, 20.49.150.241, 20.82.209.183 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, e13551.dscg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, e73586.dscf.akamaiedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.net, www.tm.lg.prod.aadmsa.trafficmanager.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, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, msagfx.live.com-6.edgekey.net, e12564.dspb.akamaiedge.net, authgfx.msa.akadns6.net, go.microsoft.com, arc.trafficmanager.net, wildcard-prod.constantcontact.com.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, cds.d2s7q6s2.hwcdn.net, login.msa.msidentity.com, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.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.{168DA7A1-9BDD-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8708124467696718
Encrypted:	false
SSDEEP:	96:rKZlZM2UW9tlbf13gKMwYqw+QcYqwLtA3P63:rKZlZM2UW9t5f1VMOyq4tAy3
MD5:	16F02D910645F8E230FB24B28C88B711
SHA1:	BA30D4CA23B6A24A4460ECD06499C6B31F97C7E8
SHA-256:	E664293A538FD07176EE4DB354A4FFE6337FA787FB27FDEB7A2BBCDB74BA85E9
SHA-512:	1437152554FA4AE8C832EDBF73034B0E04BD368A9777334D53A0B1F4C593724B513C9947AE36ECA0693DDC9E6332ACB66665DEDA9881879F9FB36FB5BAEDEA5D
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\{168DA7A3-9BDD-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24284
Entropy (8bit):	1.6541948934546493
Encrypted:	false
SSDEEP:	48:IwnGcpryGwpa2G4pQnGrapbSEGQpBuGHHpckTGUp8RGzYpm+cGop+mIRPZ3oGuwg:rNZ6QG67BScj92cWfMrMmeZg
MD5:	89DE463AE9743F7BF96EDA292B7BEE9D
SHA1:	3D72B09F14869320F0EA241D0374B359AA33F0EC
SHA-256:	28AC3F6C6446DEA2A58A6D02A38FE53AA2B999AA717AFBFB1F9C29F68A16B399
SHA-512:	0CCD482A9012F0EA3F56F0EC5630142FD6F7378FBAD994DB9B7AC0051840C7258E69F1ED3439C34B36F77F69C7A9C0BA561F79D9F61D09FBFA8AF9B119879B0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{168DA7A3-9BDD-11EB-90E5-ECF4BB570DC9}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{168DA7A4-9BDD-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5646024253807025
Encrypted:	false
SSDEEP:	48:IwuGcprDGwpauG4pQuGrapbSQGQpKJG7HpReTGIpG:ryZdQO6gBSYAoTaA
MD5:	CD29891A5996CEBA2CC31B73C71EE18C
SHA1:	E0539BD23B73CD6F5CFBBDFD84C6A73B3BD22751
SHA-256:	F9540FBA48D6AA37E443FAEB1980A3315438D720C9AE8ECA559092E15477151E
SHA-512:	B3C266FBB0296D54D6CA9D7C55C0D66E0C66A7273574996A355709A40E39172898017A21B8E60481D10C73E1BCE1690A851DC4D42A769B0BAC734862641E9066
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):	657
Entropy (8bit):	5.068109153784606
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEVnWimI002EtM3MHdNMNxOEVnWimI00ONVbkEtMb:2d6NxOcSZHKd6NxOcSZ7Qb
MD5:	25C645E3AD6A9AD4AFEC68ABB20E5EFD
SHA1:	7CB048800151597F1D5EF84AA7A3442F22214AA9
SHA-256:	D8CED8F382AB5849352B5BE30A8F1BDBE6F4667CE540E00BC54F7B351CA3BA1D
SHA-512:	556AA39E14AF5EE13D374F181AEA0BCF08DB3D4777887A44AFD4799D73D21356BD4538B1B7A76A6A0E30EEAD3B3145271F09A6F451459525B4876B0E03C2F970
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xecdff36b,0x01d72fe9</date><accdate>0xecdff36b,0x01d72fe9</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>0xecdff36b,0x01d72fe9</date><accdate>0xecdff36b,0x01d72fe9</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):	654
Entropy (8bit):	5.086800203213303
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kJicnWimI002EtM3MHdNMNxe2kJicnWimI00ONkak6EtMb:2d6Nxr4SZHKd6Nxr4SZ72a7b
MD5:	09F96910DE1B342B88D861D9BF133AFF
SHA1:	32A4E09A837096A5A039971A83CFEB9975397D57
SHA-256:	368D2A752FCA1AB5C12563663CA8BF63934F66E0A0F3AF1357D0CEB300F4A185
SHA-512:	EFA22078D2A8BD231316339F3F32D155E06615546553566A5EBF120BA8E61F42FB3258D3E6CC1549AE4ADC72E90666AD95C98B28DE89F28340B3CE1AA2E67E19
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xecd407a9,0x01d72fe9</date><accdate>0xecd407a9,0x01d72fe9</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>0xecd407a9,0x01d72fe9</date><accdate>0xecd407a9,0x01d72fe9</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):	663
Entropy (8bit):	5.078758498126462
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLbnWimI002EtM3MHdNMNxvLbnWimI00ONmZEtMb:2d6NxvnSZHKd6NxvnSZ7Ub
MD5:	BD3C3AEFC8305082525F992C2F95C9F5
SHA1:	474D35C0529E04F315A02C6DC752D76801996E2A
SHA-256:	8E97786E87032B5AC8F70229E7E98990DF737E3C3044470C8B2B12C2334F1D7D
SHA-512:	22F41F6D24BCBEEB096C1C1041ADE82E2474151D85366FFF476ABEAB0410ABC8CB620C735433CD2C39E166C1047999A90E293016BFC6F4CDDC82C5B8B7899AB
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xece255ab,0x01d72fe9</date><accdate>0xece255ab,0x01d72fe9</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>0xece255ab,0x01d72fe9</date><accdate>0xece255ab,0x01d72fe9</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):	648
Entropy (8bit):	5.060381646561089
Encrypted:	false
SSDEEP:	12:TMHdNMNxiYJOsJO/nWimI002EtM3MHdNMNxiYJOsJO/nWimI00ONd5EtMb:2d6NxrJOsJO/SZHKd6NxrJOsJO/SZ7n/
MD5:	C8750D56F64FBFB7428053859BBEB97F
SHA1:	EEE5564A00E06791F7404BA9DB1E62A514F3261F
SHA-256:	ADF78E35A808FF5ED670FAC00CFF5D81E2EEFF4214975268A5029BDEC910A5C5
SHA-512:	4E70FF1F169B98D8ACC3122DF4102F4DFD63400270AF0F2886491DC57299B7312CA2950E636AC210E59451B9C18F6BCBED845786E01A0BB6C86D73C56FE4C72
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xecdd910b,0x01d72fe9</date><accdate>0xecdd910b,0x01d72fe9</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>0xecdd910b,0x01d72fe9</date><accdate>0xecdd910b,0x01d72fe9</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):	657
Entropy (8bit):	5.089818035900865
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwbnWimI002EtM3MHdNMNxhGwbnWimI00ON8K075EtMb:2d6NxQuSZHKd6NxQuSZ7uKajb
MD5:	A938C4165D344478C3B0E654B0B5BD05
SHA1:	6EAC06E31B1254CC4697C365A14A429936D1FE8D
SHA-256:	8CA9824AD8AF4CA8F844B530437CC5D4830BA47BF5937B4A27F3E7B9A9662EF0
SHA-512:	84A1987779FE19E9FC3BF5F9E94E0A07FB1D490C30E039477E3CB093A79833681CFED4BC846F3C5E648AF3B25C54D2C9F91FB17C38F1D8E4EFED2A7591AF498C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xece255ab,0x01d72fe9</date><accdate>0xece255ab,0x01d72fe9</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>0xece255ab,0x01d72fe9</date><accdate>0xece255ab,0x01d72fe9</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):	654

