ID: 384811
Sample Name: NCA Approval Letter.html
Cookbook: default.jbs
Time: 21:26:22
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

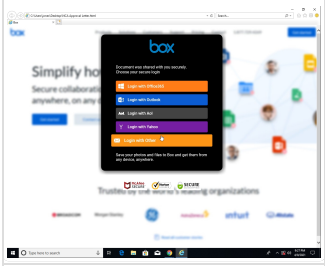
Analysis Report NCA Approval Letter.html

Overview

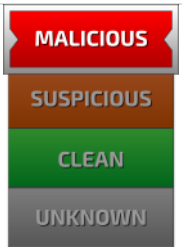
General Information

Sample Name:	NCA Approval Letter.html
Analysis ID:	384811
MD5:	2afd53761ef2429..
SHA1:	608645dc128a09..
SHA256:	6b432f5c38d2deb.
Infos:	

Most interesting Screenshot:



Detection



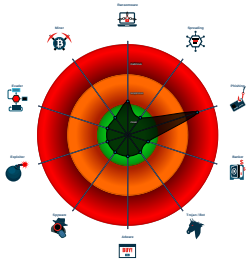
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on sh…
- Yara detected HtmlPhish7
- HTML body contains low number of …
- HTML title does not match URL
- None HTTPS page querying sensitiv…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6552 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6600 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6552 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

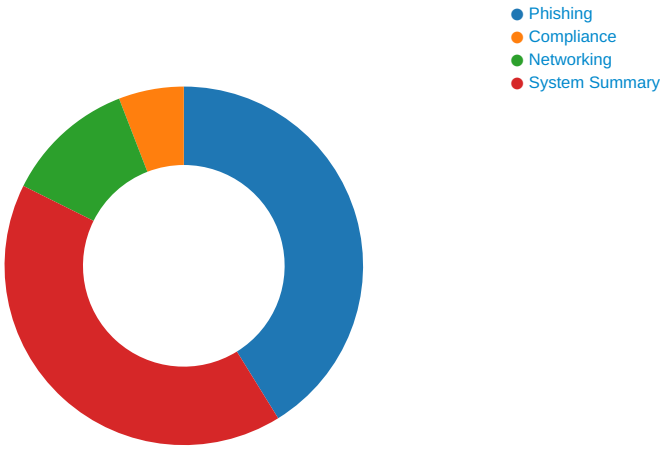
Initial Sample

Source	Rule	Description	Author	Strings
NCA Approval Letter.html	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

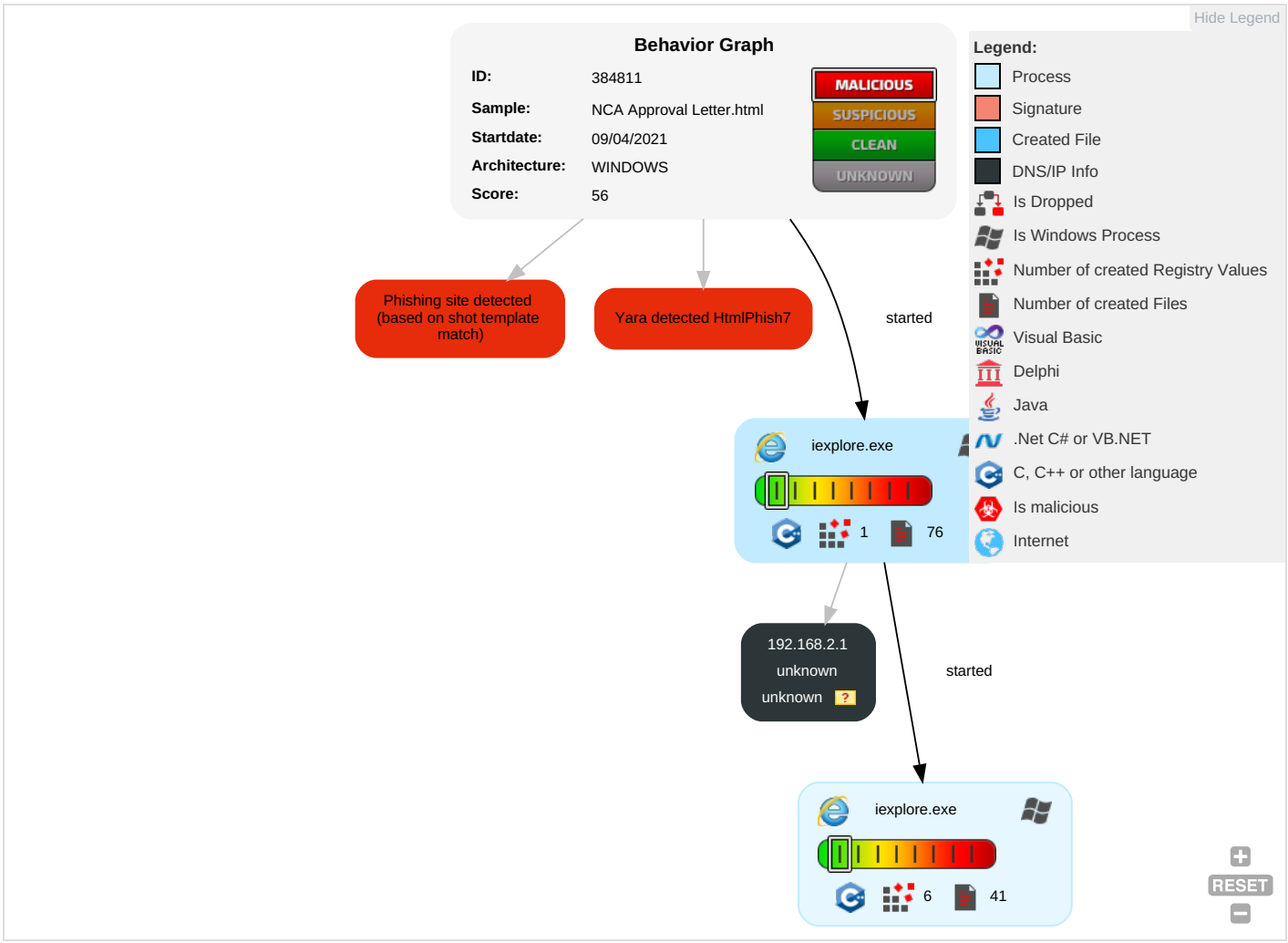
Phishing site detected (based on shot template match)

