ID: 458967
Sample Name: 0333 - CCFL Seniors Funded Facilities Risk Assessments 20210801.mhtml
Cookbook: default.jbs
Time: 23:16:59
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

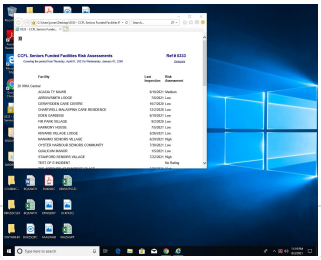
Windows Analysis Report 0333 - CCFL Seniors Funded …

Overview

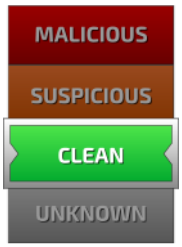
General Information

Sample Name:	0333 - CCFL Seniors Funded Facilities Risk Assessments 20210801.mhtml
Analysis ID:	458967
MD5:	129696ab429a99..
SHA1:	8bb06a0a27d7ac..
SHA256:	ff890973cd32878..
Infos:	

Most interesting Screenshot:



Detection

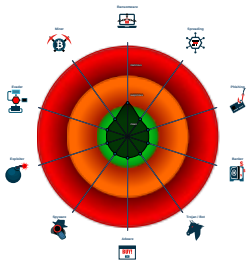


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 6944 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' C:\Users\user\Desktop\0333 - CCFL Seniors Funded Facilities Risk Assessments 20210801.mhtml MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 7012 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6944 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