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Entropy (8bit):	5.069190638690861
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nVnWimI002EtM3MHdNMNx0nVnWimI00ONxEtMb:2d6Nx0VSZHKd6Nx0VSZ7Vb
MD5:	C89C9455EE6F67C0046C07AAFBA37EA0
SHA1:	30705122D640E2F6FB508DA99ABB72D6BFC73A00
SHA-256:	D0497D6FD42689EB52675A755F7A08F7BDCC616279986465A8C8C176C9942E3A
SHA-512:	EF465D881F78B984317A801E6314846F408F41899AD079BBB1197C1A6E42E77FD24AA96CD28E59D180AEBBC3EE1D830DCD47D7E913D957C887780A33762751FI
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xecdff36b,0x01d72fe9</date><accdate>0xecdff36b,0x01d72fe9</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>0xecdff36b,0x01d72fe9</date><accdate>0xecdff36b,0x01d72fe9</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):	657
Entropy (8bit):	5.09617646976543
Encrypted:	false
SSDEEP:	12:TMHdNMNxxYJOsJO/nWimI002EtM3MHdNMNxxYJOEnWimI00ON6Kq5EtMb:2d6NxSJOsJO/SZHKd6NxSJOESZ7ub
MD5:	441D5EB912E5B6E908516B5E3D922AA3
SHA1:	702AF7094DE2D8392CABC0E63172E4EA09BF083F
SHA-256:	940F5FDECD31CCC6DD477D0D71117543CC9F22900CC7D9DCAD98AC9128432841
SHA-512:	4CCC108D2E63B6F01175339FA4C1F0760AA0294BA8F2563B8CD7217F0EFF4E45B3541C252A0CDA66891C3A55425F9728F3E59F14145B54DFB1B9B3C931E508F8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xecdd910b,0x01d72fe9</date><accdate>0xecdd910b,0x01d72fe9</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>0xecdd910b,0x01d72fe9</date><accdate>0xecdff36b,0x01d72fe9</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):	660
Entropy (8bit):	5.05279294778761
Encrypted:	false
SSDEEP:	12:TMHdNMNxcJ6cnWimI002EtM3MHdNMNxcJ6cnWimI00ONVEtMb:2d6Nxs6cSZHKd6Nxs6cSZ71b
MD5:	9B207810D05F7D05EE644D556B777E3E
SHA1:	F2DD167CB7421494128F5CCE2C0D6453D9E4FE98
SHA-256:	127E2CE59C8F02E12767D97928289A56A8F72CFAEAFB250D0E5C71A2BCD9DE38
SHA-512:	F8DD7CBD8877CD3D5844A7B7A733F711E3F0104A2F686819FDE927FC4FA2469E4D179865E63F2DBB5B19AC473DBEFC13C0AB3290BBE43F51A61B6CF844A9D45
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xecdb2ec1,0x01d72fe9</date><accdate>0xecdb2ec1,0x01d72fe9</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>0xecdb2ec1,0x01d72fe9</date><accdate>0xecdb2ec1,0x01d72fe9</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):	654
Entropy (8bit):	5.046106913945248
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnYJOsJO/nWimI002EtM3MHdNMNxfnYJOsJO/nWimI00ONe5EtMb:2d6NxQJOsJO/SZHKd6NxQJOsJO/SZ7E/
MD5:	7DBD3334977F25D96970181192621C6E
SHA1:	37EE05EE585D82A1412A52396B1E807184F6F568

