ID: 384715
Sample Name:
#Ud83d#Udcde.htm
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 16:47:59
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

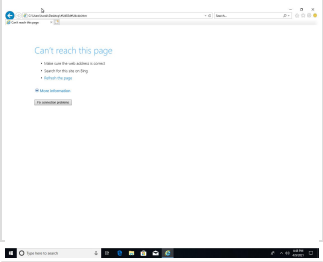
Analysis Report #Ud83d#Udcde.htm

Overview

General Information

Sample Name:	#Ud83d#Udcde.htm
Analysis ID:	384715
MD5:	5d44cee8d28ceb..
SHA1:	b53e4a9f2a2efe9..
SHA256:	c77e9dbffd377fe…
Infos:	

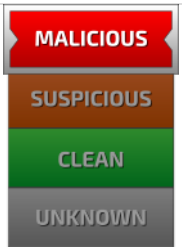
Most interesting Screenshot:



Errors

⚠ URL in Office document is not reachable.

Detection



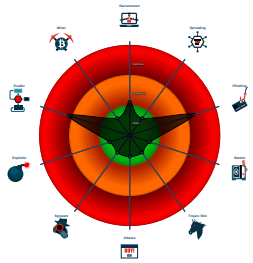
HTMLPhisher

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish35
- Obfuscated HTML file found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4604 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5488 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4604 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

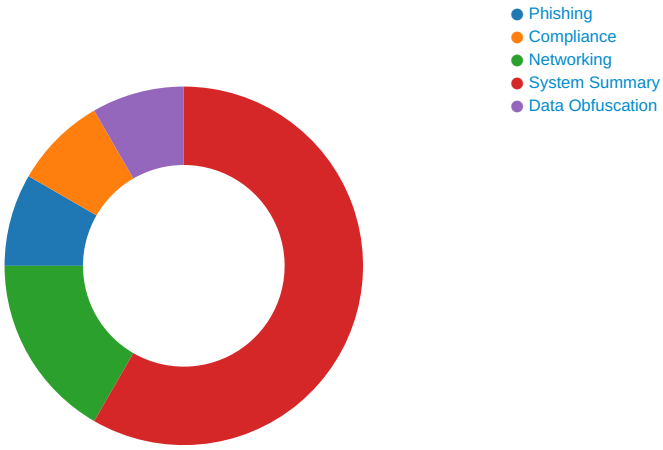
Initial Sample

Source	Rule	Description	Author	Strings
#Ud83d#Udcde.htm	JoeSecurity_HtmlPhish_35	Yara detected HtmlPhish_35	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Phishing:

Yara detected HtmlPhish35

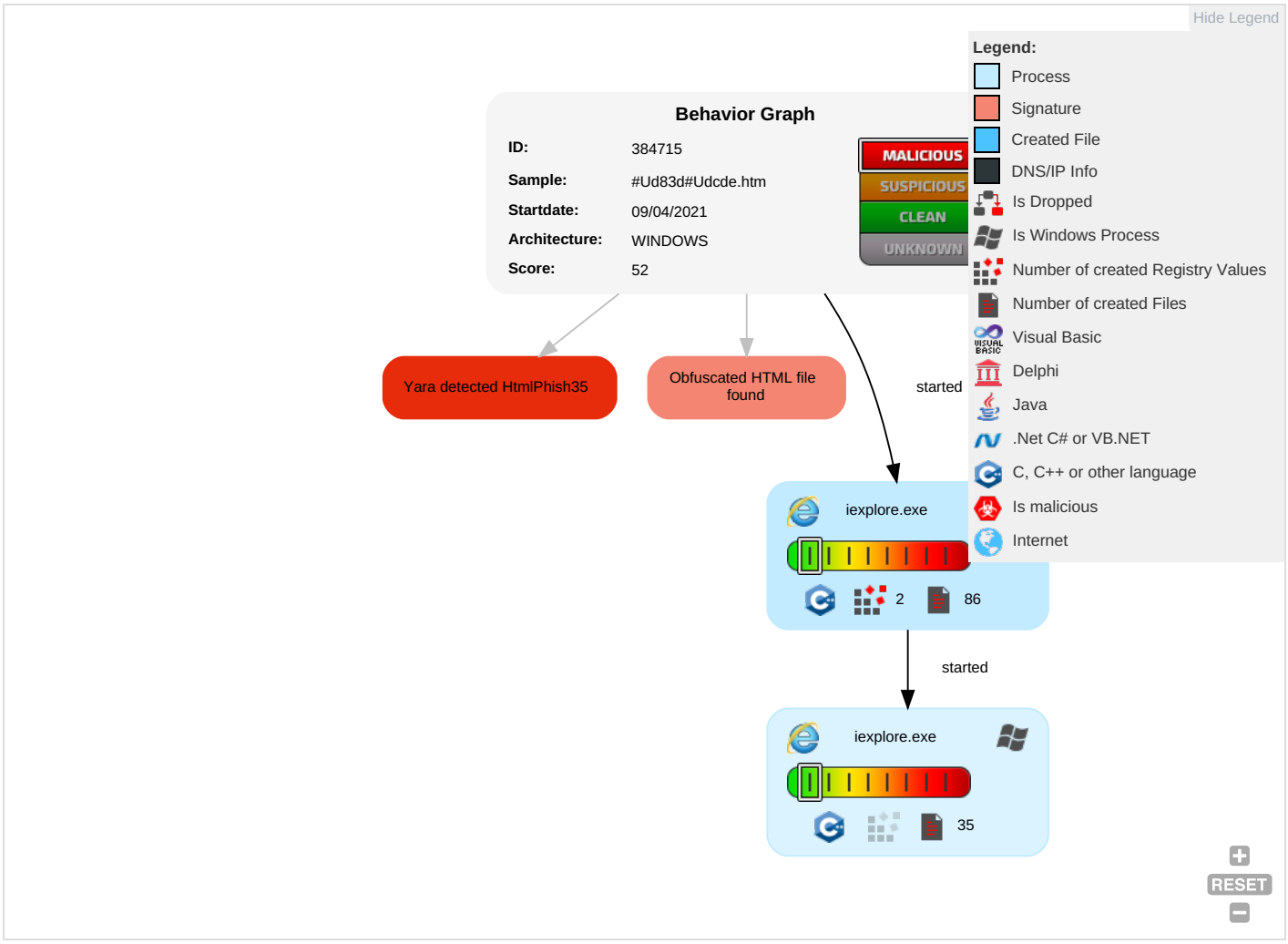
Data Obfuscation:

Obfuscated HTML file found

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	Impa
Valid Accounts	Scripting 1	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	Modif Syste Partit
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	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

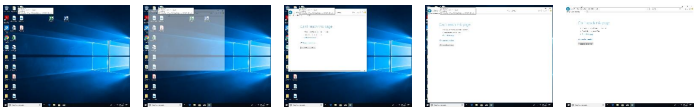
Behavior Graph

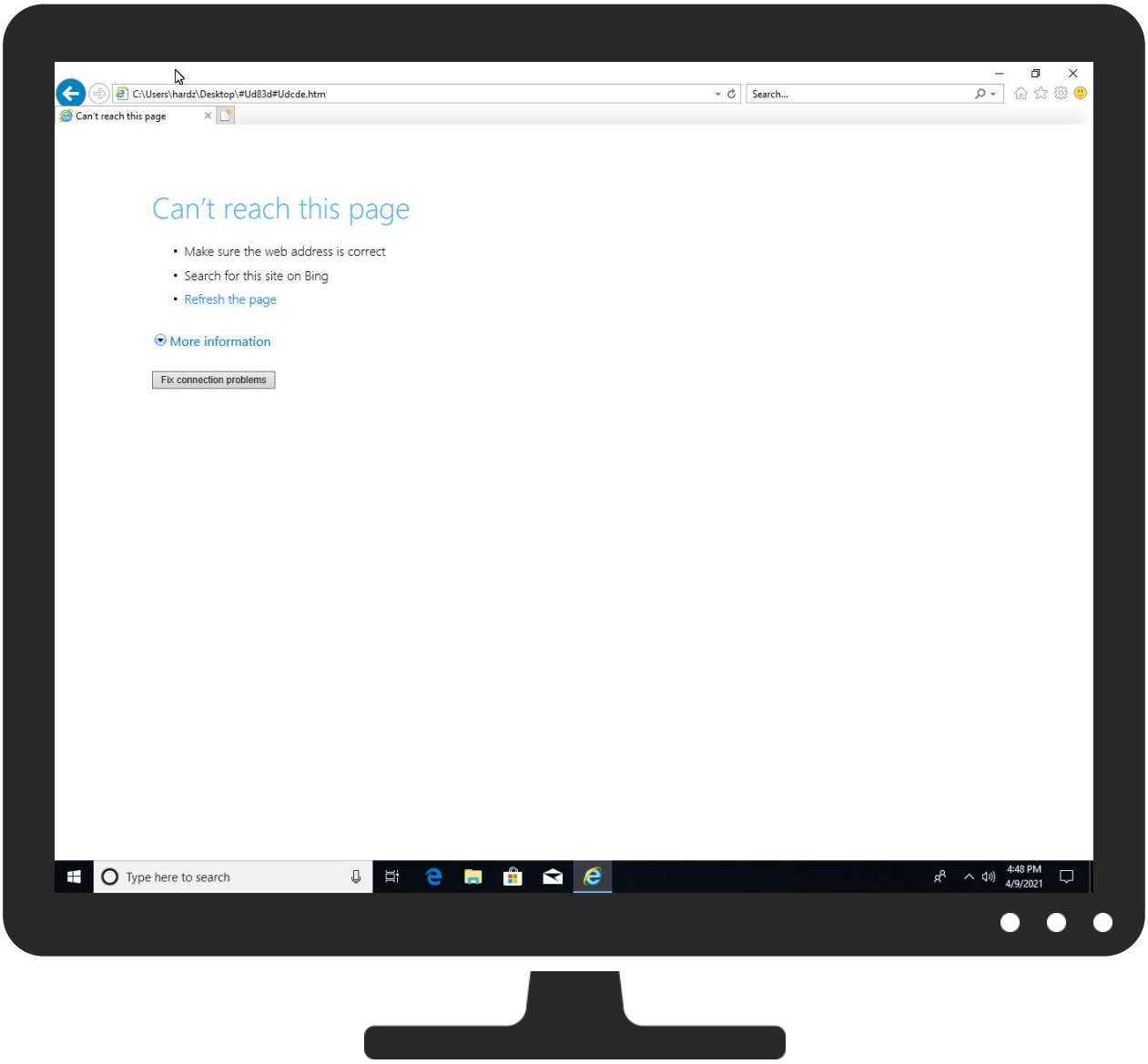


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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://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	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://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

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384715
Start date:	09.04.2021
Start time:	16:47:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#Ud83d#Udcde.htm
Cookbook file name:	defaultwindowshtmlcookbook.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:	35
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:	mal52.phis.evad.winHTM@3/20@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm • **URL browsing timeout or error**

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.139.144, 52.147.198.201, 104.83.120.32, 20.82.209.183, 23.10.249.26, 23.10.249.43, 152.199.19.161, 40.88.32.150, 95.100.54.203, 20.50.102.62, 20.82.210.154, 20.54.26.129, 23.54.113.53 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net
Errors:	• URL in Office document is not reachable.

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.{1BF4E5EF-998E-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8577983835684746
Encrypted:	false
SSDEEP:	96:rvZEZA2NWJWtJxofJNCWtMJ5OrJ+oJJTGfJvCbdX:rvZEZA2NW4t8fDRMUB4f1MX
MD5:	529D3DB5B781618C00AD60A51F014CAF
SHA1:	1D239959404EF4D269BF0AE2B5C3C3DB2B3D8FB6
SHA-256:	3F128DCE06A29F189EAD00C2F0D46A09BEEA1F5CE5A945EED38A79922076DD1F
SHA-512:	E6570FAA05F28142B72CB8E7E4C4F821780B4453CE5157CD4BE24EE086B60165B75A58052367220FC2255D61038EC9A8376BB1CA59EC4B1A7BB4C69591C51065
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\{1BF4E5F1-998E-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	34968
Entropy (8bit):	2.004349274643038
Encrypted:	false
SSDEEP:	192:rXZIQ46KkAjx2xWIM0ve08Jl4IpsI0FUBg:rJxDjCggtO3+v8ia
MD5:	3356054BF941DFF719E1A73A4C5C832C
SHA1:	F6B78D27A911AA9B6EEC20882B9E1530603CE201
SHA-256:	1473C8E6EC8C711AC04C24C95D5F61E9ED61383763B133D754DE3B574E636E37
SHA-512:	BF0B0E954B6BE485238332B09C80EF480AE2075026201C22C23A5CDE5C7E60B23E7649657959FB23BB42C83C2814A18CE0270235FA30A3FE45B13547108C347F
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\{1BF4E5F2-998E-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5672365755520632
Encrypted:	false
SSDEEP:	48:IwfGcprhGwpaYG4pQMGrapbSXGQpK9oG7HpRjTGIpG:r1Z7QI6KBShAhTJA
MD5:	32680EA53F5AE8DFC530765654C03D94
SHA1:	FA977485A4B1A97A0A35D699F4E1892786F38329
SHA-256:	FD2DFD45A5F06F53974095689D9722318A8CFAF97FCD267243A316B0AE15285A
SHA-512:	45A97C298F329ED34CBBB8C7F0F41F4055A173A4D3A26CAD0114A872B7036B8C206CE0A56A49837371C3E59169465EF797B644A15032BF918861330C23FEF9BF
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):	5.1012502598982215

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE3vCtGNnWimI002EtM3MHdNMNxOE3vCtGNnWimI00ObVbkEtMb:2d6NxO2q0NSZHKd6NxO2q0NSZ76b
MD5:	FA5577BA41F3B3A2BFA3CAB152024A16
SHA1:	D823ACB18D33825B940013C54F582E667972A793
SHA-256:	1A8BA1CF0A80896EFEF86161ADB0C51CF1B5A40D6A4FB0940491744ADA72B806
SHA-512:	AF4351A42762BB18BAF42E67AAAAFE6ADE61FFC2EF857678BDE2CBB31A7DACA8ED7444EB5D81BDFD34576425E828AE9BC9902321FAC3553E37B875D11D201A51
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xf12b7812,0x01d72d9a</date><accdate>0xf12b7812,0x01d72d9a</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>0xf12b7812,0x01d72d9a</date><accdate>0xf12b7812,0x01d72d9a</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):	5.092206219883086
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kM5f959GNnWimI002EtM3MHdNMNxe2kM5f959GNnWimI00Obkak6Es:2d6Nxrh5F5kNSZHKd6Nxrh5F5kNSZ7AS
MD5:	3911E46BAB451E9FDC0D7DB83ADB8A95
SHA1:	EB22511DFA7550EC4CACC36A2862470675BA0119
SHA-256:	91BA20FF997CBCDA4B52541E4B959CC8FEDFD6DF938A4CBA1099DB7CEE86B341
SHA-512:	EE776E5E10D0D8728A137D960C39FFB6489D64FB7B40EE709671A11880E0F97415B1A77B0E963B2D6B20A8DE93562C47872F06E373A71AFB7CC67F8074988969
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xf121eebb,0x01d72d9a</date><accdate>0xf121eebb,0x01d72d9a</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>0xf121eebb,0x01d72d9a</date><accdate>0xf121eebb,0x01d72d9a</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):	5.119050805521552
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL3vCtGNnWimI002EtM3MHdNMNxvL3vCtGNnWimI00ObmZEtMb:2d6Nxvzq0NSZHKd6Nxvzq0NSZ7mb
MD5:	0924EC6A79BE144BC77D2D711629375D
SHA1:	5DCF1409033036D1944D8F54BD8C5F2486611562
SHA-256:	AD862AB47D20474C1813C1A10C2EF4E5AE8513D49DFE6776B9F45D5A3331F160
SHA-512:	9B784FD115BFD9808E9C255B8076305689A755295820F48436FB570CF7E328BC7CA9F81C25C5EC675FD77FAF5696C3132CD3F843F818AA7A51727D62AB8AC9EE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xf12b7812,0x01d72d9a</date><accdate>0xf12b7812,0x01d72d9a</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>0xf12b7812,0x01d72d9a</date><accdate>0xf12b7812,0x01d72d9a</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):	5.121772425260688
Encrypted:	false
SSDEEP:	12:TMHdNMNxiEY1CGNnWimI002EtM3MHdNMNxiEY1CGNnWimI00Obd5EtMb:2d6NxnQFNSZHKd6NxnQFNSZ7Jjb
MD5:	9C2448BAC20A375092C5031A0A16B60B
SHA1:	3CE6A1D0E94D7CA1DDE55244440E7FB62A446F71
SHA-256:	5A70F3B1895BDA8B505D8D5F9B11D5E9FA54165EADFEA6FC4683B3A872756092

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA-512:	669F0B388102B9EDA701968D2BF40C2F003B6149651E6D4BB36CD33A79F9A5C4023ED06D1AD6B2CF3B148B37E3C9467F3B97EEFEC5EA1800516F6712190FC9F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xf12915b7,0x01d72d9a</date><acc date>0xf12915b7,0x01d72d9a</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>0xf12915b7,0x01d72d9a</date><accdate>0xf12915b7,0x01d72d9a</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):	5.132350759447095
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw3vCtGNnWimI002EtM3MHdNMNxhGw3vCtGNnWimI00Ob8K075EtMb:2d6NxQaq0NSZHKd6NxQaq0NSZ7YKajb
MD5:	6D285E0CFC2AE2A5DD9EC6B4B71552BB
SHA1:	B4FDA351AFF439EFAA421C8119AF2A076F946FFE
SHA-256:	3446FF4BE82C43358CD39FE9D63BAE5644886BC114FBEC402B892FD0EE0B1D95
SHA-512:	3271FA23D1EB54DADE12B9F5126001DE5130B8ACE908C3D82D155581971EF02B958BF98848E086CCFD9A6FCC88F4AAED00AC3D296B96DE8B76E0523DB5C5B4 97
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xf12b7812,0x01d72d9a</date>< accdate>0xf12b7812,0x01d72d9a</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>0xf12b7812,0x01d72d9a</date><accdate>0 xf12b7812,0x01d72d9a</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):	5.108121643642992
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nEY1CGNnWimI002EtM3MHdNMNx0nEYCtGNnWimI00ObxEtMb:2d6Nx0EQFNSZHKd6Nx0Ez0NSZ7nb
MD5:	5BD7A65CE54F9475F4C803D024A1656F
SHA1:	91F25DC62ABACE5AEA2CC27D7CC60B589243EEDA
SHA-256:	DF9FE2BDE2AB6E52B1940EB68188ED0D3DFDA4268312BA6D71E0D69D4C507535
SHA-512:	0B170D69E710E623B16762BACBB3EFA64285714E05E5C23F3D5E78C44E887BBCFD5040E0123C652102B7C24E707EB6C98F09DC1DB9A2B010742CD3480E3A135 D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xf12915b7,0x01d72d9a</date><a ccdate>0xf12915b7,0x01d72d9a</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>0xf12915b7,0x01d72d9a</date><accdate>0xf 12b7812,0x01d72d9a</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\pin202591677780\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):	5.146276933743086
Encrypted:	false
SSDEEP:	12:TMHdNMNxxEY1CGNnWimI002EtM3MHdNMNxxEY1CGNnWimI00Ob6Kq5EtMb:2d6Nx2QFNSZHKd6Nx2QFNSZ7ob
MD5:	D9220FD2FB735911686DCB049A3F3BAE
SHA1:	97BE84676E16857BBE23E73E5DD3C3B640DD5F81
SHA-256:	5276FB4968E44392C42A9BDD16FCFEED0EA559D1CEE7648B0D155D31573682C3
SHA-512:	AF0D66EF2592C47F2BA06149A148C2B23AD31EFCABB57B62FA4FD35BED783326EC4B998AF523D75639D5FFC2987CE3417FADA0BAA4887CCCACA8158FC06DF E36
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xf12915b7,0x01d72d9a</date><accdate>0xf12915b7,0x01d72d9a</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>0xf12915b7,0x01d72d9a</date><accdate>0xf12915b7,0x01d72d9a</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):	5.133539658800769
Encrypted:	false
SSDEEP:	12:TMHdNMNxcFv4tGNnWimI002EtM3MHdNMNxcFv4tGNnWimI00ObVEtMb:2d6Nxcw0NSZHKd6Nxcw0NSZ7Db
MD5:	9B277619AE3D239EAAEBDBF0E20416A9
SHA1:	BFF85EEE7A5111A9E6C040A50D2D55D444803E9F
SHA-256:	9BDB8DA41F3A703BD456ACEDC0F11B30E40D61138EAA1EB148CF3CC3E5DDE3F2
SHA-512:	DF5F3A948286D5911CD14289270DC2B7E5756AEF04DA89CB3E26F6D4C0FAD2B66A376CB0EE224919ED49BD11E1DFF8656A3F69E8AA9BE9E56C9DF4FF3196A5E0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf126b372,0x01d72d9a</date><accdate>0xf126b372,0x01d72d9a</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>0xf126b372,0x01d72d9a</date><accdate>0xf126b372,0x01d72d9a</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):	5.120682610214922
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnFv4tGNnWimI002EtM3MHdNMNxfnFv1CGNnWimI00Obe5EtMb:2d6NxNw0NSZHKd6NxNdFNSZ7ijb
MD5:	E6D8D4868726613CB1FB1F6CFCC82294
SHA1:	BFFE4EBA449B855DF8ABFEAC0F362F6456E2D4DB
SHA-256:	73E554BC713A257ABC270A953F597ABD6115755655B135104AF961894FF6E345
SHA-512:	11D374D4945234C50C30599EA96EF0646BABA079D26FEB907ACF2EAD7BC26E9B366F9A49C54E726A292A25A86C3FC44BDBE805D9A3142C7829A682FAED1A86B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf126b372,0x01d72d9a</date><accdate>0xf126b372,0x01d72d9a</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>0xf126b372,0x01d72d9a</date><accdate>0xf12915b7,0x01d72d9a</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\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/errorPageStrings.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dnserror[1]	
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Temp\~DF66F230E66A897653.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\~DF6EB57ED6FD070CBB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47896554910023414
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loYtF9loYn9lWYbRwIRkduwIRkdnkdthuhA:kBqoITFpjGT
MD5:	10961072E197DC9164A404831A397C4C
SHA1:	344C66A8A05FE13C6EEFEB1D06B0028CAC2F6E8F
SHA-256:	CBBEC659E6F11B46A7815E9CFEB85B06E211F8CB5CAA4BA64735E2565FCCE6ED
SHA-512:	B785767884D71714F1CC63FB9AED47379D4AFB8B8B8A98B993727B5D9EEA4778C16B270485C9CC4EF23CA0AAA3BFE3EFCB8810779DB3EFE3A464ED79AE2065C0
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE6EAF55C3EFBA2B3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DFE6EAF55C3EFBA2B3.TMP	
Category:	dropped
Size (bytes):	44169
Entropy (8bit):	1.3443058489048458
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+mg6Tg7M2ilOs32eBu7viUJN+N8/VeMvrzEil2eBu7viUJN+N8/b:kBqoxKAuqR+mg6Tg7MJlp/fry/fr2
MD5:	616ACBC6A2841A6456BD4E257974B029
SHA1:	8F92B98FE828D712BB12F2F5F83C5080C96C7D92
SHA-256:	736BD494ECEF89143CA7445E3F74A3F33BE98C6675673BF73E0C474B41494A06
SHA-512:	A0F08B5E83F283D510481A84588D6379E04D419831693516CCAA2B44EAD03066B9BCFE3680EC5E3CD48648701B0AC7498229D7BCEAD25DF6C0AE22195D01796
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Entropy (8bit):	6.001485823782198
TrID:	• HyperText Markup Language (15015/1) 20.56% • HyperText Markup Language (12001/1) 16.44% • HyperText Markup Language (12001/1) 16.44% • HyperText Markup Language (11501/1) 15.75% • HyperText Markup Language (11501/1) 15.75%
File name:	#Ud83d#Udcde.htm
File size:	5008
MD5:	5d44cee8d28cebf028ac3afc7c4309d0
SHA1:	b53e4a9f2a2efe93ca896cd6a56af26bf861cf0f
SHA256:	c77e9dbffd377fe486c902715fd1d5587c2c7ef58cfb2839284d109a72a6a645
SHA512:	5b780cf8fe3e3ae18ef82c5ce00cdcbc21a591bd4283a2169446c2fff5d5728f9730f9382f093760e44d7734940cc599d954cc3f0b7fde04fa4e4b599215f32a
SSDEEP:	96:RPCt3y7Xc3CXZXXbFn+jk2EYi3hmU3ZVrkqsnQaKA9jhGZxTc0hLat:gt3y7XfXZXEk2EYi3hV3ZPSUrZxXg
File Content Preview:	<!DOCTYPE html><html><head><script>var mizzs="Y2hlcnJ5cEB1d2diLmVkdQ=="</script>..<script>var paso1="@!&wAV9fCcXIbQnz4oSp@&!OehA8igcfspk3JE5MoTRF1DZPdwS6&@!";if(window.location.href.indexOf("bre=")==-1) window.location.href = document.location.pathname+"

Network Behavior

UDP Packets

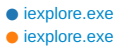
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:48:35.776309013 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:48:35.788712978 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 9, 2021 16:48:37.775918961 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:48:37.788491964 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 9, 2021 16:48:38.437644958 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:48:38.450244904 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 9, 2021 16:48:39.298160076 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:48:39.311851025 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 9, 2021 16:48:41.922792912 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:48:41.943383932 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 9, 2021 16:48:44.263015032 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:48:44.276182890 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 9, 2021 16:48:53.025429010 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:48:53.040402889 CEST	53	58361	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 16:48:55.467267036 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:48:55.483159065 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 9, 2021 16:48:58.799864054 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:48:58.812514067 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:01.542345047 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:01.557282925 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:02.342935085 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:02.358896971 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:03.008661032 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:03.021655083 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:03.211007118 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:03.223623991 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:03.634320021 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:03.649322033 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:05.117769003 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:05.130742073 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:08.056973934 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:08.074805021 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:09.715960979 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:09.729191065 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:10.482801914 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:10.495407104 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:11.475661993 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:11.487840891 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:12.072616100 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:12.087064981 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:12.404416084 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:12.419790030 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:12.567594051 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:12.580827951 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:13.066031933 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:13.079132080 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:13.564762115 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:13.577703953 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:14.080488920 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:14.093643904 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:14.580457926 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:14.593215942 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:16.099196911 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:16.111917973 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:16.837147951 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:16.850107908 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:17.714143991 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:17.735352039 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:20.112317085 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:20.124046087 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:20.846620083 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:20.859268904 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:38.228400946 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:38.241431952 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 9, 2021 16:49:44.749378920 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:49:44.767862082 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 9, 2021 16:50:13.474402905 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:50:13.613092899 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 9, 2021 16:50:21.477319956 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:50:21.503181934 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 9, 2021 16:50:24.468103886 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:50:24.486752033 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 9, 2021 16:51:03.027721882 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:51:03.040455103 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 9, 2021 16:51:03.250854015 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 9, 2021 16:51:03.284955025 CEST	53	61292	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4604 Parent PID: 792

General

Start time:	16:48:40
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:	0x7ff71b160000
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	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: 5488 Parent PID: 4604

General

Start time:	16:48:41
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:4604 CREDAT:17410 /prefetch:2
Imagebase:	0xea0000
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

Disassembly