ID: 411367
Cookbook: browseurl.jbs
Time: 20:32:53
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

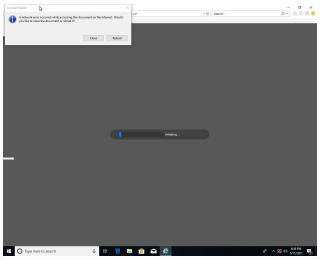
Analysis Report http://louisville.edu/coronavirus/assets…

Overview

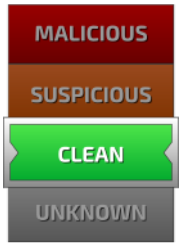
General Information

Sample URL:	http://louisville.edu/coronavirus/assets/Dec12020InterimPolicyforUniversityTravel.pdf
Analysis ID:	411367
Infos:	

Most interesting Screenshot:



Detection

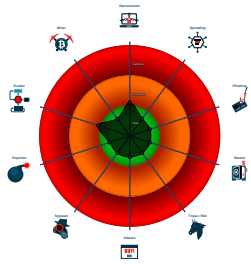


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Contains functionality to access load…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5916 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4552 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5916 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - AcroRd32.exe (PID: 5140 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' /o /eo /l /b /ac /id 4552 MD5: B969CF0C7B2C443A99034881E8C8740A)
      - AcroRd32.exe (PID: 5452 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 /o /eo /l /b /ac /id 4552 MD5: B969CF0C7B2C443A99034881E8C8740A)
- **cleanup**

Malware Configuration

No configs have been found

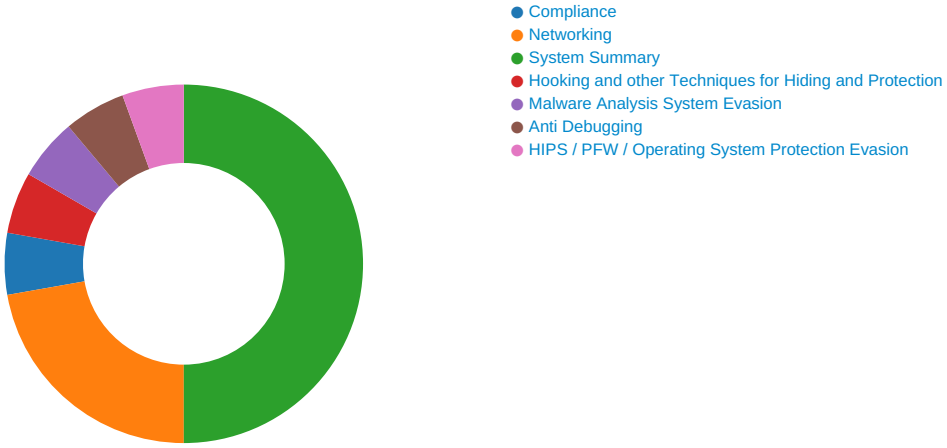
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



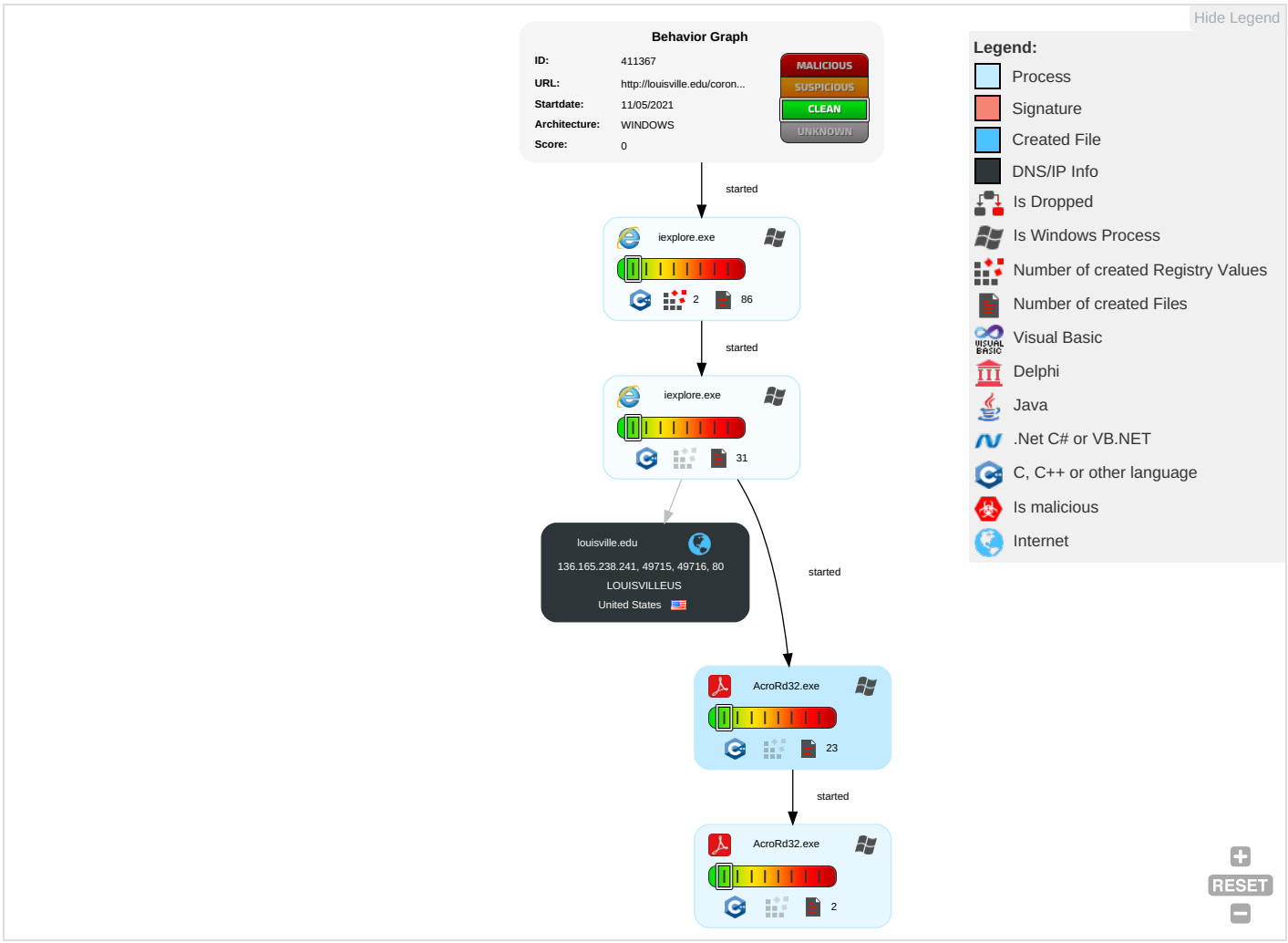
Click to jump to signature section

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
Spearphishing Link 1	Windows Management Instrumentation	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Process Discovery 2	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
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
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