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA-256:	BA71CA56B9512AF0849F43DD2CB912E0147D4499D3383F7B2BE7B1E9B126F116
SHA-512:	A2CFCCF8FD4A4F73B47A69910888D59E690CD746508AE87F5A1E73DE5EA3FA5A3371F368C46C309E9B9CBA9D2206435073D1528920ACE4404045F6498FC2AF5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xecdd910b,0x01d72fe9</date><accdate>0xecdd910b,0x01d72fe9</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>0xecdd910b,0x01d72fe9</date><accdate>0xecdd910b,0x01d72fe9</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\FOREIGN NATIONAL MAY 19[1].PDF	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PDF document, version 1.4
Category:	dropped
Size (bytes):	380221
Entropy (8bit):	7.870253128299
Encrypted:	false
SSDEEP:	6144:LH99lF27Z3muoJm47QrCCCxplY8rOqagivFXRmNBvC0qgptotTfPA2/KnkTCez:BvFXQrCCCxiKgiYNBVzYLPAsT1
MD5:	7CEE0CC3667DC762E921DC006870B895
SHA1:	37867E09FE1523D1D93FDBC22CCCF6EDD239F3C4
SHA-256:	3EFA37CB85D44EE6AFB881863BA35EAC6C83BABD65B2BDD179DAB6B3BF710611
SHA-512:	F5468455B50B977E5D706D90A5F8BCC5B389A883F19ED1EBD7F4ECE61C936E2200969C29CF868218379CD137873E80500883DB5FC7A0DCD7286CC1D8A02E226
Malicious:	false
Reputation:	low
Preview:	%PDF-1.4.%.....1 0 obj.<<./Type /Catalog./Pages 2 0 R.>>.endobj.3 0 obj.<<./Creator (Canva)./Producer (Canva)./CreationDate (D:20200512072550+00'00')./ModDate (D:20200512072549+00'00')./Keywords (DADfsHXOwPo,BADIiQWyoa4)./Author (excwrk5)./Title (Commercial flyer).>>.endobj.2 0 obj.<<./Type /Pages./Count 1./Kids [4 0 R].>>.endobj.4 0 obj.<<./Type /Page./Resources <<./ProcSets [/PDF /Text /ImageB /ImageC /ImageI]./ExtGState <<./G3 5 0 R.>>./XObject <<./X5 6 0 R./X9 7 0 R.>>./Font <<./F4 8 0 R./F6 9 0 R./F7 10 0 R./F8 11 0 R.>>.>>./MediaBox [0.0 7.9199977 360.0 511.91998]./Contents 12 0 R./StructParents 0./Parent 2 0 R./BleedBox [0.0 7.9199977 360.0 511.91998]./TrimBox [0.0 7.9199977 360.0 511.91998].>>.endobj.5 0 obj.<<./ca 1./BM /Normal.>>.endobj.6 0 obj.<<./Length 298844./Type /XObject./Subtype /Image./Width 1023./Height 680./ColorSpace /DeviceRGB./BitsPerComponent 8./Filter /DCTDecode./ColorTransform 0.>>.stream.....JFIF.....C..... .....