Yara detected HtmlPhish7

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

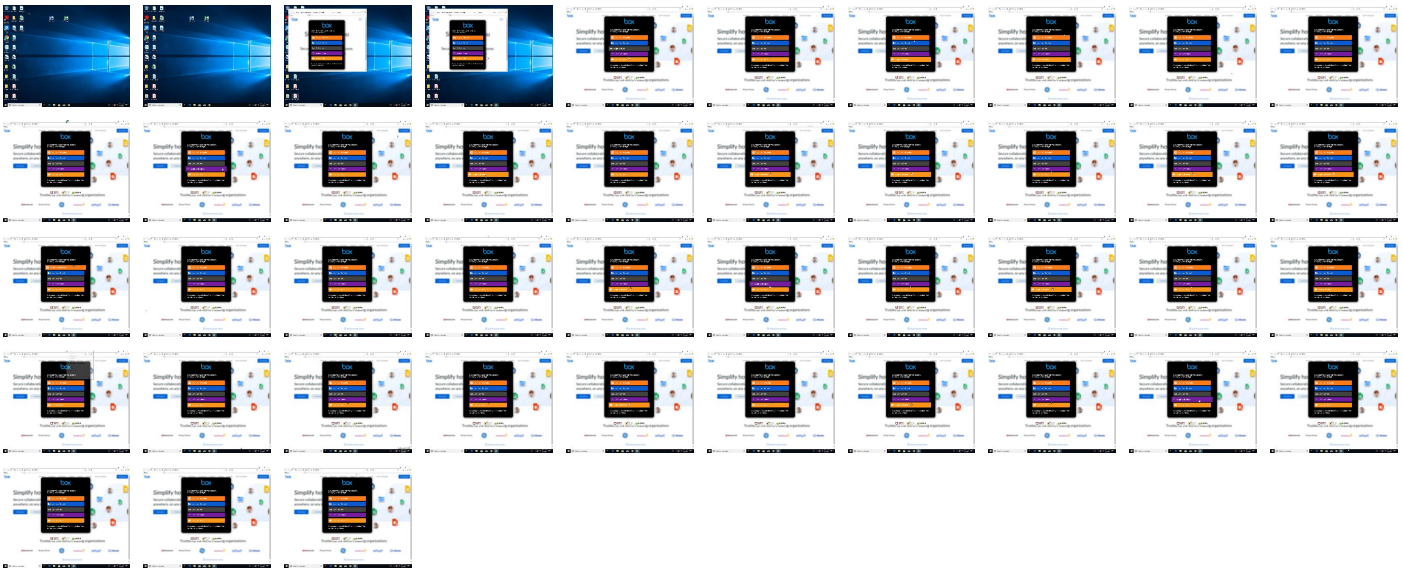
Behavior Graph

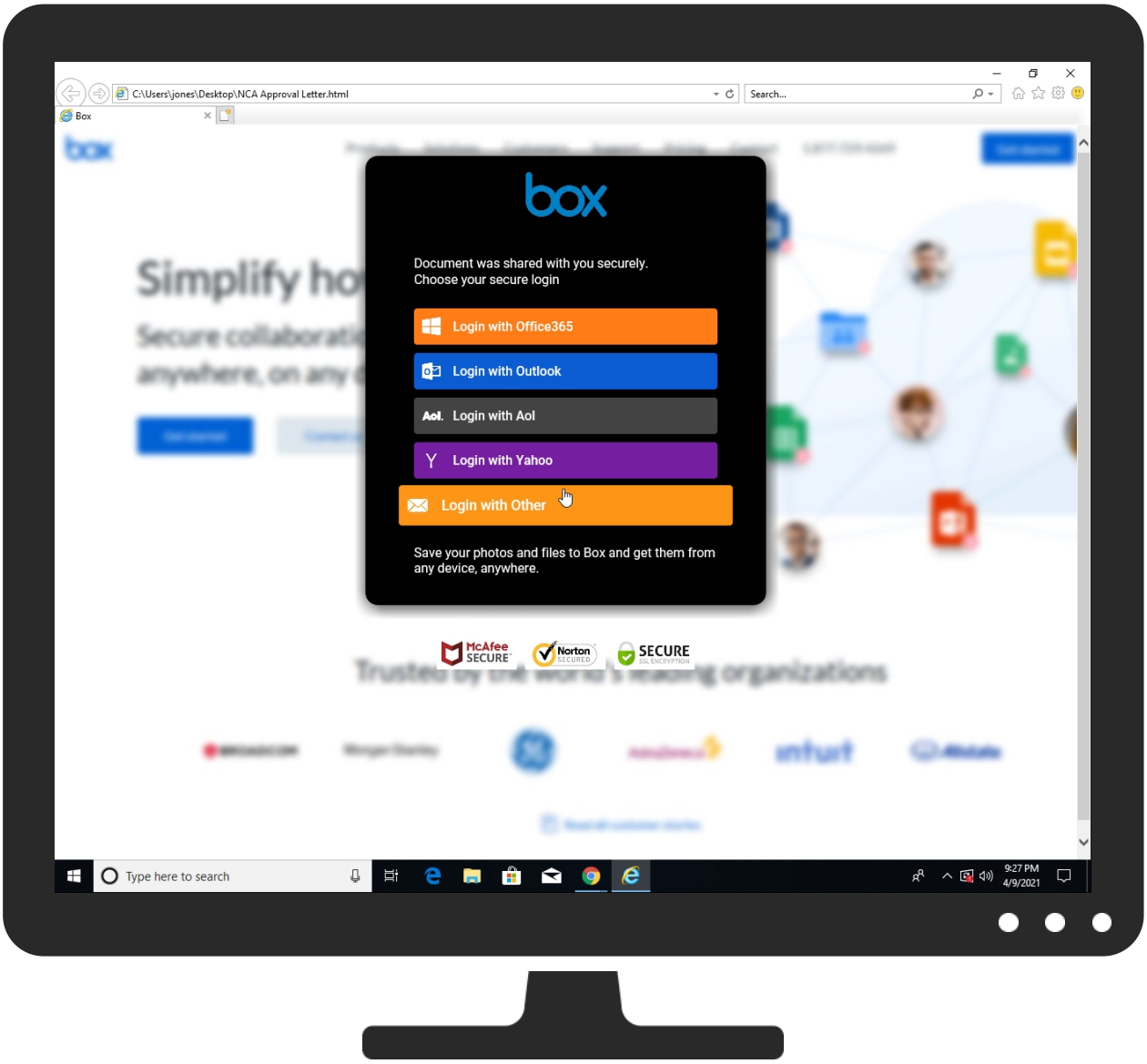


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
NCA Approval Letter.html	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://islandweddingsofhawaii.com/bin/ds/	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

No contacted domains info

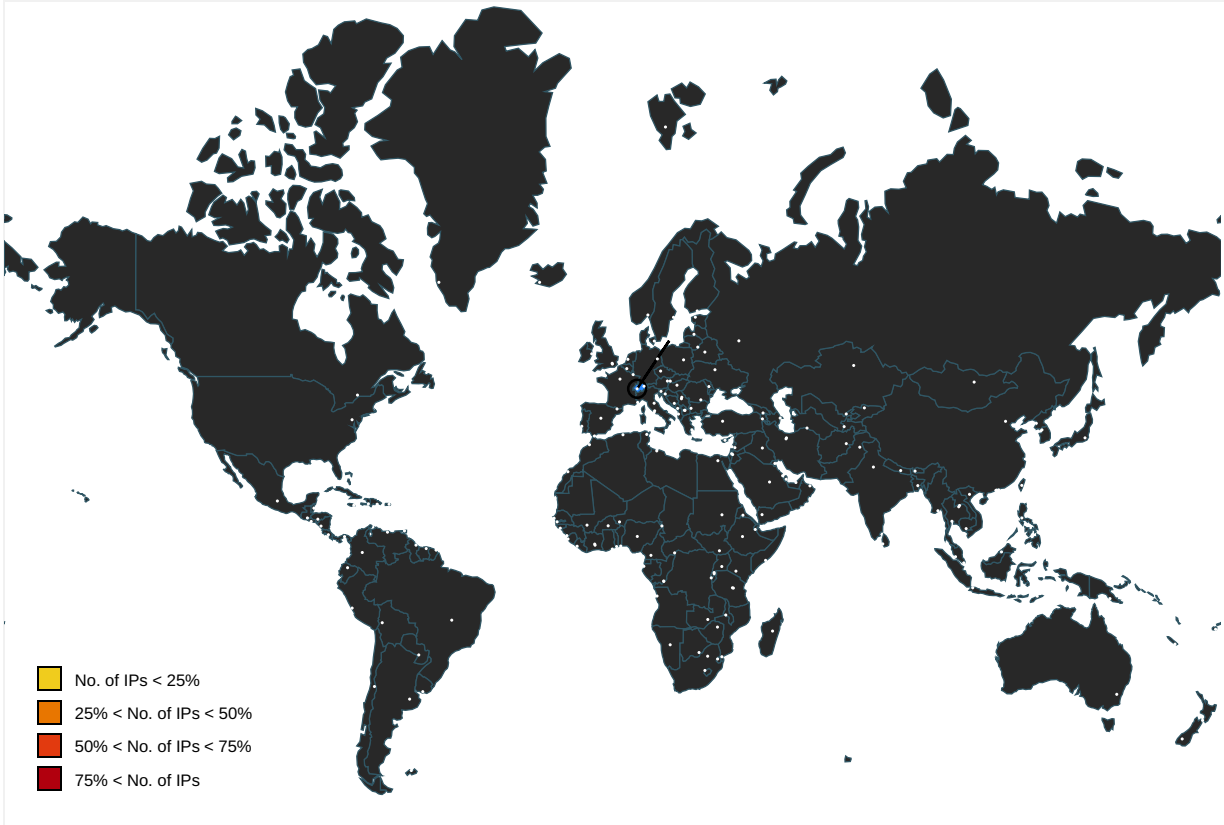
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/NCA%20Approval%20Letter.html	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://islandweddingsofhawaii.com/bin/ds/	NCA Approval Letter.html	false	• Avira URL Cloud: 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.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384811
Start date:	09.04.2021
Start time:	21:26:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NCA Approval Letter.html
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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.winHTML@3/23@0/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 13.88.21.125, 104.42.151.234, 168.61.161.212, 2.18.101.230, 216.58.215.234, 172.217.168.10, 216.58.215.227, 13.64.90.137, 20.50.102.62, 23.10.249.43, 23.10.249.26, 152.199.19.161, 20.82.210.154, 20.54.26.129, 23.54.113.53 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.bing.com, fonts.googleapis.com, skypedataprdcolwus17.cloudapp.net, dual-a-0001.a-msedge.net, ajax.googleapis.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/384811/sample/NCA Approval Letter.html