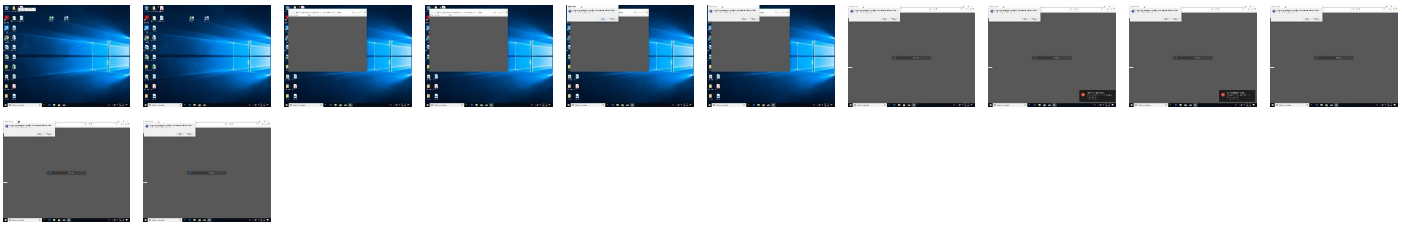
Behavior Graph

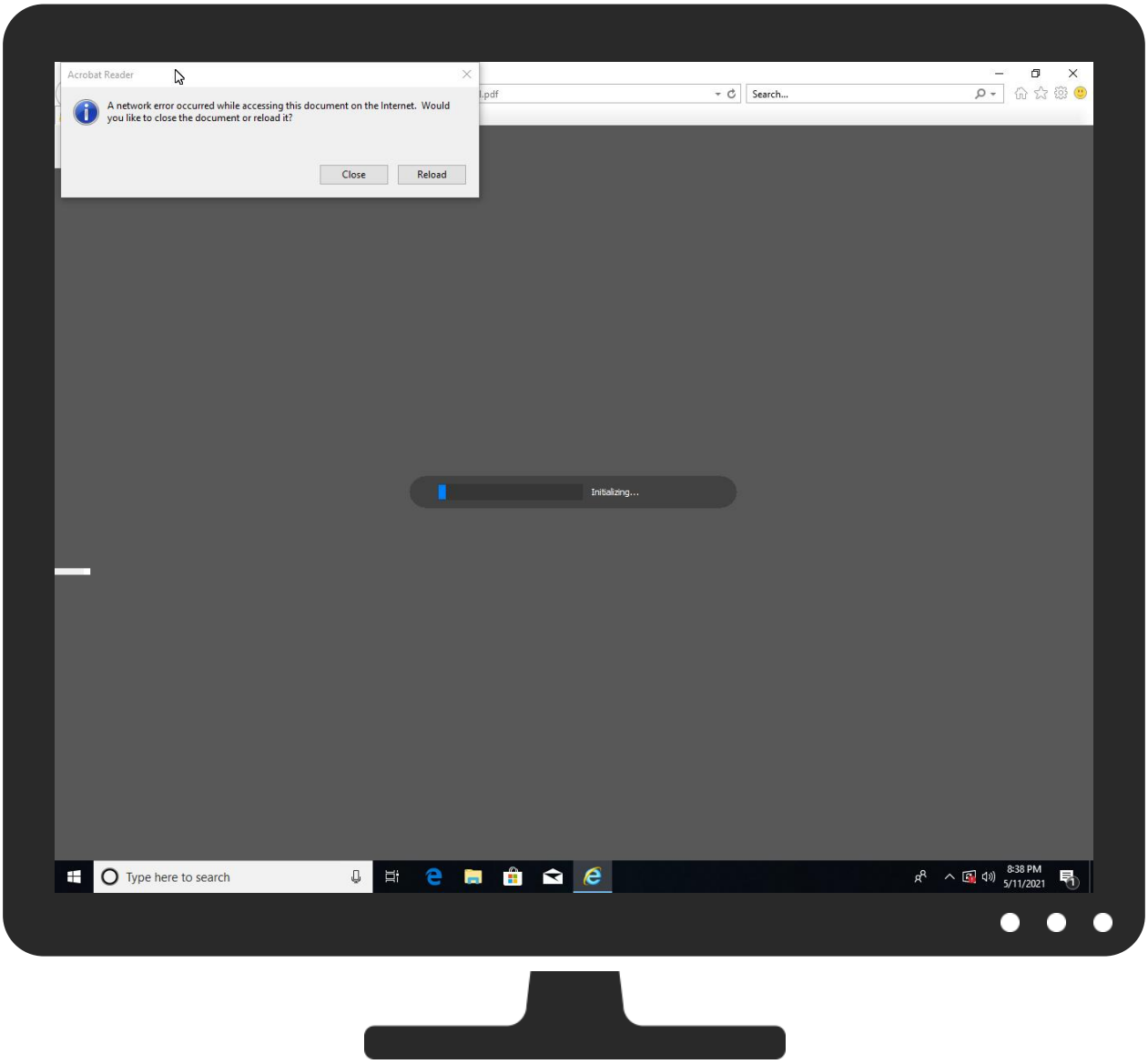


Screenshots

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://louisville.edu/coronavirus/assets/Dec12020InterimPolicyforUniversityTravel.pdf	0%	Virustotal		Browse
http://louisville.edu/coronavirus/assets/Dec12020InterimPolicyforUniversityTravel.pdf	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	

Source	Detection	Scanner	Label	Link
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/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/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/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$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$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.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.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.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	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
louisville.edu	136.165.238.241	true	false		high