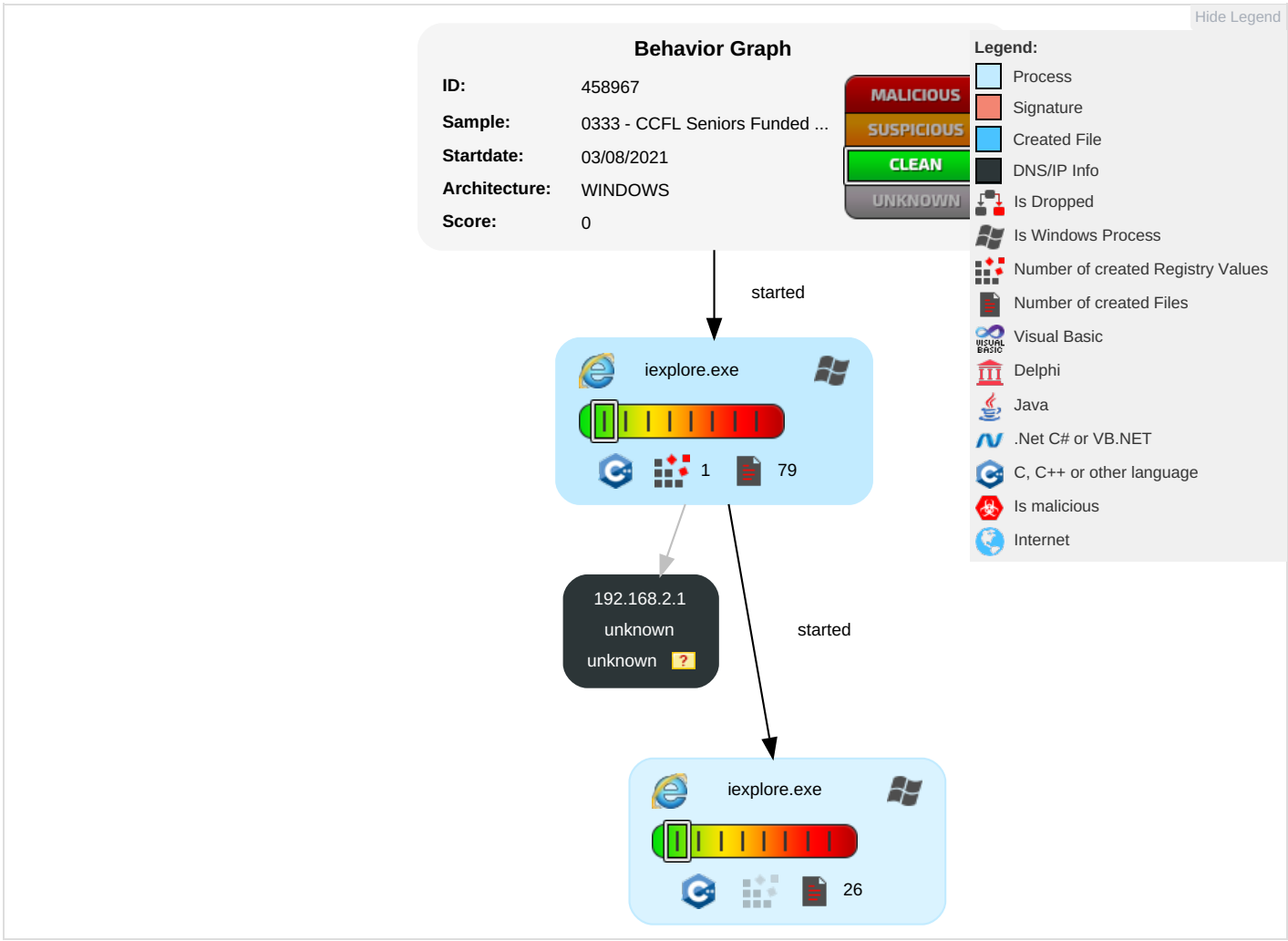
Click to jump to signature section

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

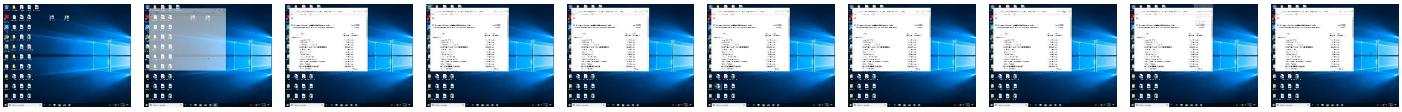
Behavior Graph

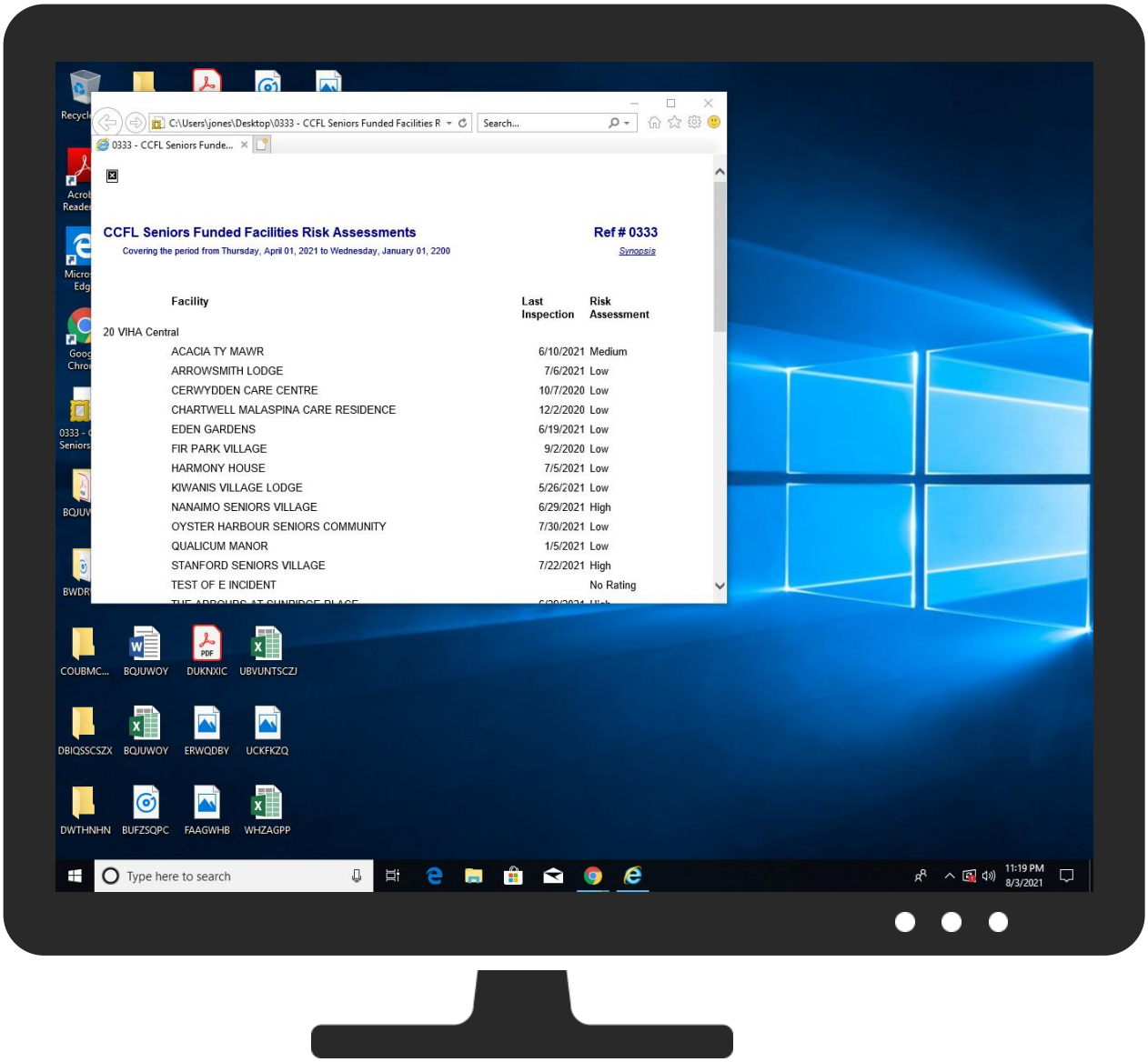


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://ravens.healthspace.ca/ReportServer?%2FVIHA%2FCCFL%2F0333%20-%20CCFL%20Seniors%20Funded%20Fac	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.healthspace.com/Clients/Common/ReportDefinitions.nsf/RefNum/0333	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458967
Start date:	03.08.2021
Start time:	23:16:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0333 - CCFL Seniors Funded Facilities Risk Assessments 20210801.mhtml
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winMHTML@3/14@0/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .mhtml
Warnings:	Show All

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.{3F393D3B-F4A0-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24152
Entropy (8bit):	1.753517549125157
Encrypted:	false
SSDEEP:	96:rDZQZkV2kP6WkP9FktkP9xfkP9rCCtkP9ryk7L/zWkP9+fyZH/:rDZQZq2pWQktgfTCt07L/zWUH/
MD5:	EA8AAF53A3E9254BCD799DAB1650C704
SHA1:	44A0C24BDE509E525B5C632308A45DAAA02B472D
SHA-256:	B9BA6329ED0B3C4E96D6EFE19C1C05997A79095FC60A3D0AC041A0D0624C995A
SHA-512:	0547C9710937368142EF1ABDC49F6F0AEDF99B7D617CF190ACBF89DB406F66C2316D31FEBACABA87A3032CE4B2159E3A9B089112B059D013EA160626ED5DD8 0
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\{3F393D3D-F4A0-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28954
Entropy (8bit):	2.2316766846831606
Encrypted:	false
SSDEEP:	192:r9ZWQmtW8ocoB7bO2HMOQZIpGvc/fmImB:rTjWvl8fO2sOEIpcf