C:\Users\user\AppData\Local\Temp\~DF0BE9630EA18F6468.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34477
Entropy (8bit):	0.37129571299060793
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw8F9lwli9l2K9l2q9lu:kBqoxKAuvScS+vRT6+I+ImIRPZ3W
MD5:	283F1781A03758B6D92462223056DA78
SHA1:	1A2CF458ADB591E99AD7743FF33613AD8163D073
SHA-256:	01E780B7710B61256EF17C9E53D4BFB0BBDD59D9774683B05507332E55D50348
SHA-512:	0F8C93AC377CB011F274039C5084002A020D717DDF5D08CB03628C83AC766C45CB4A366C0FE1CED324DB47222F6B875F989B78C98458A4703768E9A96CC50DA
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF0DA265B4E0FD1AC2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5132048052970682
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loD9loD9lWkOQOY:kBqoIkakR1
MD5:	B2EA602620B46AC16A3C3D179FF1BD28
SHA1:	3B78CA602D2B8FA1BA0B5D970D92282461A1DC98
SHA-256:	565B3E5AF95DB8225230C22BDF7F1AB3BB1D3F6684CCD53E2CD8EF1FBFE55CB3
SHA-512:	64FF482E761B1F9919F9E5E5E269A7811457273B5D16398110113FCC43862BFCEEDCCF8A1CEE9F0EE4EC750D7805976FE224AEC09DFCA34FA156DB61AAA569A1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF0DA265B4E0FD1AC2.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