Contacted URLs

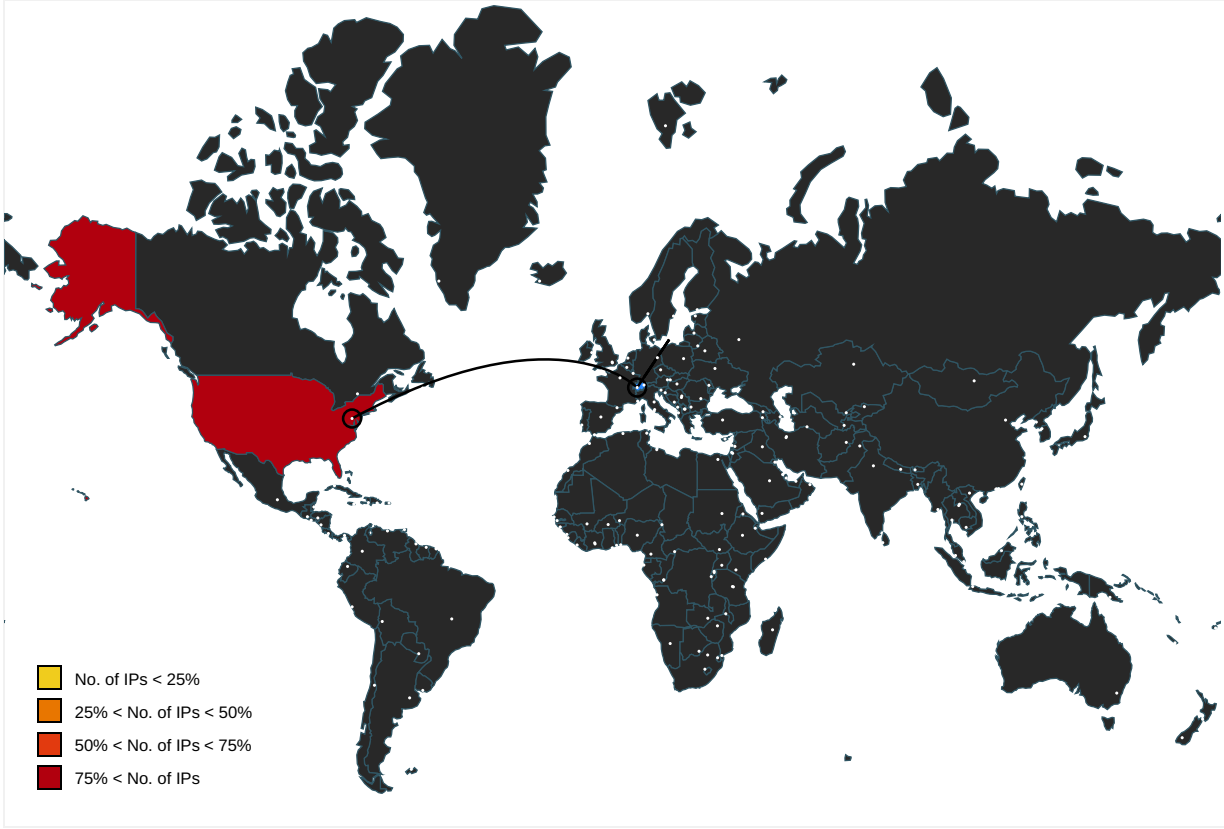
Name	Malicious	Antivirus Detection	Reputation
http://louisville.edu/coronavirus/assets/Dec12020InterimPolicyforUniversityTravel.pdf	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.louisville.edu/coronavirus)	AcroRd32.exe, 00000004.00000002.1661021220.0000000009998000.00000004.00000001.sdmp, Dec 1 2020 - Interim Policy for University Travel[1].pdf.2.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://louisville.edu/coronavirus/assets/Dec12020InterimPolicyforUniversityTravel.pdfs	AcroRd32.exe, 00000004.00000002.1660481864.0000000009794000.00000004.00000001.sdmp	false		high
http://https://ims-na1.adobelogin.com:	AcroRd32.exe, 00000004.00000002.1660857750.0000000009950000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000004.00000002.1653199339.0000000008030000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://louisville.edu/coronavirus/assets/Dec12020InterimPolicyforUniversityTravel.pdfRoot	{D9051C57-B2D2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000004.00000002.1653199339.0000000008030000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://forms.office.com/Pages/ResponsePage.aspx?id=Sm4k3TRUFU6K45Gtl5eyCSa4a5uPy2ZEov0th0MezgJUN0NK	Dec 1 2020 - Interim Policy for University Travel[1].pdf.2.dr	false		high
http://louisville.edu/studyabroad/policies/travel-warning-policy)	Dec 1 2020 - Interim Policy for University Travel[1].pdf.2.dr	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000004.00000002.1653199339.0000000008030000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000004.00000002.1653199339.0000000008030000.00000002.00000001.sdmp	false	• URL Reputation: safe • 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, 00000004.00000002.1653199339.0000000008030000.00000002.00000001.sdmp	false	• URL Reputation: safe • 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 • 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, 00000004.00000002.1653199339.0000000008030000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000004.00000002.1653199339.0000000008030000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000004.00000002.1660857750.0000000009950000.00000004.00000001.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, 00000004.00000002.1653199339.0000000008030000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
136.165.238.241	louisville.edu	United States		1657	LOUISVILLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411367
Start date:	11.05.2021
Start time:	20:32:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://louisville.edu/coronavirus/assets/Dec12020InterimPolicyforUniversityTravel.pdf
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@7/17@1/1
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

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.{D9051C55-B2D2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	36440
Entropy (8bit):	1.8880688792959317
Encrypted:	false
SSDEEP:	96:r2ZZZk2cWOMtOzfO2BMOqjOqIOqrOqtOq8fOqd8X:r2ZZZk2cWrt8f/BMpjpIprptp8fpd8X
MD5:	03C6C287F3B033DFF4B8DB78D7230C52
SHA1:	ED93357D6D3A37BBD854E1C79A900D9F8EA878B5
SHA-256:	2B6D7B446B599492541E869E44B789A80F430929C8C988C81E0191A85E0713FC
SHA-512:	45EBF88173055660B005914475E8F4AE098F1758D67BD9B2172E9D2C5248C29FEB7EA52096489FF7D49A0FED116444A493C639E4E5BE190A5DF210928B2E54E6
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\{D9051C57-B2D2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24280
Entropy (8bit):	1.6532995324916002
Encrypted:	false
SSDEEP:	48:Iw7GcpreGwpaSG4pQSGrapbScGQpBCGHHpcjTGUp8QGzYpm7HoGoptVsbG6Npm:rhZWQi6UBS0jZ29WkM7ojStg
MD5:	11590ACBB4BBC2652A84BF459E3BBA1F
SHA1:	6E46F385BFE26436FF4D392A8F198635B38FC81A
SHA-256:	99470707D44999BE757DD61D680946EC3B82D44BB161AF5965EF1AEA47588BC9
SHA-512:	2162DDE1F306719F80AA665FC3C4756F0074B4F1B8AB6634A1988EE82D0A3C48D8D62C88BEAF8C7A4E83EC18EAF45E41C2A9A90E9FC6816ED2E5C58285221A 8
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\{D9051C58-B2D2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565792769306293
Encrypted:	false
SSDEEP:	48:IwkGcprZGwpa8G4pQMGrapbSDGQpKXG7HpRoTGIpG:r4ZTQc6KBS9A2TsA
MD5:	7A58ACDC00F9DE3D3A8AEBC52023B5F5
SHA1:	04D541AC2542DD7445515D85C3DABD91C05FEFAA
SHA-256:	4F251B2BFEA41B7B278138BACC56FB0F6C932F10BBFBB32BD83F4C5C9B6B384C
SHA-512:	F7B3F46894AA14F71777709827C04B394380C9ECB683DBD86581E553B2CC706F5E8752EC3D69AEFC5B9579D675ABA510C3D81897CA6C0A71599C2C9C2D8B099
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.06320493364117
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEwDYBDjnWimI002EtM3MHdNMNxOEwDYBDjnWimI00ObVbkEtMb:2d6NxOzQjSZHKd6NxOzQjSZ76b
MD5:	97182FB7867A4AD6E78E2FFF5043FB47
SHA1:	3410EB7ACC90AEF9BFA59FAEFE360B4BC22E2846
SHA-256:	AF3C56F70A40AFE084CF32B43479CAB54311F22AFC1682EDC2E8A9C9B5D9AF50
SHA-512:	6D3FC406247AB0580868F377BF8AFEB27831FB458F4E208981580E6A016A49FB965E82176B7E606FBE9A80BA4901E72C20380216AC7C113169E0FA2E6F5BDB80
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xaefc1cd2,0x01d746df</date><accdate>0xaefc1cd2,0x01d746df</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>0xaefc1cd2,0x01d746df</date><accdate>0xaefc1cd2,0x01d746df</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.103142634927204
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SSDEEP:	12:TMHdNMNxe2kwNMBNfnWimI002EtM3MHdNMNxe2kwNMBNfnWimI00Obkak6EtMb:2d6NxrISZHKd6NxrISZ7Aa7b
MD5:	B20DB0D7F299CFF27611CD94A9BB9232
SHA1:	069692348E768E2F2F26CEDB7D2634F495446EB0
SHA-256:	25732DACB3773AB512860946FFA522887F21208A7CEF3ADDCAF21FC8D20603D3
SHA-512:	E0A7B739C38A290F5C48FD478C94F0CE33FCA3258F6E1D1D4DC28DECE714BE37CAB7B47156363E8BBFC456B0639C7A57A914300601189E0745F2C0879E1140C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xaef4f5bf,0x01d746df</date><accdate>0xaef4f5bf,0x01d746df</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>0xaef4f5bf,0x01d746df</date><accdate>0xaef4f5bf,0x01d746df</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.080279154526209
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLwDYBDjnWimI002EtM3MHdNMNxvLwDYBDjnWimI00ObmZEtMb:2d6NxvUQjSZHKd6NxvUQjSZ7mb
MD5:	AEC8609B7B29EFBE6056C8D3E94DF9CD
SHA1:	AD3FA181DE1AC9F1CDEC3F798EB18A9945B2DC01
SHA-256:	BF8F3B20D86E8E5DA7DF8A821E206B5FBF3129F3E0331C6B407B81DE6AE78A1A
SHA-512:	FF25043F1B79959F0D70112CCB297BA43DA9C49453DD0F442ACE8054DE63D5F0EB1CB59675973CA652F6066CD15C4DD04EE03A4E64C187FCE88A65F548BCD88
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xaefc1cd2,0x01d746df</date><accdate>0xaefc1cd2,0x01d746df</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>0xaefc1cd2,0x01d746df</date><accdate>0xaefc1cd2,0x01d746df</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.078530873431818
Encrypted:	false
SSDEEP:	12:TMHdNMNxiwDYBDjnWimI002EtM3MHdNMNxiwDYBDjnWimI00Obd5EtMb:2d6NxtQjSZHKd6NxtQjSZ7Jjb
MD5:	8964DE777205E3831C83A707B0CD13D5
SHA1:	55C7A99B0EE97C251F5303F41B05B65821AC7E4E
SHA-256:	766C9192FB02D8A86B62AC87AFE2EDEC676C614DD0E793DA686FE4A8C94CE6D7
SHA-512:	372CEDD4D93F979F04994E6126C7EB0B3D13D3A769CD57E2B110997AFA5B259071AF395E263225B921F04BD947436630443FAB40AFAFF6556716D2229A5C04DC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xaefc1cd2,0x01d746df</date><accdate>0xaefc1cd2,0x01d746df</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>0xaefc1cd2,0x01d746df</date><accdate>0xaefc1cd2,0x01d746df</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.097967420004993
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwwDYBDjnWimI002EtM3MHdNMNxhGwwDYBDjnWimI00Ob8K075EtMb:2d6NxQXQjSZHKd6NxQXQjSZ7YKajb
MD5:	2DF15EBD274982E0AB3405FC91805BC4
SHA1:	4FB0FFA0E173D84BDA02200657E9EAEDF9B69637
SHA-256:	E8C73CFF3AD09F338D3EE3765CB5DE75F8B3BA699AF47C68B6D1204C657665A2