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3F393D3D-F4A0-11EB-90EB-ECF4BBEA1588}.dat	
MD5:	E9622E82DA52E25233FD9AF76E802F9F
SHA1:	E31132B11EFBD875C2EE5CDE77133B95A6B4A215
SHA-256:	397C085AEE05E5E47F8F27DDE4A6086C8CF88F2D702685D885E9CDD739E892B3
SHA-512:	B839BD05126998B1D6C2FB33344B30A00C0258ABA794039ACD0A40E85A562C4B3E80AA525F2FA74D4833E765D61830551D49B36FCA17BEB639D6217548D19EF4
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):	5.072624047947721
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEL23vq23vuNnWimI002EtM3MHdNMNxOEL23vq23vuNnWimI00OYGVb2:2d6NxOI23C23ISZHKd6NxOI23C23ISZ2
MD5:	DF44614A9A6CD79F6C1D30A27E1E3F94
SHA1:	972CEB904C2DA335280B131DC61A6FB7A84BD013
SHA-256:	7B95E527ED2532A40DF880A24508AB0716DAB4D60BEF0AF439DA879AA085B247
SHA-512:	52159597746925BBF1260A506A231A117FEDB4EBE9EB5A018FE808C6AC85D32606617C32E7240C5E3EAF893AB09BB404B8F99521E31FA3500AD2E93682ED3C52
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x14c40b34,0x01d788ad</date><accdate>0x14c40b34,0x01d788ad</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>0x14c40b34,0x01d788ad</date><accdate>0x14c40b34,0x01d788ad</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):	5.150647426570353
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k55kv05kvuNnWimI002EtM3MHdNMNxe2k55kv05kvuNnWimI00OYGv:2d6Nxr2i8iISZHKd6Nxr2i8iISZ7Yzan
MD5:	F27FB87A42B5F21C85B668886CCBFD7F
SHA1:	2D446CD11C34971E7E47625ECEFD17BA6F8C05E7
SHA-256:	35ED7766D95E924EA7F6BCCAEB59086CDA8D7B2B19B1AD36FFA0ABE4269357C8
SHA-512:	72F6D2DF529A59AE740F8120F54D70688C2337E1573ADF3009BD9565562E7ABD4A9A901F66CA4823266DAC4AD66F483A2F01F29BBBBD1EF575CB667C3997889
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x14945f42,0x01d788ad</date><accdate>0x14945f42,0x01d788ad</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>0x14945f42,0x01d788ad</date><accdate>0x14945f42,0x01d788ad</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):	5.090901506310693
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLL23vq23vuNnWimI002EtM3MHdNMNxvLL23vq23vuNnWimI00OYGmZt:2d6Nxv323C23ISZHKd6Nxv323C23ISZy
MD5:	03FC59F90ACEA334D57D9E6CAD9B3717
SHA1:	257D7CAEFDD63115195BF7D02F3C34B55503F479
SHA-256:	F4A16A58597331CA1BF1AEFCBD70A88E173D797D50E206A49A3A4AE54156E499
SHA-512:	B49AD042B64183E6B5E2F6845E46B68AEB4355A4815CE9D92B9AAD5B2D7DD2189498344BEAA56FE980A67138DD289E5A9D19719170380CE0E85DA0DEA6B8099 8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x14c40b34,0x01d788ad</date><accdate>0x14c40b34,0x01d788ad</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>0x14c40b34,0x01d788ad</date><accdate>0x14c40b34,0x01d788ad</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):	5.053433908395234
Encrypted:	false
SSDEEP:	12:TMHdNMNxievxvuNnWimI002EtM3MHdNMNxievxvuNnWimI00OYGd5EtMb:2d6NxtZISZHKd6NxtZISZ7YEjb
MD5:	AAEC48334C8FC91452D09C0927CA4916
SHA1:	BC4B964FE5BC3D44187FA70AC0A8BCE7D0430093
SHA-256:	235B4B279625AF62C6A176786EB2B3A8F8C0B5F1A6329A5BE258FDAE5873428A
SHA-512:	1E9F26F845C15C356E6003C625C82D9CBB82E351D77A43CC096DA61577397FB3FDE6C0CC13944F3C60CB1603429F96ED92B986BC97CA4280E32FA8A649076F9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x14ac33ac,0x01d788ad</date><accdate>0x14ac33ac,0x01d788ad</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>0x14ac33ac,0x01d788ad</date><accdate>0x14ac33ac,0x01d788ad</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):	5.106861393380306
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwhvivuNnWimI002EtM3MHdNMNxhGwhvivuNnWimI00OYG8K075EtMb:2d6NxQsaISZHKd6NxQsaISZ7YrKajb
MD5:	50E65D990429DE83B78EA6C5A3538606
SHA1:	941E64B86A09A1A4D71D642F214CEE4489DB5116
SHA-256:	4831377DEBB2248704751B25363369F224476A1F4CE15FB410C039C5F3E176AA
SHA-512:	A68868E716B8A7BFC9CC857215851A50ADDB1F930768E96C09F1721FD9D7791D305C4AEE78CD0CE25524273F67C0D6EC711540B510E5D8940DB0AA80EA35E34
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x14cb31e9,0x01d788ad</date><accdate>0x14cb31e9,0x01d788ad</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>0x14cb31e9,0x01d788ad</date><accdate>0x14cb31e9,0x01d788ad</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):	5.0515852499020015
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nevxvuNnWimI002EtM3MHdNMNx0nevq23vuNnWimI00OYGxEtMb:2d6Nx0eZISZHKd6Nx0eC23ISZ7Ygb
MD5:	C993D204B5758736A33250EA39536578
SHA1:	352A75A7F90B80411507127ACA9A37D767F18BF3
SHA-256:	A1F987AAEC89763DCCBA939619EF49C93A17D621E1B63A13024474E574A83EB2
SHA-512:	F346B5A8236C75A5ED31DAE5441427C990EF9108C255A43D4621C698A21EFEC7A5C30FA64B8C7CE1D9E6DC18C1BE14A31C1B74F0DE929D228B2C19D07A9F4A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x14ac33ac,0x01d788ad</date><accdate>0x14ac33ac,0x01d788ad</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>0x14ac33ac,0x01d788ad</date><accdate>0x14c40b34,0x01d788ad</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):	5.078374875494457
Encrypted:	false
SSDEEP:	12:TMHdNMNxxevxvuNnWimI002EtM3MHdNMNxxevxvuNnWimI00OYG6Kq5EtMb:2d6NxUZISZHKd6NxUZISZ7Yhb
MD5:	A484BFC5AD35517E6C3C6938A4BC1207
SHA1:	57D2EA297A7D263B8ED96CB22A4EA3F02DD1B383
SHA-256:	58C4CAF3752A96F207047278C8BA654950A8DD7D1D143C4488460DD0B8F7F06E
SHA-512:	3FA7FEBFD136447BAFC44B126BDBECC36AEAAC57CBAD9A6DAEE9BE3B0B90B7CF1C77BD0C4F4445810FA81BDFA6EDEAF791504A739112FAA19D11587CC975 8032
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x14ac33ac,0x01d788ad</date> accdate>0x14ac33ac,0x01d788ad</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>0x14ac33ac,0x01d788ad</date><accdate>0 x14ac33ac,0x01d788ad</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):	5.068156126395315
Encrypted:	false
SSDEEP:	12:TMHdNMNxcgvXvuNnWimI002EtM3MHdNMNxcgvXvuNnWimI00OYGVEtMb:2d6NxJ/ISZHKd6NxJ/ISZ7Ykb
MD5:	71DAC2DB16EBAFD7556001FAF262A706
SHA1:	F825D2CFEA40A67CE05963A4FB3D2A345CAD0ECF
SHA-256:	71B495D2B10A92AE0A5EF59A8D6AC7CBD987B4DF1D4EA4AECF023B55B73F25DA
SHA-512:	4282EC7A6ACA1DFBF458C43CE215E028D2C21CE49DDA25370CC1FFC4161DD01C8F911A784012B0F7042870532F3737D6575EB5C2746FA822941E6FCB1FB3CA 9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x14a50c70,0x01d788ad</date> <accdate>0x14a50c70,0x01d788ad</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>0x14a50c70,0x01d788ad</date><accdate >0x14a50c70,0x01d788ad</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):	5.049848553005894
Encrypted:	false
SSDEEP:	12:TMHdNMNxfngvXvuNnWimI002EtM3MHdNMNxfngvXvuNnWimI00OYGe5EtMb:2d6NxI/ISZHKd6NxI/ISZ7YLjb
MD5:	122D3F92D33534BFF054B6DAC0164BBD
SHA1:	7E1AA5FF25F409CF206AE3E852DBB119DA46EC48
SHA-256:	ED692214CFEB258038208B4267B17AF6491C2391E5BEC74CC6F86060C4D04ECC
SHA-512:	C445751B171300CF2C6CF8BE92EC19D6F7DC8CC898648306D1A9BA2760400F6618364F7B0E555A73DBC29BB00EF34A300A5E73A0E45C47355DFBA8EA685800B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x14a50c70,0x01d788ad</date><a ccdate>0x14a50c70,0x01d788ad</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>0x14a50c70,0x01d788ad</date><a ccdate>0x14a50c70,0x01d788ad</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\wbk9C9B.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	34439

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\wbk9C9B.tmp	
Entropy (8bit):	5.69367155071897
Encrypted:	false
SSDEEP:	384:giBIupO8JyaJlwlSEs+2+1H7W/A2GJcyicpanQ+nl:gQYH7W/A2GJkcpanQ+nl
MD5:	7FC1AFC6BB13B58A1AAD7E446788248E
SHA1:	C5B14BE408CA0C26E547C8E455B542D98407EBD8
SHA-256:	D6E17DED91970B0284E54A8D922D8B633C5648834658D42645F7BEB6274295A0
SHA-512:	9E15C6966683840A05C6D0A508778EB47264FB32C287AF29C2E4996EF3B562A10F150671DC7A8D152D5107CE1B29626BC543599CA5AB135B63E08F39FFF2B070
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><html>..<head><title>0333 - CCFL Seniors Funded Facilities Risk Assessments</title>..<META http-equiv="Content-Type" content="text/html; charset=utf-8"/><META http-equiv="Content-Style-Type" content="text/css"/><META http-equiv="Content-Script-Type" content="text/javascript"/><META HTTP-EQUIV="Location" CONTENT="https://ravens.healthspace.ca/ReportServer?%2FVIHA%2FCCFL%2F0333%20-%20CC FL%20Seniors%20Funded%20Facilities%20Risk%20Assessments"/><META HTTP-EQUIV="Uri" CONTENT="https://ravens.healthspace.ca/ReportServer?%2FVIHA %2FCCFL%2F0333%20-%20CCFL%20Seniors%20Funded%20Facilities%20Risk%20Assessments"/><META HTTP-EQUIV="Last-Modified" CONTENT="08/03/2021 17:21:17"><META NAME="StartDate" CONTENT="4/1/2021 12:00:00 AM"><META NAME="EndDate" CONTENT="1/1/2200 12:00:00 AM"><META NAME="SourceDa tabase" CONTENT=""><META NAME="Generator" CONTENT="Microsoft Report 8.0 "/><META NAME="Originator" CONTENT="Microsoft Report 8.0 "/><style t