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.{90D684E2-9969-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8683370524977623
Encrypted:	false
SSDEEP:	192:rcZHZb27W6tlifGmUzMFMBJyD1MBqytAmzj3:rc5yyS1L2mGhr
MD5:	4111EB66CF0E8D65EB6CA4CD91460198
SHA1:	37E53E46483F9ED02CE8A766519F5F8DD0075A4D
SHA-256:	6163F996DC2CA0ED3422F87ED00268A08B8705A06550E945978409CEF2898F49
SHA-512:	E686FC5AB3430F15FD92BDA3DA8484DCF68F9539039EAEAFC8ADCBE470989DD5BE8B51BE239118B4638034D8CC2DEA7B161E247A0574EDB232648C363AE3A D5
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\{90D684E4-9969-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28402
Entropy (8bit):	1.9390180816254627

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{90D684E4-9969-11EB-90EB-ECF4BBEA1588}.dat	
Encrypted:	false
SSDEEP:	96:rqZZQ16TBSzjB2NWOM6XG28G0/7cwpkWp/7cw7RiGqGr:rqZZQ16TkzjB2NWOM6X98sWkBzGr
MD5:	F76C830751B0019C0E22D4BFF69C183A
SHA1:	E7902A5E52224A29F44AF1A4A3B50FFE833722AA
SHA-256:	4F4CF69975AB8C5E79C1F894AC275CE02D84142BD8840AA51D547274828C0D5F
SHA-512:	99953B5173E4D939058A7A3FC6038D4275DCA84035CB2775A41DF2BEE161B59F6F7A6CA0CDF680D9BD6FD27ECF96577173746DD5EB667964ECCAC720D3FAEB5
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\{90D684E5-9969-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565011187223363
Encrypted:	false
SSDEEP:	48:Iw0GcprPGwpaiG4pQOGrapbS/GQpKiG7HpRvTGIpG:roZ5QS6ABSpANTNA
MD5:	4957A999DBC0C10DA9E5E59DFF150F4F
SHA1:	A6FABC3814FBABA723E5EC0BFA723FCFEEA834DF
SHA-256:	8F46CA36714F87F11C171B68C6F824F2B71CFAD175FB84011C35AC9AC22D1791
SHA-512:	6D606FD1210A0F2A65032C769B838AC5F9A42FA6A87CD239B6D8CBFA0AB2FF722E09D89B106E245099AC44FF4E3A624B4765AC5DE4B91214CA81D47E6069AC7
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):	5.1071347877544495
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEYvGvBnWimI002EtM3MHdNMNxOEYvGvBnWimI00OYGVbkEtMb:2d6NxOBOpSZHKd6NxOBOpSZ7YLb
MD5:	94D83CB84E5E5345C37EB264458C1C56
SHA1:	CEB0C347145E3633867B9F08764A2E911E53A547
SHA-256:	FC93E4DC179BCEB8E64FC586CF9B5351DB7AFC64CA1C1E626EA62BE951130F10
SHA-512:	1FFEA8738CAE4A7CF46DBB63E5C6F489C707C3CD816BC78CCEAFF273343F471BCF655AC52008CDAC2B6D3636CFE3F6D1C6C834E3BBE9C85D793B90F1514432
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x663a6282,0x01d72d76</date><accdate>0x663a6282,0x01d72d76</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>0x663a6282,0x01d72d76</date><accdate>0x663a6282,0x01d72d76</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):	5.134461045481408
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kYAZqAZtnWimI002EtM3MHdNMNxe2kYAZqAZtnWimI00OYGkak6Ety:2d6NxrhAoArSZHKd6NxrhAoArSZ7Yzan
MD5:	2EE5EB4FDC959E6BD35969188D0AAB20
SHA1:	01B09CDE07D48756B6AF8287432D1A7875498238
SHA-256:	3A47FA04C6D35477078FDB0356CAC7445C0929FA9D9D71017CDB048ADDEF380F