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
SHA-512:	13E179CD497698304F23FAE6714ACEADFA8C94B575C6A386DB3A0959E4098F4DE0AEFEAACA7DD16972FC554233A6B0F303D43A394BDB22291952D10991EB11D 8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xaefc1cd2,0x01d746df</date> accdate>0xaefc1cd2,0x01d746df</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>0xaefc1cd2,0x01d746df</date><accdate>0 xaefc1cd2,0x01d746df</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.061747821604419
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nwDYBDjnWimI002EtM3MHdNMNx0nwDYBDjnWimI00ObxEtMb:2d6Nx04QjSZHKd6Nx04QjSZ7nb
MD5:	06985B1225A03C1A40FC42A807E3E874
SHA1:	30FA1CA210B71D1EFED6126BE5E4B1096A956BDD
SHA-256:	53C31899C62D705AC12B80C82EC8BFB74A600A5AD573674F52CDB6225C636534
SHA-512:	B2F11CB6B6AC3C78CB83C0ED813FFDC758FD71EE1A0629C26DB22481B06BA56CAC6ACA5347388B964009CAA7CD3EFB4ACE57DDB3F92B9DD490CEE072BE4F 32A8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xaefc1cd2,0x01d746df</date><a ccdate>0xaefc1cd2,0x01d746df</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>0xaefc1cd2,0x01d746df</date><accdate>0xa efc1cd2,0x01d746df</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></ msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.103628634911867
Encrypted:	false
SSDEEP:	12:TMHdNMNxxwDYBDjnWimI002EtM3MHdNMNxxwDYBDjnWimI00Ob6Kq5EtMb:2d6NxeQjSZHKd6NxeQjSZ7ob
MD5:	78E5B3D4B6792F55109A3394DC00111B
SHA1:	B3F77CC3EFF4570D0C1CF4462C1368AD5CA9D104
SHA-256:	0455B866036C4420AC0BE2219E9C346B123A35A6CF7A382351207FEC35DEB65C
SHA-512:	6187716B7BD3430F06135FBE734174B56292B618E0BCA5899A5E920D475488166B5588E61DED9F9EB5CE6EFCD4D44CA31A44B46A3A5B22D28376397F5252CC8F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xaefc1cd2,0x01d746df</date> accdate>0xaefc1cd2,0x01d746df</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>0xaefc1cd2,0x01d746df</date><accdate>0 xaefc1cd2,0x01d746df</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.094317234838545
Encrypted:	false
SSDEEP:	12:TMHdNMNxcwNMBNfnWimI002EtM3MHdNMNxcwNMBNfnWimI00ObVEtMb:2d6NxwSZHKd6NxwSZ7Db
MD5:	526FC0216224127EE4BAA4956DD66C5A
SHA1:	1F8F7EB62F4DF4B8D024C87660CE1C1DCDA575CF
SHA-256:	50439721984984E1E0FB82674D8E858CF07D2CC0A5550A21418BC1B280BB3A31
SHA-512:	125CBE75558D1FE64CF9B450AC9579ADF6F9F315DBC92BDD12A3CA55D326E576336063E23B44479B917848277A840CB1685C06889FBCA63D9105225BEB24EF5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xaef4f5bf,0x01d746df</date><accdate>0xaef4f5bf,0x01d746df</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>0xaef4f5bf,0x01d746df</date><accdate>0xaef4f5bf,0x01d746df</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.064493914043756
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnwDYBDjnWimI002EtM3MHdNMNxfnwDYBDjnWimI00Obe5EtMb:2d6NxwQjSZHKd6NxwQjSZ7ijb
MD5:	41512AA2443DA028B6A40EBA89FE469E
SHA1:	70839999CF7123B86DF7B7590815945254159E9D
SHA-256:	6F266EC16A01DBC3334E042B02CCD356AB3FEC7218A6148E2EFE29CC146F7E2E
SHA-512:	448ECFD731A8170E2788245D746BCE72B054B4AEE4A80EE2817C3BEE565E3D309D9D155FFBF5E0AB44797C1921C7A528A075AA9F6744CB3593D3026A268D818
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xaefc1cd2,0x01d746df</date><accdate>0xaefc1cd2,0x01d746df</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>0xaefc1cd2,0x01d746df</date><accdate>0xaefc1cd2,0x01d746df</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\WJ8I2OL4\Dec 1 2020 - Interim Policy for University Travel[1].pdf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PDF document, version 1.7
Category:	dropped
Size (bytes):	38636
Entropy (8bit):	7.925387978690509
Encrypted:	false
SSDEEP:	768:y0IO9EIBB6IX0H1g39SbuJid3KmGzXEHGvzH9+NXARPTJvZdnRSkFEydtGdtV/yo:ZOIB0dhNwRZTnDq/dCpslFp
MD5:	84B945EA01E67415B849525E3C623CDD
SHA1:	8C2630011FFC04A701561221027451EFD67AD233
SHA-256:	AF7CD94F971A203F204B6C869F6C4E8271B0C2530BA8B4BC26ABF0CBEEBB9DBC
SHA-512:	67EFFE2EC39BCFCBC640271585953B21200A8D3B2141962B1BBB1A8FC6BF660B261DE0F2142D8652F2E1E0BE1892DC1B13781EE3934809592927701E294937DB
Malicious:	false
Reputation:	low
Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 28 0 R/MarkInfo<</Marked true>>/Metadata 101 0 R/ViewerPreferences 102 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 1/Kids[3 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 9 0 R/F3 11 0 R/F4 13 0 R>>/ExtGState<</GS7 7 0 R/GS8 8 0 R>>/XObject<</Meta18 18 0 R>>/ProcSet[/PDF/Text/ImageB/ImageC/ImageI] >>/Annots[19 0 R 20 0 R 21 0 R 22 0 R 23 0 R 24 0 R 25 0 R 26 0 R] /MediaBox[0 0 612 792] /Contents 4 0 R/Group<</Type/Group/S/Transparency/CS/DeviceRGB>>/Tabs/S/StructParents 0>>..endobj..4 0 obj..<</Filter/FlateDecode/Length 4134>>..stream..x....r.6..3..>J..&....x..5.M.icw...A.eG.[RE.....,..=c.....o.....z<Y'.}w..z=.|.^%.N...?O.....w..|..-..7.k..f:...../_$...ei.?#B.,)..jD.....?.$.....G..I2J.....%$).:.,..*.....}..4|..F|.....>.....?..^..~9>z,X....%U.fuR.B....P.W?.HN#8z.X..wq4.^,.{...h.....s....49.|.\.g..U3[?$.!.\'o..Y..g....q.{{!y....|..... 8..I^.u..