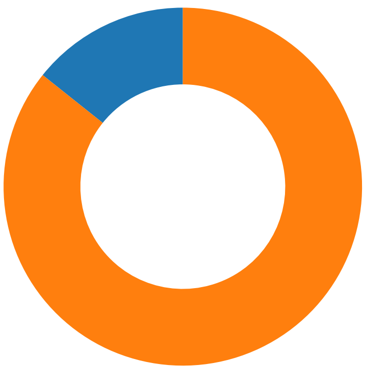
C:\Users\user\AppData\Local\Temp\~DF94FD20260357933D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.32289858027910606
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAWSC:kBqoxxJhHWSVSEabWSC
MD5:	9FEC8EC4CADDDD7B70105CB782B5B2B0
SHA1:	4B900E6940FEA009F41A0AE2D96383B30514A874
SHA-256:	3FD713D792171A7D94CE16DB87C092B4383B99D9422383C3157F120347D26F24
SHA-512:	B702C607049AD451F931FC7C6DF0E753F19E7E810A126879B44A4853248710466301E1ED2A7293623D50C2BDAD3A33E384C0EB5F95CA59BBC23373A1027D5F73
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



Total Packets: 63

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:19:06.788369894 CEST	49702	80	192.168.2.5	208.75.122.11
Apr 12, 2021 15:19:06.788968086 CEST	49703	80	192.168.2.5	208.75.122.11
Apr 12, 2021 15:19:06.917009115 CEST	80	49703	208.75.122.11	192.168.2.5
Apr 12, 2021 15:19:06.917041063 CEST	80	49702	208.75.122.11	192.168.2.5
Apr 12, 2021 15:19:06.917164087 CEST	49703	80	192.168.2.5	208.75.122.11
Apr 12, 2021 15:19:06.917529106 CEST	49702	80	192.168.2.5	208.75.122.11

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:19:06.917999983 CEST	49703	80	192.168.2.5	208.75.122.11
Apr 12, 2021 15:19:07.052350044 CEST	80	49703	208.75.122.11	192.168.2.5
Apr 12, 2021 15:19:07.060214996 CEST	80	49703	208.75.122.11	192.168.2.5
Apr 12, 2021 15:19:07.060235023 CEST	80	49703	208.75.122.11	192.168.2.5
Apr 12, 2021 15:19:07.060321093 CEST	49703	80	192.168.2.5	208.75.122.11
Apr 12, 2021 15:19:07.075143099 CEST	49703	80	192.168.2.5	208.75.122.11
Apr 12, 2021 15:19:07.202436924 CEST	80	49703	208.75.122.11	192.168.2.5
Apr 12, 2021 15:20:56.217231989 CEST	49702	80	192.168.2.5	208.75.122.11
Apr 12, 2021 15:20:56.344779015 CEST	80	49702	208.75.122.11	192.168.2.5
Apr 12, 2021 15:20:56.344806910 CEST	80	49702	208.75.122.11	192.168.2.5
Apr 12, 2021 15:20:56.345072031 CEST	49702	80	192.168.2.5	208.75.122.11