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SHA-512:	40F2DA810A6727870C5075B6AEF1261D0BBDDB4378E4C4BB69D31D29B91F1DE30F1BC7CE728292B928BD1E7F9A4F2D3AE86347C446EFC83806EBBA0C651AA4CD
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x66333b62,0x01d72d76</date><accdate>0x66333b62,0x01d72d76</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>0x66333b62,0x01d72d76</date><accdate>0x66333b62,0x01d72d76</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):	5.1303196242938744
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLYvGvBnWimI002EtM3MHdNMNxvLYvG5unWimI00OYGmZEtMb:2d6NxvMOpSZHKd6NxvMO5uSZ7Yjb
MD5:	D12BB716ADD36AC5B868831A7CB280CE
SHA1:	A313AD83A3D464B589D7A3D73BE8F8E279D64EBE
SHA-256:	3F6403599A2D78165CEB43FC6A799769C2E2AB7738199E3642B5BCFECEBB4163
SHA-512:	E25C4880571C472FCEDDAB1A3BF2BA7C8BBA5F1E73C56B332EB53BEE62158C8E895E628364D32A0B4D071A7830C998D7768EEFFB3C4B142DDD03790030A2B6A5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x663a6282,0x01d72d76</date><accdate>0x663a6282,0x01d72d76</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>0x663a6282,0x01d72d76</date><accdate>0x663cc4bd,0x01d72d76</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):	5.117586557518992
Encrypted:	false
SSDEEP:	12:TMHdNMNxiYaxqaxtnWimI002EtM3MHdNMNxiYaxqaxtnWimI00OYGd5EtMb:2d6NxfKqKtSZHKd6NxfKqKtSZ7YEjb
MD5:	C939C90576104BD4F144CD796EDFE26C
SHA1:	CBEF433DB22A0A8ABC785F231A9DFC41E14D7ABB
SHA-256:	F499ED953039A5E6737F25B0DB23CAA84AE2D6EF7A8EB9864DD4AD98D02F17AE
SHA-512:	B325CB3FDA4F4BEF63261B49C6E07DB3CDD5BC43D6DC406A7EF38DBDF407E41805037A2481F9EF85957C18BE6D1285C812E1EBFB46D60508D6B4718D3BFC1530
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x66380035,0x01d72d76</date><accdate>0x66380035,0x01d72d76</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>0x66380035,0x01d72d76</date><accdate>0x66380035,0x01d72d76</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):	5.131313246552989
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwY555unWimI002EtM3MHdNMNxhGwY555unWimI00OYG8K075EtMb:2d6NxQN555uSZHKd6NxQN555uSZ7YrKG
MD5:	8F35828019AC14C4B56DB21E48D4F8EC
SHA1:	C7597C47AA5BA802C7922254CC5B45E21F60336A
SHA-256:	B76A509976AFF4E30B05C60B2BA56BF236EF6AF452ED78DB389206FB4063B3E1
SHA-512:	E2AC91DF59867183EEC46067E3807A3F11A723E9665B01B7E204C718DBA8AA492409F5A00D8CB27C3BFB74B00F91FCB9DBDFE317A8D5A38743FE659C3873883
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x663cc4bd,0x01d72d76</date><accdate>0x663cc4bd,0x01d72d76</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>0x663cc4bd,0x01d72d76</date><accdate>0x663cc4bd,0x01d72d76</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):	5.1084073387605455
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nYvGvBnWimI002EtM3MHdNMNx0nYvGvBnWimI00OYGxEtMb:2d6Nx0YOpSZHKd6Nx0YOpSZ7Ygb
MD5:	6B8E38320F8D466A719FAD67262070E1
SHA1:	8B1B81C41B8DD8020D0EB18D533F259EBDB4585E
SHA-256:	4C8B9FC797F8A6CCC7088D9596E859FEA43A3FE4005BE3850CD960278EDB507A
SHA-512:	338F85C4947E0CEB47D686E83887973A1E5DA853D6158A34C281C03C06792612BA5B4298047C8174AA4FAB6749769B0D27FF0A9253B984010B412DE3E9E3160B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x663a6282,0x01d72d76</date><accdate>0x663a6282,0x01d72d76</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>0x663a6282,0x01d72d76</date><accdate>0x663a6282,0x01d72d76</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):	5.141647381566213
Encrypted:	false
SSDEEP:	12:TMHdNMNxxYaxqaxtnWimI002EtM3MHdNMNxxYaxqaxtnWimI00OYG6Kq5EtMb:2d6NxqKqKtSZHKd6NxqKqKtSZ7Yhb
MD5:	ACA5C72D0DCF62FCCB218EE20EC09DCD
SHA1:	9400C61E835A38D9EC16F0DDEE7937B14F5C7CA0
SHA-256:	952FB47AEE8863FBF1555F3A6B4FAB58A73805F0DC4D23EAF91138820832CC5C
SHA-512:	9A1E0D497155BE993E4B4B5E30164E414D63E507AE87C18702544CFC7EBC244A775607E127FCECE3A207A22D41FFAACBEEE78D1A30A8995677CA4623F3D4145 8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x66380035,0x01d72d76</date><accdate>0x66380035,0x01d72d76</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>0x66380035,0x01d72d76</date><accdate>0x66380035,0x01d72d76</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):	5.1256225870707
Encrypted:	false
SSDEEP:	12:TMHdNMNxcY1s1XnWimI002EtM3MHdNMNxcY1s1XnWimI00OYGVEtMb:2d6NxJKNSZHKd6NxJKNSZ7Ykb
MD5:	04F42D5CCBF7B58A7B277FBC97978372
SHA1:	890186FC586AC5556A5E15965F8801314AB0D657
SHA-256:	6997D2A430D33EEEF3BB5B5D0AA87CBFD17A695E7585D69AC3611FF671A3396A
SHA-512:	0DE84826DA52C32579758C42F6FB9818BF793EC2D455DC7086DF065637EB56467328723689F459DA02DD0D67B577B221EAD9919B309599DBF7EDA217D9481B1C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x66359dde,0x01d72d76</date><accdate>0x66359dde,0x01d72d76</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>0x66359dde,0x01d72d76</date><accdate>0x66359dde,0x01d72d76</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):	5.102854479717978