C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R4wl84n_777wlx_47g.tmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	modified
Size (bytes):	32768
Entropy (8bit):	**7.994442390753805**
Encrypted:	**true**
SSDEEP:	768:NIecnWYJ9CQYJnK+hRtEZv+XsFfYo/QhvLa9Z4:NHcnW/HxdyZvXmoYhzaw
MD5:	89468E8FFA187D5EC442E0BD15053321
SHA1:	744D9880DB326C75C072C9C499BEB1F5BBA45B2E
SHA-256:	67F852951CD601C7E5AFAEE4222BB892CCE8E1084A4D80CB3DC5542CD5951991
SHA-512:	80A610CE1B463D1C6CCE174A1F916245D574B97C2045C275F2ADC060726ABB5B644EAEA8EAE4916D2C96CF89AABAD0DFAB7DD8FD3A2CCB33DB8D67811748E65D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R4wl84n_777wlx_47g.tmp

Preview:

.}......S.P..i.......IS.6.eO...p...6....c...-.EN);.c.y!..{.'[....V....N...i..E.>...t.#m?.....9.;1....`..!..........[...x......rJ..^1-..8.'...i....+U.+9P.c,L.S.|.Z..w.l.d.(..H.4./..b\v.B....y..il........_q9".8
a0?.J.....dP...t..8..a....#.X..$...(.=...Fl..z.o...f.`_\...z......9.i......VA.....4.T...g.P....~....Y,3.......g..i..h....Mi?..K.,D..P%.l-a'Z..Jw...X....K.L&...q..yW@..{.$.f?..Ba....~.....p........5}%.
..~....o....iNv.Z&"T....O.7..v...}...a.....(Mjn....R.0X.......3.j....#.<<......Z.......Wf+..c.|../.k?@f.v\(._=..D..Z....K!.....Q.bF.g8.5.P.g.K_...3M../...;=.P.2....s..wu...k.....5.w..X....M.
'.X].`.mT...V.S .Y.....8?..7u.)..S|ox...d.....Y..~8..NI.".q.+.......qZ.. .....M2>....db..D.h.U....a ..k...&U.......`W....a../L7.....guS.B.<...W..@I.......M.pl...A......q\N..V.*..H\......g...d....r8...
...T}..;...>...$."B..p....U#....r.p..L.<.....$7xx.\.H.l.qp.4...o$.h....d|........". ..|....?....H.LC..j...vb..Q;..05JX=.....3...Z....".PkK....h.K.

C:\Users\user\AppData\Local\Temp\~DF5E4421C38C2CE13F.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34473
Entropy (8bit):	0.37064969110499696
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwj99lwh9l2/9l2/9l/0:kBqoxKAuvScS+jeU+X7I7/VsfKX
MD5:	769971887C0E80852D82B8E877ED591F
SHA1:	E3D8D3C9B1DD1D43B147EAE99F5825B6466DF1AC
SHA-256:	037B4F5461B2892FB601BB978FDFB7ACA309A2A72C8DC83492D6F967BF87BCE8
SHA-512:	3470A8026DF9DDCD24EB5CAF26CF3622A5FD4AEF96DC63586EFB0C520039E5468C5A1D8F39544D1ECA0BC8FF2ED64F9D6AA003527B844AE674FF4A11950E2F C7
Malicious:	false
Reputation:	low

Preview:

............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....
....
....
....

C:\Users\user\AppData\Local\Temp\~DF65406A083BBA58B1.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low

Preview:

............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....
....
....
....