C:\Users\user\AppData\Local\Temp\~DF34CD3393F0C35364.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38539
Entropy (8bit):	0.9561710410084375
Encrypted:	false
SSDEEP:	96:kBqoxK7pwFjFLY+OOOdObO7IV/o75/oV1iO5fm:kBqoxK7pKhLY+OOOdObO7I8c/fm
MD5:	F81C189E1CF5D59F960AECA02072A1A0
SHA1:	131D5F0BD554BAA7804C861D991691FFB2F5DDED
SHA-256:	55C711D39BC3E02AA21E2BF26045F245423041432D780C8976FD5DDA135C1242
SHA-512:	9CAFEF9989881F72EE8B3B1543212B4661978C215F5C87742BBA750DD96FE4EB270B7B8796BE4602BE1F59F324265026019D670C193C06952CB32CED8FE742A2
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF7AB7A8B365382B36.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12965
Entropy (8bit):	0.4129652521876017
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lok39lok39lWkP9F+ry9+V:kBqoIk4kmkP9F+ry9+V
MD5:	FEC9DC8CA6C2DA6C4E3CB15957EC5B69
SHA1:	C7B87850A3BC9613109162B014D1A47BEEFDBCC9
SHA-256:	6E1367087FCFDBBFE10C2ADC1F377F74711A96211EA3B930B4B828F28090D92B
SHA-512:	E7C48D01B367D1C306B0E388547AE671D37715A63E0F959C3A744223DCB098DF3C3AC3EB834BC5B1A48FE9EA8F4025B459DE3843CDC05BDECF171842AFD5A4 DD
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	MIME entity, ASCII text, with CRLF line terminators
Entropy (8bit):	5.850048759606687
TrID:	
File name:	0333 - CCFL Seniors Funded Facilities Risk Assessments 20210801.mhtml

General

File size:	47641
MD5:	129696ab429a996fba603f5946f20389
SHA1:	8bb06a0a27d7ac48a92576b27abb02eaf1acd21c
SHA256:	ff890973cd32878dff5325414d4a6d36e483c828fbda3eaf6f0fa469fbb2d987
SHA512:	cafbb699cd7c1e5f3e8600ae42d731c1b2ee6dfd4fa85b975cd6ae670482331e50b3120c0dc9339497afa1d3d6718bf8b4e25c4734869b85a7d7fe221ab22985
SSDEEP:	768:zI5uJgbvHGuj4BdhvFzZJhiFi2DRimrdaMIzQOXOYProBc6m+PPQ72xF/Bc5Ix6H:z9mOuj4BfvFNJhiFi2DRiSoMIzQOXOYF
File Content Preview:	MIME-Version: 1.0..Content-Type: multipart/related;...boundary="----=_NextPart_01C35DB7.4B204430"..X-MSSQLRS-ProducerVersion: V12.0.6164.21....This is a multi-part message in MIME format.....------=_NextPart_01C35DB7.4B204430..Content-Disposition: inline;

File Icon

Icon Hash:	e4e0c8c3ccccccf5

Network Behavior

Network Port Distribution

UDP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 23:18:05.270133972 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6944 Parent PID: 6036

General

Start time:	23:17:46
Start date:	03/08/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' C:\Users\user\Desktop\0333 - CCFL Seniors Funded Facilities Risk Assessments 20210801.mhtml
Imagebase:	0x7ff63a040000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 7012 Parent PID: 6944

General

Start time:	23:17:47
Start date:	03/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6944 CREDAT:17410 /prefetch:2
Imagebase:	0xf20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Disassembly