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnYaxqaxtnWimI002EtM3MHdNMNxfnYaxqaxtnWimI00OYGe5EtMb:2d6NxgKqKtSZHKd6NxgKqKtSZ7YLjb
MD5:	37CFC681BA4129146B9053628963BE51
SHA1:	07EDAE7C0D92EECB88C60D687B1DEFDB351FF960
SHA-256:	0DBFF7B7AFA666D1885C9C0BBF76592148DF06493CEEC087419F299F2F2054A0
SHA-512:	48CDBFD9E0DA97E0568836936C5DDAA8BEB12BE82931BC2EB092EDB74A517BED647514023C054661A00EC9D20F79A856DD1DCD495248CC5B9A6F719F884F48 7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x66380035,0x01d72d76</date><a ccdate>0x66380035,0x01d72d76</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>0x66380035,0x01d72d76</date><a ccdate>0x66380035,0x01d72d76</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\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20532, version 1.1
Category:	downloaded
Size (bytes):	20532
Entropy (8bit):	7.966425322589798
Encrypted:	false
SSDEEP:	384:tfEIIA0zhnegvIQxhXmqd8lpP/FwL0cV8yP1JSRHbNHlZL7qwZkoEu3HTbpXcyKd:tr0zhnewHxRmqd8PdwLLeR/ZLGwZLbTA
MD5:	DA2721C68B4BC80DB8D4C404F76B118C
SHA1:	3A32E8B7EFBC9DFB52F024D657B8C8C0A80E5804
SHA-256:	BD811625271ACCA47F7DAC48B460F13E08EE947B2A8E17E278C4D5CCB5D9323C
SHA-512:	5110656E41A261BD2A06F8B5B2A362FF8836B4289E1DE0777D83DB8E9D709C4C4248B67653A28FA47AD4AE823021ADBFC587900E142BF6887C2A7C936F7F4C33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff
Preview:	wOFF.....P4.....l.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`t...cmap.....#cvt .....\...\1..Kfpgm...8...2.....$.gasp...l.....glyf... x..<e..n..W..hdmx..H....m....+1.3head..IP...6...6...rhhea..I.... ...$....hmtx..I.....S.loca..L8.....maxp..N4... ... .4..name..NT.....:.post..O0..... .m.dprep..OD.....S.. .)x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&./ 6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D.._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..>}{....|.....DT..N....Hy.F.Jez.....7. 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20332, version 1.1
Category:	downloaded
Size (bytes):	20332
Entropy (8bit):	7.970235088150752
Encrypted:	false
SSDEEP:	384:U0iwaxoOUPVkOJJSu6SsCKTIRDqG9oHKwZh98OSv+MsgkAOY:75mlUmOSu1guh+fZhLSxkAr
MD5:	DC3E086FC0C5ADDC09702E111D2ADB42
SHA1:	B1138B84FF19EAC5F43C4202297529D389BD09B7
SHA-256:	EA50AC7FDDB61A5CE248A7F8B3A31A98FE16285E076B16E6DA6B4E10910724BB
SHA-512:	10123C785C396CF0844751A014413ECF4D058AD0C00CAAEF5F8FFEF504C370F03EACD0B3C2A49211EEE0877B7AE7D0EF6E01264F04FC910C2660584B5E943BE
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....Ol.....x.....GDEF.....G...d....GPOS.....IGSUB.....OS/2...L...P...`t...cmap.....#cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf.. .L..;...m.&.x.hdmx..H....m..../.head..H....6...6.j.zhhea..H.... ...$....hmtx..H.....]uloca..Kp.....m,maxp..Mp... ... .4..name..M.....t.U9.post..N`..... .m.dprep..Nt.....I .f..x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y. .C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..").[...._..T..T.. ...+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[1].css	
Size (bytes):	1201
Entropy (8bit):	5.121392988253753
Encrypted:	false
SSDEEP:	24:5/iOYP0aNxoh/iOYGaNxsl/iOY7aNxUv/iOY4aNxa/iOYN0aNx5/iOYkaNxi8:UOS0aNhO1aNROEaNKCOXaNbOpaNGObaB
MD5:	46B23D5DA766A6942E67152A54C8E8AF
SHA1:	FE14DD484957BE4959CD054111529A0CAB7B4328
SHA-256:	8F3BA63CDC337593307BD2C831E8D69605E1C3890FC4A7E7D096450982EE9060
SHA-512:	1B85EF91C4D690E8F87CB7ADD8402FD8140347496C96B6FA9947AEF4AA50C3CAC17883B4CF1AD7F562B61D40AFEEA398E44107165179E0D9C55EE3172DCD8C F
Malicious:	false
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 100;. font-display: swap;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOkCnqEu92Fr1MmgV xIIzQ.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/roboto/v2 7/KFOlCnqEu92Fr1MmSU5fBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https: //fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. font-display: swap;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font- weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOkCnqEu92Fr1MmgVxIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20424, version 1.1
Category:	downloaded
Size (bytes):	20424
Entropy (8bit):	7.973322748597765
Encrypted:	false
SSDEEP:	384:UaoO8n3eceZ+fUC1WCz8P+IgjhYSHA/fFb4+hQC:Bl8nOcBfUqT/jOgAiC
MD5:	04B7FD97F88B82DCCCE5EC446CCC29E6
SHA1:	9A3C1CE2EAB659A91AF7016570287428CC82C458
SHA-256:	A38AD0B609E4D2039D18B0F9DC89E9060F2E2E05F2F42764A6A93354346A6C37
SHA-512:	4B71614F447F4E250AB8060026BA002F3F0DAA9286F207AA4B0652201D9053BD72865C09D1AB90155CF932E17D5897D7A1F659C98F1B1AACFDF6397D6DB47DA8
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOkCnqEu92Fr1MmgVxIIzQ.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t..{cmap.....#cvt .....H...H.2..fpgm.....3...._...gasp...0.....glyf...<..<...q....Lhdmx..H....q...."&.(head..l@...6...6.G..hhea..Ix... ...$...whmtx..I....y.....lCloca..L.....X.;.maxp..N.... ... .4..name..N4.....x..9.post..O..... .m.dprep..O..... +6.x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._.T..T... ..+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20404, version 1.1
Category:	downloaded
Size (bytes):	20404
Entropy (8bit):	7.970248785137973
Encrypted:	false
SSDEEP:	384:8uFoOxqigBacqKz8RGLv6K5a+jZ/rFSyeM5B8r/WjRy0BsM16t/PJ:PFlIvUKz8R+t5N53eGar/gY0Bv6tp
MD5:	BF0F407102FAF3A0B521D3B545F547A5
SHA1:	CA357CD0DE5DD0242E8EFACFB8D24AB60FDC86AB
SHA-256:	855A06974032BB69157D469ABA6F63440E8BE47C421F45C3F396F4E0B87B6DE8
SHA-512:	85359028F7FE49B1DF90B72E48DC7DE4B21F1B65E8BF109595705A3F4EAF9FA79854B5AEF060FE266291C5ECE9D04FCEAD1DE09BAA2C5E20601E1579212520C 8
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF.....O.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t6..cmap.....#cvt .....X...X/...fpgm.....4.....".gasp...@.....glyf.. .L..<'..m..]5Yhdmx..Ht...m....),..head..H....6...6.Y.ihhea..I.... ...$....hmtx..I<.....Dd.loca..K.....maxp..M.... ... .4.\name..M.....|..9.post..N..... .m.dprep..N.....:z /.Wx...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.|.k..NF.....mox.;...7&.Y.. C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._.2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._.T..T... ..+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.|{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20396, version 1.1
Category:	downloaded
Size (bytes):	20396
Entropy (8bit):	7.974131663185347
Encrypted:	false
SSDEEP:	384:SfXdUIIA0zhyKR28ePpAwxZ5M3py8wtshtdf45DEVTGdYb7H2Q/VEgm:Svdj0zhbRmjIQ8wtsV4lEVGdY3/i/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
MD5:	68D6DABFE54E245E7D5D5C16C3C4B1A9
SHA1:	7FDAB895EAEBECEDB3FB5473EAB94A1B292CEF19
SHA-256:	A01A632E56731A854F35701AA8C3A6A19A113290D9032FF9048F8064C45383BD
SHA-512:	44EB151F85178A2F9600E85AD43FAE470FABE0F247C9A03E67931B36028E600C7550D9DE2D69B3576A06577A5DEAF54822EE4BDC9DCBB47588D1972C8A959D4
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`u...cmap.....#cvt .....H...H+~..fpgm...$...3...._...gasp...X..... ...glyf...d..< .l..C^]hdmx..H....m....03#7head..H....6...6...\hhea..I,... ...$.&..hmtx..IL.....".J.loca..K.....maxp..M.... ... .4..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&. /6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\..\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\KFOlCnqEu92Fr1MmYUtfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20412, version 1.1
Category:	downloaded
Size (bytes):	20412
Entropy (8bit):	7.970834733902595
Encrypted:	false
SSDEEP:	384:af5t4IIA0zhLqV6fCjKK/bF+ituwbilrCG36/C4odv4QobGOo8y0rO+:arn0zhLqnDFbuwb0rCGPdv4QoKOByf+
MD5:	64BBA9C4E8156C152050C657E9D24BF1
SHA1:	90ECF87091FAABE7BC0FF54A43828FA4DD483278
SHA-256:	D33864E01E5103EBE439732BB606E694C73B6851F24DA25D41901EB17CB5D98E
SHA-512:	2456A688A4C51759293E482D434A324BA81EFAC9DC203226007C256D468E424A88C678D1B8BCAD9E3950C6AC4F7FF76CACAD71A730709A600CA45569586910C
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmYUtfBBc-.woff
Preview:	wOFF.....O.....|.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...O...`v...cmap.....#cvt .....Z...Z...=fpgm...4...3.....#.gasp...h.....glyf... t..<...lL....hdmx..H....n....47(;head..H....6...6...Rhhea..I,... ...$.]..hmtx..IL.....,.A.loca..K.....Bs.maxp..M.... ... .4..name..M.....\|..9.post..N..... .m.dprep..N.....8...Cx...1.. P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....\|o..c.x.R.r"B.....m...../.&. /6..5D.AGX.....)<'.)....?.... .Y4>\|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\..\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	88145
Entropy (8bit):	5.291106244832159
Encrypted:	false
SSDEEP:	1536:yTExXUZinxD7oPEZxkMV4SYKFMbRHZ6H5HOHCWrcElzuu7BRCKKBEqBsojZlOPma:ygZm0H5HO5+gCKWZyPmHQ47GKe
MD5:	220AFD743D9E9643852E31A135A9F3AE
SHA1:	88523924351BAC0B5D560FE0C5781E2556E7693D
SHA-256:	0925E8AD7BD971391A8B1E98BE8E87A6971919EB5B60C196485941C3C1DF089A
SHA-512:	6E722FCE1E8553BE592B1A741972C7F5B7B0CDAFCE230E9D2D587D20283482881C96660682E4095A5F14DF45A96EC193A9B222030C53B1B7BBE8312B2EAE440I
Malicious:	false
IE Cache URL:	http://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js
Preview:	/*! jQuery v3.4.1 | (c) JS Foundation and other contributors | jquery.org/license */.!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports? module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window? window:this,function(C,e){"use strict";var t=[],E=C.document,r=Object.getPrototypeOf,s=t.slice,g=t.concat,u=t.push,i=t.indexOf,n={},o=n.toString,v=n.hasOwnProperty ,a=v.toString,l=a.call(Object),y={},m=function(e){return"function"==typeof e&&"number"!=typeof e.nodeType},x=function(e){return null!=e&&e===e.window},c={type:! 0,src:!0,nonce:!0,noModule:!0};function b(e,t,n){var r,i,o=(n=n||E).createElement("script");if(o.text=e,t)for(r in c)(i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild(o)}function w(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?n[o.call(e)]||"object":typeof e}var

C:\Users\user\AppData\Local\Temp\~DF7FB1374DB7F2A750.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	36099
Entropy (8bit):	0.617090788279253
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+6cGPc3GU/7cwpkWp/7cw7RiG:kBqoxKAuqR+6cGPc38WkB
MD5:	5475D1F2385E329DFC26CCA1400AF599
SHA1:	916315E738AC1BA062922F77EB7B38642DE8AC22
SHA-256:	FABAD26B7C951933E2BAE0BCAB74044753D49B0639DF0CD27D453A5EB45033B0

C:\Users\user\AppData\Local\Temp\~DF7FB1374DB7F2A750.TMP	
SHA-512:	266B4961D9F70C91A5B7E5118A1ED9E9AC2647B0C4313357D1D1C4C8328F251BD844E9275255A835821C6C19159142C180435D5D1F81851747C59C7C17E5A236
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFD164B0FD8321DF14.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
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFD54D0D56F24D12CD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5074213590624014
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRsF9l8fRM9lTqmhjwKR:c9lLh9lLh9lIn9lIn9lo89loM9lWA
MD5:	70DFAE05CF68E68E2EBB1465580895A9
SHA1:	92772860E02632EF297FB81A9FABEF9ABED29FB2
SHA-256:	B38F372AB5A18F67DA11B4CA3DD2CEF176F80A5AA97E24ECB1E6C84AA9211A74
SHA-512:	C1C3E9C630DBCE672552FF89AA7B846E097A743576F111AD790E0C5EB90FDD4907260D2B54417DF370107AE2637F24DC9849FBC0014AB6B2059226CDA73D07C
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.937000649346314
TrID:	
File name:	NCA Approval Letter.html
File size:	785492
MD5:	2afd53761ef2429d41a21b16067b27c0
SHA1:	608645dc128a0986dbf4b9779fa3c9dee89eff6e
SHA256:	6b432f5c38d2deb98fb938341cf8a9732555b4992c310a7edd010594fa723b13
SHA512:	e781aa2d07edf4c7259a9a641241fe71ea935283a9bc5c8c238bde7895cbe1b9381bd332cbacc9c02519e87e2ad4f50d52917d423b1798af2306476794dc82df
SSDEEP:	12288:EH7o9Qto881Ev5aPCN1VYwcQUMiDOwmmjHa6yeVl2OuJYetlUkKQ5B:Mo9QzgPsX/NiDOjbxnlUkLB

General

File Content Preview:	.....<!DOCTYPE html>..<html lang="en">....<head>.. <meta charset="UTF-8">.. <meta name="viewport" content="width=device-width, initial-scale=1.0">.. <meta http-equiv="X-UA-Compatible" content="ie=edge">.. .. <title>Box</title>...<style>..@im

File Icon

Icon Hash:	f8c89c9a9a998cb8

Network Behavior

UDP Packets

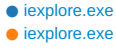
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 21:26:57.996661901 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:26:58.009994984 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 9, 2021 21:26:58.351927996 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:26:58.364542961 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 9, 2021 21:26:59.508533955 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:26:59.522056103 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:00.489165068 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:00.502079964 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:01.765924931 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:01.778595924 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:02.827483892 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:02.840403080 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:05.030769110 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:05.042927980 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:06.069360971 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:06.087990999 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:06.317768097 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:06.331510067 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:07.218071938 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:07.231585979 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:07.252063036 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:07.265917063 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:07.451211929 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:07.466367006 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:07.588026047 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:07.602699041 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:08.934061050 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:08.946814060 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:09.967880011 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:09.980690002 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:10.874299049 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:10.886929989 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:11.894840002 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:11.908945084 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:12.880855083 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:12.894756079 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:13.682895899 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:13.696218967 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:14.749063969 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:14.761704922 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:15.748873949 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:15.763983965 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:16.702337027 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:16.714786053 CEST	53	61522	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 21:27:17.702330112 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:17.716602087 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:18.823328972 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:18.835555077 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:27.676862001 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:27.690907955 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:30.667608976 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:30.689150095 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:36.084928989 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:36.103457928 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:36.730932951 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:36.743005037 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:37.084623098 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:37.107393980 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:37.722568989 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:37.735203028 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:38.183957100 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:38.197880030 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:38.740578890 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:38.754288912 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:40.176042080 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:40.190048933 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:41.144942999 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:41.158552885 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:44.177603006 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:44.192661047 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 9, 2021 21:27:45.145298004 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:27:45.159262896 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 9, 2021 21:28:04.441483974 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:28:04.476761103 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 9, 2021 21:28:06.652054071 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:28:06.671284914 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 9, 2021 21:28:39.063524961 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:28:39.091188908 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 9, 2021 21:28:49.255738020 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:28:49.283576012 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 9, 2021 21:28:50.881957054 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 9, 2021 21:28:50.900454998 CEST	53	50183	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6552 Parent PID: 800

General

Start time:	21:27:05
Start date:	09/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6f1f70000
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

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: 6600 Parent PID: 6552

General

Start time:	21:27:05

Start date:	09/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6552 CREDAT:17410 /prefetch:2
Imagebase:	0xd90000
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

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

Disassembly