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:18:57.195163965 CEST	52704	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:18:57.252574921 CEST	53	52704	8.8.8.8	192.168.2.5
Apr 12, 2021 15:18:57.385423899 CEST	52212	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:18:57.434305906 CEST	53	52212	8.8.8.8	192.168.2.5
Apr 12, 2021 15:18:57.701565981 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:18:57.764841080 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 12, 2021 15:18:57.991409063 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:18:58.049997091 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 12, 2021 15:18:58.338965893 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:18:58.372776985 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:18:58.404958963 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 12, 2021 15:18:58.421545982 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:00.719647884 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:00.780303001 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:05.471481085 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:05.533642054 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:06.712677002 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:06.774744034 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:06.802594900 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:06.851794004 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:07.080960035 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:07.142441034 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:09.328388929 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:09.390604973 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:26.886754990 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:26.949954987 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:31.844438076 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:31.897313118 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:33.030312061 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:33.079998970 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:34.096780062 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:34.149822950 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:35.488280058 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:35.538528919 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:36.260453939 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:36.309067965 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:36.503468990 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:36.552143097 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:37.257545948 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:37.315336943 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:37.503601074 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:37.563009977 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:38.269494057 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:38.318314075 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:39.519500971 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:39.568207979 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:40.269707918 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:40.326908112 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:43.597547054 CEST	63183	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:19:43.646311998 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:44.285749912 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:44.343308926 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:44.868835926 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:44.920469999 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:47.156686068 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:47.205323935 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:48.541523933 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:48.593079090 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:49.743335009 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:49.800481081 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:51.022154093 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:51.073843002 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:53.560250998 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:53.608885050 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:54.259708881 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:54.308511972 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 12, 2021 15:19:55.596672058 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:19:55.645845890 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 12, 2021 15:20:17.141606092 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:20:17.199884892 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:00.270756960 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:00.322156906 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:29.189321995 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:29.261440039 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:48.415178061 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:48.477737904 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:49.512181044 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:49.587318897 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:50.861028910 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:50.933968067 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:51.626597881 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:51.686646938 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:52.233217955 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:52.293164015 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:52.934613943 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:53.011869907 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:54.046004057 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:54.096122026 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:55.766287088 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:55.823585987 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:57.158423901 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:57.207694054 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 12, 2021 15:21:57.872054100 CEST	51649	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:21:57.929920912 CEST	53	51649	8.8.8.8	192.168.2.5
Apr 12, 2021 15:23:54.075620890 CEST	65086	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:23:54.136023998 CEST	53	65086	8.8.8.8	192.168.2.5
Apr 12, 2021 15:23:55.310157061 CEST	56432	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:23:55.380156040 CEST	53	56432	8.8.8.8	192.168.2.5
Apr 12, 2021 15:24:03.221530914 CEST	52929	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:24:03.290947914 CEST	53	52929	8.8.8.8	192.168.2.5
Apr 12, 2021 15:24:07.987732887 CEST	64317	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:24:08.055860043 CEST	53	64317	8.8.8.8	192.168.2.5
Apr 12, 2021 15:24:08.412378073 CEST	61004	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:24:08.469455957 CEST	53	61004	8.8.8.8	192.168.2.5
Apr 12, 2021 15:26:37.848639965 CEST	56895	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:26:37.897789001 CEST	53	56895	8.8.8.8	192.168.2.5
Apr 12, 2021 15:27:12.401345968 CEST	62372	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:27:12.466770887 CEST	53	62372	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:18:57.991409063 CEST	192.168.2.5	8.8.8.8	0xa5d4	Standard query (0)	clientconf ig.passport.net	A (IP address)	IN (0x0001)
Apr 12, 2021 15:19:06.712677002 CEST	192.168.2.5	8.8.8.8	0x5090	Standard query (0)	r20.rs6.net	A (IP address)	IN (0x0001)
Apr 12, 2021 15:19:07.080960035 CEST	192.168.2.5	8.8.8.8	0x6feb	Standard query (0)	files.constantcontact.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:18:58.049997091 CEST	8.8.8.8	192.168.2.5	0xa5d4	No error (0)	clientconf ig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:19:06.774744034 CEST	8.8.8.8	192.168.2.5	0x5090	No error (0)	r20.rs6.net	rs6.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:19:06.774744034 CEST	8.8.8.8	192.168.2.5	0x5090	No error (0)	rs6.net		208.75.122.11	A (IP address)	IN (0x0001)
Apr 12, 2021 15:19:07.142441034 CEST	8.8.8.8	192.168.2.5	0x6feb	No error (0)	files.constantcontact.com	wildcard-prod.constantcontact.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:23:54.136023998 CEST	8.8.8.8	192.168.2.5	0x9830	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- r20.rs6.net