C:\Users\user\AppData\Local\Temp\~DFFF3F5C6B9F825167.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13125
Entropy (8bit):	0.5451951693227013
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lodF9lo39lWuNqEqM6qBqKq:kBqoI4muNqEqM6qBqh
MD5:	A920DA73E61CDDA9390E7D2162FB6B0A
SHA1:	402BFC37DA51392E415D3546B810903AB8518951
SHA-256:	709FC76BC86194A6968B23FE65433D6925CD2980F2A95B51F8BF2F26E8172F04
SHA-512:	7935E28FBD5D12E07FC5038A8244AD051DAD9FF97DE472D0E321E48625760E0B2444E1756EBF45A7C08633A7ACAB227A58117B2D16D69BD8FFF17DB9398D9D8
Malicious:	false
Reputation:	low

Preview:

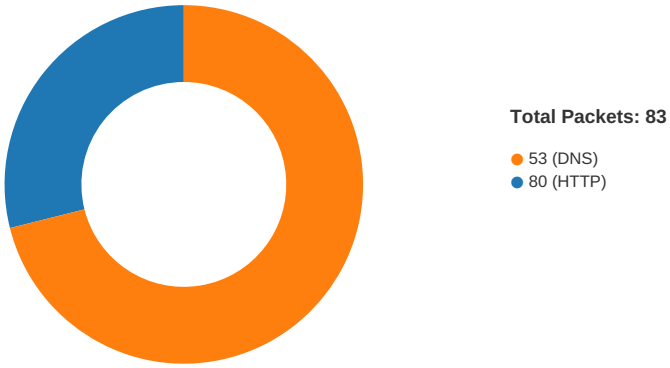
............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....
....
....
....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:33:45.599827051 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.599987984 CEST	49716	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.761102915 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.761137962 CEST	80	49716	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.761269093 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.761334896 CEST	49716	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.763324976 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.923095942 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937477112 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937500954 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937524080 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937547922 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937549114 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.937572002 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937572956 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.937593937 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937618017 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937627077 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.937644958 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937648058 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.937669992 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937678099 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.937686920 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:45.937697887 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.937719107 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:45.937740088 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:46.101633072 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101658106 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101670027 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101682901 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101700068 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101717949 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101731062 CEST	80	49715	136.165.238.241	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:33:46.101735115 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:46.101751089 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101768970 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101775885 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:46.101784945 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101800919 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101815939 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101829052 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:46.101830959 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101847887 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101846933 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:46.101864100 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101878881 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:46.101883888 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101901054 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101908922 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:46.101917028 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101927996 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:46.101933002 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101949930 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:33:46.101959944 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:46.101990938 CEST	49715	80	192.168.2.3	136.165.238.241
May 11, 2021 20:33:46.267220974 CEST	80	49715	136.165.238.241	192.168.2.3
May 11, 2021 20:34:45.921159983 CEST	80	49716	136.165.238.241	192.168.2.3
May 11, 2021 20:34:45.921361923 CEST	49716	80	192.168.2.3	136.165.238.241
May 11, 2021 20:35:34.928066015 CEST	49716	80	192.168.2.3	136.165.238.241
May 11, 2021 20:35:35.086971045 CEST	80	49716	136.165.238.241	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:33:37.224772930 CEST	50620	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:37.276420116 CEST	53	50620	8.8.8.8	192.168.2.3
May 11, 2021 20:33:38.312508106 CEST	64938	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:38.361545086 CEST	53	64938	8.8.8.8	192.168.2.3
May 11, 2021 20:33:39.088257074 CEST	60152	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:39.146723032 CEST	53	60152	8.8.8.8	192.168.2.3
May 11, 2021 20:33:39.295406103 CEST	57544	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:39.347206116 CEST	53	57544	8.8.8.8	192.168.2.3
May 11, 2021 20:33:40.042587996 CEST	55984	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:40.094602108 CEST	53	55984	8.8.8.8	192.168.2.3
May 11, 2021 20:33:40.922749043 CEST	64185	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:40.971935034 CEST	53	64185	8.8.8.8	192.168.2.3
May 11, 2021 20:33:41.872699976 CEST	65110	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:41.921628952 CEST	53	65110	8.8.8.8	192.168.2.3
May 11, 2021 20:33:43.636934996 CEST	58361	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:43.697138071 CEST	53	58361	8.8.8.8	192.168.2.3
May 11, 2021 20:33:44.117597103 CEST	63492	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:44.185013056 CEST	53	63492	8.8.8.8	192.168.2.3
May 11, 2021 20:33:44.860064983 CEST	60831	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:44.912158966 CEST	53	60831	8.8.8.8	192.168.2.3
May 11, 2021 20:33:45.525552988 CEST	60100	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:45.583208084 CEST	53	60100	8.8.8.8	192.168.2.3
May 11, 2021 20:33:45.914628983 CEST	53195	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:45.967145920 CEST	53	53195	8.8.8.8	192.168.2.3
May 11, 2021 20:33:49.106151104 CEST	50141	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:49.154844046 CEST	53	50141	8.8.8.8	192.168.2.3
May 11, 2021 20:33:50.512593985 CEST	53023	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:50.561570883 CEST	53	53023	8.8.8.8	192.168.2.3
May 11, 2021 20:33:51.792617083 CEST	49563	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:51.841552019 CEST	53	49563	8.8.8.8	192.168.2.3
May 11, 2021 20:33:53.001874924 CEST	51352	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:53.050693035 CEST	53	51352	8.8.8.8	192.168.2.3
May 11, 2021 20:33:53.838274002 CEST	59349	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:33:53.887079954 CEST	53	59349	8.8.8.8	192.168.2.3
May 11, 2021 20:33:54.747421026 CEST	57084	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:54.798157930 CEST	53	57084	8.8.8.8	192.168.2.3
May 11, 2021 20:33:56.145703077 CEST	58823	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:56.197326899 CEST	53	58823	8.8.8.8	192.168.2.3
May 11, 2021 20:33:57.330096006 CEST	57568	53	192.168.2.3	8.8.8.8
May 11, 2021 20:33:57.389296055 CEST	53	57568	8.8.8.8	192.168.2.3
May 11, 2021 20:34:01.721692085 CEST	50540	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:01.770529985 CEST	53	50540	8.8.8.8	192.168.2.3
May 11, 2021 20:34:02.684662104 CEST	54366	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:02.736207962 CEST	53	54366	8.8.8.8	192.168.2.3
May 11, 2021 20:34:11.943348885 CEST	53034	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:12.002760887 CEST	53	53034	8.8.8.8	192.168.2.3
May 11, 2021 20:34:14.132914066 CEST	57762	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:14.181756973 CEST	53	57762	8.8.8.8	192.168.2.3
May 11, 2021 20:34:15.024446964 CEST	55435	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:15.081799030 CEST	53	55435	8.8.8.8	192.168.2.3
May 11, 2021 20:34:15.151463032 CEST	57762	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:15.200406075 CEST	53	57762	8.8.8.8	192.168.2.3
May 11, 2021 20:34:16.026624918 CEST	55435	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:16.075609922 CEST	53	55435	8.8.8.8	192.168.2.3
May 11, 2021 20:34:16.198246956 CEST	57762	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:16.247097015 CEST	53	57762	8.8.8.8	192.168.2.3
May 11, 2021 20:34:16.665625095 CEST	50713	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:16.723833084 CEST	53	50713	8.8.8.8	192.168.2.3
May 11, 2021 20:34:17.073093891 CEST	55435	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:17.123318911 CEST	53	55435	8.8.8.8	192.168.2.3
May 11, 2021 20:34:18.290467978 CEST	57762	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:18.341634989 CEST	53	57762	8.8.8.8	192.168.2.3
May 11, 2021 20:34:19.119632006 CEST	55435	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:19.169595957 CEST	53	55435	8.8.8.8	192.168.2.3
May 11, 2021 20:34:22.307642937 CEST	57762	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:22.360076904 CEST	53	57762	8.8.8.8	192.168.2.3
May 11, 2021 20:34:23.119786024 CEST	55435	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:23.168530941 CEST	53	55435	8.8.8.8	192.168.2.3
May 11, 2021 20:34:31.948184967 CEST	56132	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:32.005697966 CEST	53	56132	8.8.8.8	192.168.2.3
May 11, 2021 20:34:33.713370085 CEST	58987	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:33.770751953 CEST	53	58987	8.8.8.8	192.168.2.3
May 11, 2021 20:34:35.081949949 CEST	56579	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:35.141115904 CEST	53	56579	8.8.8.8	192.168.2.3
May 11, 2021 20:34:42.987179041 CEST	60633	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:43.055875063 CEST	53	60633	8.8.8.8	192.168.2.3
May 11, 2021 20:34:56.054220915 CEST	61292	53	192.168.2.3	8.8.8.8
May 11, 2021 20:34:56.115648031 CEST	53	61292	8.8.8.8	192.168.2.3
May 11, 2021 20:35:17.587557077 CEST	63619	53	192.168.2.3	8.8.8.8
May 11, 2021 20:35:17.654825926 CEST	53	63619	8.8.8.8	192.168.2.3
May 11, 2021 20:35:40.870258093 CEST	64938	53	192.168.2.3	8.8.8.8
May 11, 2021 20:35:40.927452087 CEST	53	64938	8.8.8.8	192.168.2.3
May 11, 2021 20:36:28.720570087 CEST	61946	53	192.168.2.3	8.8.8.8
May 11, 2021 20:36:28.777877092 CEST	53	61946	8.8.8.8	192.168.2.3
May 11, 2021 20:36:29.810992956 CEST	64910	53	192.168.2.3	8.8.8.8
May 11, 2021 20:36:29.867907047 CEST	53	64910	8.8.8.8	192.168.2.3
May 11, 2021 20:36:30.487509966 CEST	52123	53	192.168.2.3	8.8.8.8
May 11, 2021 20:36:30.547513008 CEST	53	52123	8.8.8.8	192.168.2.3
May 11, 2021 20:36:31.159152031 CEST	56130	53	192.168.2.3	8.8.8.8
May 11, 2021 20:36:31.218460083 CEST	53	56130	8.8.8.8	192.168.2.3
May 11, 2021 20:36:31.794131994 CEST	56338	53	192.168.2.3	8.8.8.8
May 11, 2021 20:36:31.853203058 CEST	53	56338	8.8.8.8	192.168.2.3
May 11, 2021 20:36:32.456187963 CEST	59420	53	192.168.2.3	8.8.8.8
May 11, 2021 20:36:32.506105900 CEST	53	59420	8.8.8.8	192.168.2.3
May 11, 2021 20:36:33.430186987 CEST	58784	53	192.168.2.3	8.8.8.8
May 11, 2021 20:36:33.480163097 CEST	53	58784	8.8.8.8	192.168.2.3
May 11, 2021 20:36:35.655929089 CEST	63978	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:36:35.715584993 CEST	53	63978	8.8.8.8	192.168.2.3
May 11, 2021 20:36:36.761265039 CEST	62938	53	192.168.2.3	8.8.8.8
May 11, 2021 20:36:36.811424017 CEST	53	62938	8.8.8.8	192.168.2.3
May 11, 2021 20:36:37.670710087 CEST	55708	53	192.168.2.3	8.8.8.8
May 11, 2021 20:36:37.719393015 CEST	53	55708	8.8.8.8	192.168.2.3
May 11, 2021 20:38:32.863888025 CEST	56803	53	192.168.2.3	8.8.8.8
May 11, 2021 20:38:32.921166897 CEST	53	56803	8.8.8.8	192.168.2.3
May 11, 2021 20:38:33.610927105 CEST	57145	53	192.168.2.3	8.8.8.8
May 11, 2021 20:38:33.677917004 CEST	53	57145	8.8.8.8	192.168.2.3
May 11, 2021 20:38:40.202306986 CEST	55359	53	192.168.2.3	8.8.8.8
May 11, 2021 20:38:40.269273043 CEST	53	55359	8.8.8.8	192.168.2.3
May 11, 2021 20:38:44.442126989 CEST	58306	53	192.168.2.3	8.8.8.8
May 11, 2021 20:38:44.518428087 CEST	53	58306	8.8.8.8	192.168.2.3
May 11, 2021 20:38:44.876787901 CEST	64124	53	192.168.2.3	8.8.8.8
May 11, 2021 20:38:44.934597015 CEST	53	64124	8.8.8.8	192.168.2.3
May 11, 2021 20:41:12.290935993 CEST	49361	53	192.168.2.3	8.8.8.8
May 11, 2021 20:41:12.350517035 CEST	53	49361	8.8.8.8	192.168.2.3
May 11, 2021 20:41:12.906342983 CEST	63150	53	192.168.2.3	8.8.8.8
May 11, 2021 20:41:12.981420040 CEST	53	63150	8.8.8.8	192.168.2.3
May 11, 2021 20:41:45.937783003 CEST	53279	53	192.168.2.3	8.8.8.8
May 11, 2021 20:41:46.013698101 CEST	53	53279	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2021 20:33:45.525552988 CEST	192.168.2.3	8.8.8.8	0x1eac	Standard query (0)	louisville.edu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 20:33:45.583208084 CEST	8.8.8.8	192.168.2.3	0x1eac	No error (0)	louisville.edu		136.165.238.241	A (IP address)	IN (0x0001)
May 11, 2021 20:38:32.921166897 CEST	8.8.8.8	192.168.2.3	0x6def	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 20:41:12.350517035 CEST	8.8.8.8	192.168.2.3	0x9cc3	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- louisville.edu

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49715	136.165.238.241	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

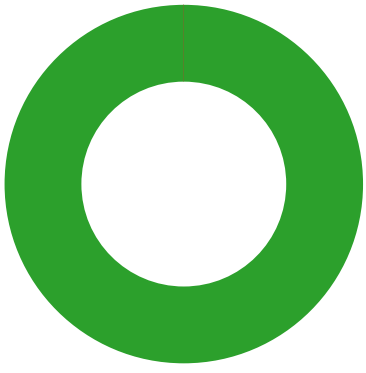
Timestamp	kBytes transferred	Direction	Data
May 11, 2021 20:33:45.763324976 CEST	716	OUT	GET /coronavirus/assets/Dec12020InterimPolicyforUniversityTravel.pdf HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: louisville.edu Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 20:33:45.937477112 CEST	938	IN	HTTP/1.1 200 OK Server: nginx/1.20.0 Date: Tue, 11 May 2021 18:33:45 GMT Content-Type: application/pdf Content-Length: 69481 Connection: keep-alive Last-Modified: Mon, 03 May 2021 21:11:17 GMT Content-Disposition: inline; filename="Dec 1 2020 - Interim Policy for University Travel.pdf" X-Varnish: 32621914 Age: 0 Via: 1.1 varnish (Varnish/6.0) Accept-Ranges: bytes Data Raw: 25 50 44 46 2d 31 2e 37 0d 0a 25 b5 b5 b5 b5 0d 0a 31 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 54 79 70 65 2f 43 61 74 61 6c 6f 67 2f 50 61 67 65 73 20 32 20 30 20 52 2f 4c 61 6e 67 28 65 6e 2d 55 53 29 20 2f 53 74 72 75 63 74 54 72 65 65 52 6f 6f 74 20 32 38 20 30 20 52 2f 4d 61 72 6b 49 6e 66 6f 3c 3c 2f 4d 61 72 6b 65 64 20 74 72 75 65 3e 3e 2f 4d 65 74 61 64 61 74 61 20 31 30 31 20 30 20 52 2f 56 69 65 77 65 72 50 72 65 66 65 72 65 6e 63 65 73 20 31 30 32 20 30 20 52 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 32 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 54 79 70 65 2f 50 61 67 65 73 2f 43 6f 75 6e 74 20 31 2f 4b 69 64 73 5b 20 33 20 30 20 52 5d 20 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 33 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 54 79 70 65 2f 50 61 67 65 2f 50 61 72 65 6e 74 20 32 20 30 20 52 2f 52 65 73 6f 75 72 63 65 73 3c 3c 2f 46 6f 6e 74 3c 3c 2f 46 31 20 35 20 30 20 52 2f 46 32 20 39 20 30 20 52 2f 46 33 20 31 31 20 30 20 52 2f 46 34 20 31 33 20 30 20 52 3e 3e 2f 45 78 74 47 53 74 61 74 65 3c 3c 2f 47 53 37 20 37 20 30 20 52 2f 47 53 38 20 38 20 30 20 52 3e 3e 2f 58 4f 62 6a 65 63 74 3c 3c 2f 4d 65 74 61 31 38 20 31 38 20 30 20 52 3e 3e 2f 50 72 6f 63 53 65 74 5b 2f 50 44 46 2f 54 65 78 74 2f 49 6d 61 67 65 42 2f 49 6d 61 67 65 43 2f 49 6d 61 67 65 49 5d 20 3e 3e 2f 41 6e 6e 6f 74 73 5b 20 31 39 20 30 20 52 20 32 30 20 30 20 52 20 32 31 20 30 20 52 20 32 32 20 30 20 52 20 32 33 20 30 20 52 20 32 34 20 30 20 52 20 32 35 20 30 20 52 20 32 36 20 30 20 52 5d 20 2f 4d 65 64 69 61 42 6f 78 5b 20 30 20 30 20 36 31 32 20 37 39 32 5d 20 2f 43 6f 6e 74 65 6e 74 73 20 34 20 30 20 52 2f 47 72 6f 75 70 3c 3c 2f 54 79 70 65 2f 47 72 6f 75 70 2f 53 2f 54 72 61 6e 73 70 61 72 65 6e 63 79 2f 43 53 2f 44 65 76 69 63 65 52 47 42 3e 3e 2f 54 61 62 73 2f 53 2f 53 74 72 75 63 74 50 61 72 65 6e 74 73 20 30 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 34 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 46 69 6c 74 65 72 2f 46 6c 61 74 65 44 65 63 6f 64 65 2f 4c 65 6e 67 74 68 20 34 31 33 34 3e 3e 0d 0a 73 74 72 65 61 6d 0d 0a 78 9c c5 1c db 72 db 36 f6 dd 33 fe 07 3e 4a 9d 98 26 00 de d4 ed 78 a6 b9 35 dd 4d b7 69 63 77 a7 93 f6 41 96 65 47 1b 5b 52 45 c9 a9 f7 eb 17 07 d7 03 10 90 2c 91 89 3d 63 9b a2 00 1c e0 dc 6f e4 e9 f7 ab f5 ec 7a 3c 59 27 df 7d 77 fa fd 7a 3d 9e 7c 9c 5e 25 1f 4e cf 17 cb 3f 4f cf 1f 96 d3 d3 77 e3 9b d9 7c bc 9e 2d e6 a7 ef 37 97 6b b8 f5 66 3a be 9a ae ce ce 92 e7 2f 5f 24 7f 1d 1f 65 69 06 3f 23 42 93 2c 29 f9 df 6a 44 93 d5 f4 f8 e8 3f df 24 f3 e3 a3 e7 e7 c7 47 a7 af 49 32 4a ce af 8f 8f 08 1f 93 25 24 29 8a 3a a5 2c a9 f2 2a cd ab e4 fc 8e 8f f9 e1 7d 95 dc 34 7c bd e4 46 7c aa d5 a7 1f 8e 8f 3e 0c 92 e1 9f c9 f9 3f 8f 8f 5e f1 d5 7e 39 3e 7a 2c 58 9a 10 e2 c0 25 55 91 66 75 52 b1 42 c3 15 e0 c2 50 92 57 3f bd 48 4e 23 38 7a be 58 af 17 77 71 34 bd 5e 2c d6 7b a3 89 f9 68 ca d3 8c 16 09 ab d2 82 ff 73 b7 9b c0 8a 34 39 9f 7c 18 5c cc 67 f7 d3 55 33 5b 3f 24 8b 21 Data Ascii: %PDF-1.7%1 0 obj<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 28 0 R/MarkInfo<</Marked true>>/Metadata 101 0 R/ViewerPreferences 102 0 R>>endobj2 0 obj<</Type/Pages/Count 1/Kids[3 0 R] >>endobj3 0 obj<</Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 9 0 R/F3 11 0 R/F4 13 0 R>>/ExtGState<</GS7 7 0 R/GS8 8 0 R>>/XObject<</Meta18 18 0 R>>/ProcSet[/PDF/Text/ImageB/ImageC/ImageI] >>/Annots[19 0 R 20 0 R 21 0 R 22 0 R 23 0 R 24 0 R 25 0 R 26 0 R] /MediaBox[0 0 612 792] /Contents 4 0 R/Group<</Type/Group/S/Transparency/CS/DeviceRGB>>/Tabs/S/StructParents 0>>endobj4 0 obj<</Filter/FlateDecode/Length 4134>>streamxr63>J& x5MicwAeG[RE,=coz<Y'}wz=|^%N?Ow|-7kf:/_$ei?#B,)jD?$GI2J%$):,*}4\|F\|>?^~9>z,X%UfuRBPW?HN#8zXwq4^,{hs49 \|\gU3[?$!

Code Manipulations

Statistics

Behavior



iexplore.exe
iexplore.exe
AcroRd32.exe
AcroRd32.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5916 Parent PID: 792

General

Start time:	20:33:42
Start date:	11/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff72ad00000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4552 Parent PID: 5916

General

Start time:	20:33:43
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5916 CREDAT:17410 /prefetch:2
Imagebase:	0x330000
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: 5140 Parent PID: 4552

General

Start time:	20:33:46
Start date:	11/05/2021
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 4552
Imagebase:	0xb50000
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	object name collision	1	B865C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R4wl84n_777wlx_47g.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close	success or wait	1	B9EA85	NtCreateFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\Device\NamedPipe\AIPC_SRV\AcroSBL_4552_5140	unknown	1040	success or wait	4	BB5549	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	B9CF19	RegCreateKeyW

Analysis Process: AcroRd32.exe PID: 5452 Parent PID: 5140

General

Start time:	20:33:47
Start date:	11/05/2021
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 4552
Imagebase:	0xb50000
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	Value	Ascii	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