HTTP Packets

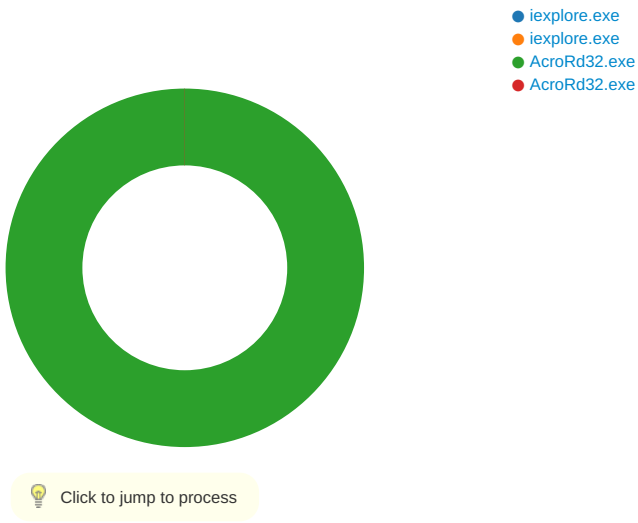
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49703	208.75.122.11	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:19:06.917999983 CEST	1316	OUT	GET /tn.jsp?f=001UR9DU5DWULSSQKRSbHmS5tW1BYzJdf5a5nCBJP8j6WTiQVP7-HJVYmCgrw0XB_uf_QV56Haa_M0mobYIQXKQSaOe6Xu-1xTkGHmKJGzfmmZ2amUpZf-ss1HRg0GxKivYopLHGEV8UEW0_6cIw3aFuQi_2vwTONr1CLcH72kMluSyn6F3FeMZ-MnNHeyuCyEwaUdYWjqc4gJLjgQuRM_rdz9h3O3GIfxNvpPnSjOOSeM=&c=5vPu-3Qs9yW2IEWn1dtOMdgOR2JdmjhB8RamT_IPEu6k3Sz7qp1rDA==&ch=t9Qhnt_2hiJ7oXunOWnQpfuylRuTM4kuFHw1DTZGabFSxZ_AG1kZXw== HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: r20.rs6.net Connection: Keep-Alive
Apr 12, 2021 15:19:07.060214996 CEST	1349	IN	HTTP/1.1 302 Found Date: Mon, 12 Apr 2021 13:19:06 GMT Server: Apache P3P: CP="CAO DSP TAIa OUR NOR UNI" Location: https://files.constantcontact.com/54e1b5c9701/a2191b8c-25d2-4fe8-aff0-8b4735afdc69.pdf Content-Length: 0 Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate, no-cache="Set-Cookie" Pragma: no-cache Connection: close Content-Type: text/html;charset=ISO-8859-1

Code Manipulations

Statistics

Behavior



System Behavior

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

General

Start time:	15:19:03
Start date:	12/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff73e7b0000
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: 5904 Parent PID: 5620

General

Start time:	15:19:04

Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5620 CREDAT:17410 /prefetch:2
Imagebase:	0xbf0000
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

Analysis Process: AcroRd32.exe PID: 3100 Parent PID: 5904

General

Start time:	15:19:07
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' /o /eo /l /b /ac /id 5904
Imagebase:	0x320000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3565C3	CreateDirectoryExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\Device\NamedPipe\AIPC_SRV\AcroSBL_5904_3100	unknown	1040	success or wait	4	385549	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	36CF19	RegCreateKeyW

Analysis Process: AcroRd32.exe PID: 5680 Parent PID: 3100

General

Start time:	15:19:08
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 /o /eo /l /b /ac /id 5904
Imagebase:	0x320000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
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	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis