ID: 433128
Sample Name: Payment Data.html
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 11:09:28
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

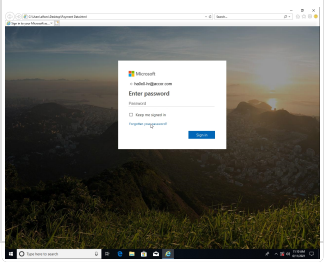
Analysis Report Payment Data.html

Overview

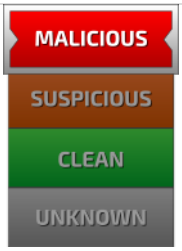
General Information

Sample Name:	Payment Data.html
Analysis ID:	433128
MD5:	c3334584ded661..
SHA1:	d10d17599c325e..
SHA256:	6ea0976949a655..
Infos:	

Most interesting Screenshot:



Detection



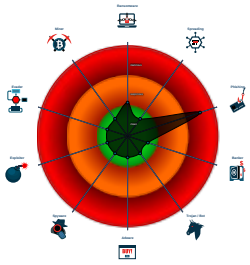
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish19
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- None HTTPS page querying sensitiv…
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5108 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5888 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5108 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Payment Data.html	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
Payment Data.html	JoeSecurity_HtmlPhish_19	Yara detected HtmlPhish_19	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Phishing:

Yara detected HtmlPhish10

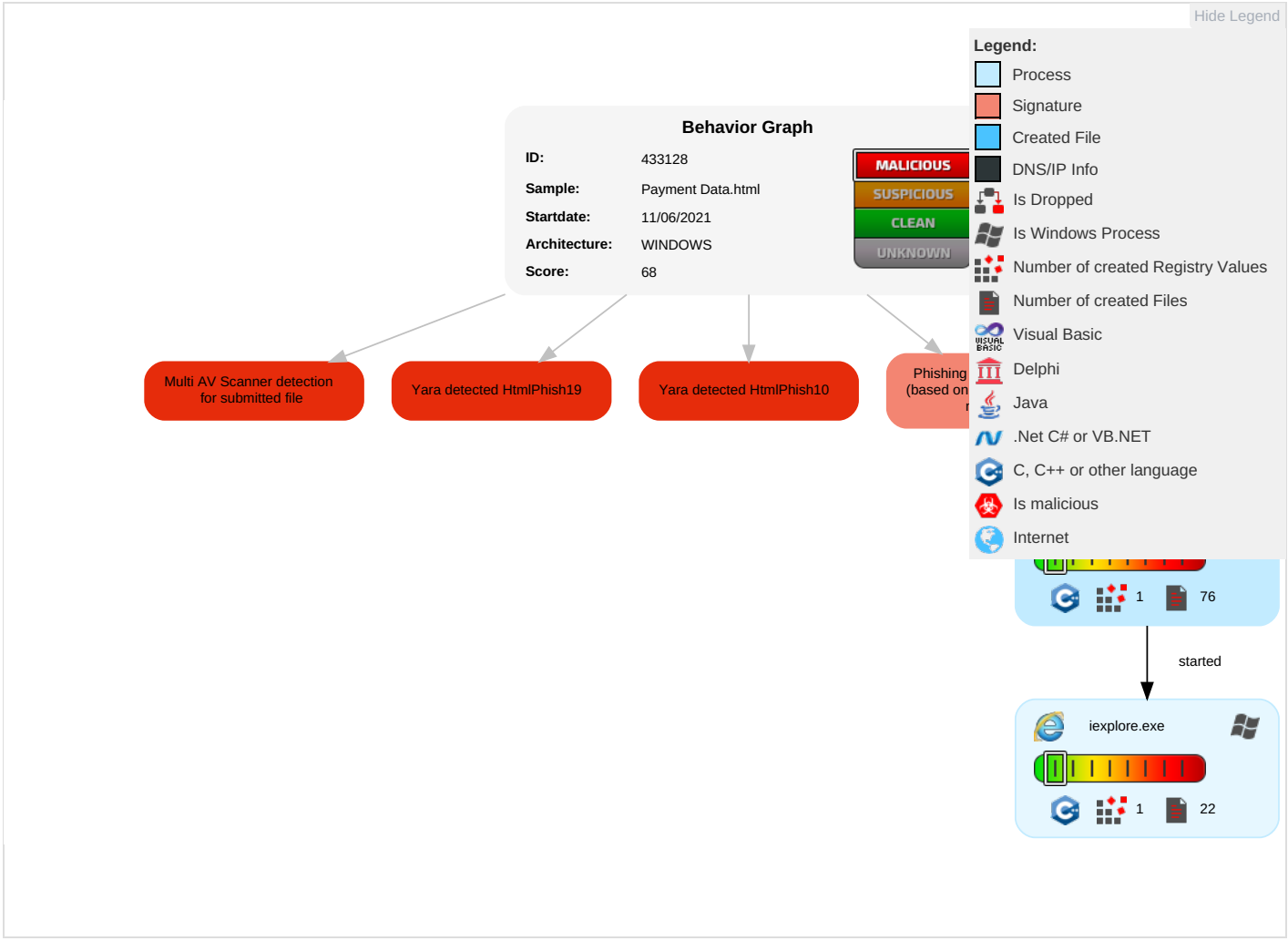
Yara detected HtmlPhish19

Phishing site detected (based on logo template match)

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	In
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	M Sy Pa
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	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 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	D D D

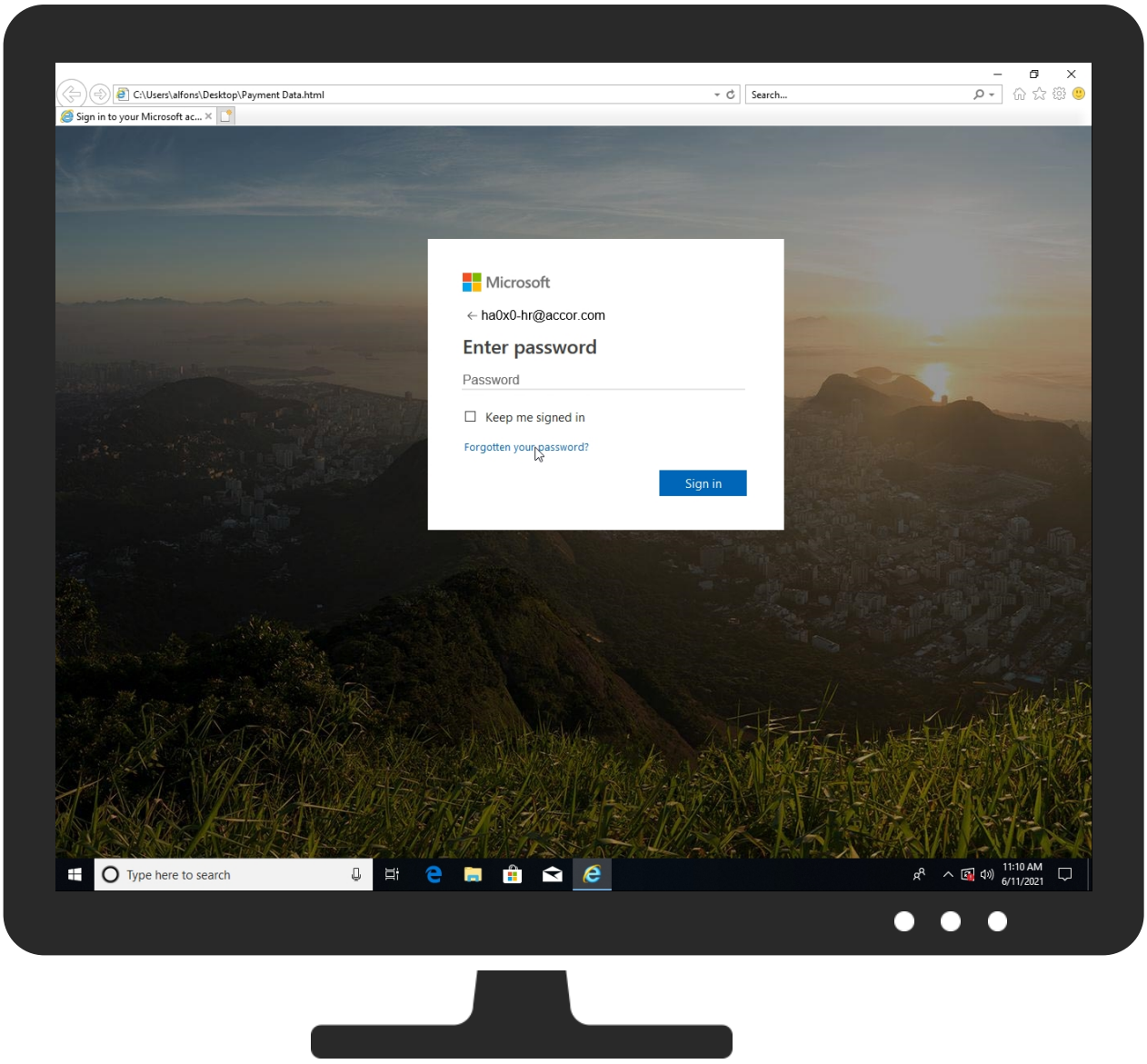
Behavior Graph



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
Payment Data.html	12%	Virustotal		Browse

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	

Source	Detection	Scanner	Label	Link
http://https://cristoenlinea.tv/yellow.php	5%	Virustotal		Browse
http://https://cristoenlinea.tv/yellow.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/Payment%20Data.html	true		low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433128
Start date:	11.06.2021
Start time:	11:09:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Data.html
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:	30
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:	mal68.phis.winHTML@3/15@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html
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.{452781B6-CAE0-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8532463398055872
Encrypted:	false
SSDEEP:	96:rLZQZp2XWStvbf7z0KMqMqo/SQo6xfomzh6X:rLZQZp2XWStzf7NMkoroEfomMX
MD5:	1EDD2A8EFDFD3F62BA5CAA885DEF5F58
SHA1:	014CD8FF071A3128EB9610E645013079C02C20A0
SHA-256:	27D970AF7AF642882B7BD2816D0C6F27ADF1FD4D054FE334D2F2760A949A3708
SHA-512:	E425DDD29C69C01055C233396083EB7AEACED584E387C01FE625F584285F5329B5139D8481A6378D65F2CF70B674328524EB93E9882BBDF012A25D2EF023E686
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\{452781B8-CAE0-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28350
Entropy (8bit):	1.934106019579748
Encrypted:	false
SSDEEP:	48:IwzGcpraGwpaaG4pQ2GrapbSQGQpBuGHHpcfTGUp82xGzYpmSYyGophsfwG2XpKN:rJZCQa64BSYj92pW2/M/aHnMN2RhfeRr
MD5:	CC98FF2AA379C6620F89559A07CB071A
SHA1:	7120D92C0408749FB68EA625B7FF062E6655E52D
SHA-256:	C29D74BC52CD9F84428CE04A70F5B3A8AD1A589AC47199C24D242CC254EDD894

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{452781B8-CAE0-11EB-90E5-ECF4BB570DC9}.dat	
SHA-512:	C281C0A0FAF9B7110B6C3EF8FFF3E139E0EE3D351F29F4C84BA78DA1D0BA9067AC38ECBAF6F9AD413A18F83A6C998EAD0325B00801BCA103C82D7AC314DEBE96
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\{452781B9-CAE0-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5638307386229509
Encrypted:	false
SSDEEP:	48:IwuGcprPGwpaLG4pQRhGrapbS5GQpKoWG7HpRQTGIpG:ryZ5QN6RxBSTAoBTEA
MD5:	4EF5B99E91A57D4D4C66875E591CFBA6
SHA1:	EA431FFAC00F32B05D500B9948B80B9AD8A19252
SHA-256:	F958C269536AD8FDAF0BCE4E6829502522F16EEB80D07E46366447FE419C353F
SHA-512:	5D24621D9F2D941DFB102DC692BF9C8CA81F52BA967102C737C7CD3A081D2F3B4FBC617954FD3F8B332FF411569DB30514CE394AF18F4E911BF8C4D1BFB36B2
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.045892959304556
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE3LUELUwnWimI002EtM3MHdNMNxOE3LUBnWimI00ONVbkEtMb:2d6NxOav3SZHKd6NxOacSZ7Qb
MD5:	B3888AC0B9D43F7A86510DD6A326CE64
SHA1:	E2A1528C6EFDCD46D8A1D66237BAD5BC658150BE
SHA-256:	4F9AEBC1A3C21000BA6018685107F4F13DFCA423969D23BFA2C32DFEA7BBFCBF
SHA-512:	E0904D754761D04C5BAAE4201BFB3558E30B1A6BB41FC1461229BC80C2EFC68D0E8E0269360F2ECD8D8FCA4D77E9F664D55E75668BE517029DD8C09E22A7F8E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</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>0x1a7d1410,0x01d75eed</date><accdate>0x1a869d89,0x01d75eed</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.044231084204398
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k3LUELUwnWimI002EtM3MHdNMNxe2k3LUELUwnWimI00ONkak6EtMb:2d6Nxr6v3SZHKd6Nxr6v3SZ72a7b
MD5:	E27F236C18E437CD7AF9467032DF1072
SHA1:	6668E36FF5586AF5B76BADEDE0B8BE6EA0930217
SHA-256:	28B5D2F05642D8A845A199F59CD508C3981B8CA57C8439036B9BEE547D925E99
SHA-512:	889AACC3E197490CB375CFEAEEE4B62A1219DED57C67C73A6C60A233963843E6AB0C16A95AC95BD1A8CCDB228CB55E3B4CCB0D87955E96B6D29F02BA1C3D6FB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</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>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.089087752051609
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLZnWimI002EtM3MHdNMNxvLZnWimI00ONmZEtMb:2d6NxvFSZHKd6NxvFSZ7Ub
MD5:	2EC3FADF0ADB3801B07115045F914F9C
SHA1:	8A930FD9C5260FDFA0485DB7B44604C32C44FF2D
SHA-256:	995A39471C453E841C08289F6057E022D5640905321F034E27D7D9E3230D6326
SHA-512:	ED281AECE04672A9FF7364060D41B41D4A917BDE094CA25860A1FCCAD18190DB71874CB3BB435A49CABD803EBE85C334832408004C93EFF04B123A34D100C8F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x1a869d89,0x01d75eed</date><accdate>0x1a869d89,0x01d75eed</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>0x1a869d89,0x01d75eed</date><accdate>0x1a869d89,0x01d75eed</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.031521063741118
Encrypted:	false
SSDEEP:	12:TMHdNMNxi3LUELUwnWimI002EtM3MHdNMNxi3LUELUwnWimI00ONd5EtMb:2d6Nxkv3SZHKd6Nxkv3SZ7njb
MD5:	D806649E701D7299F3BA57E6EBC02ACE
SHA1:	F6121B2E931748B5B4DBCEAEF6BB930EE4F69ADF
SHA-256:	891F2D38D6926313F6F6550CB2E2037FA17E57B191EFDF17DB6780373DFF3579
SHA-512:	41C652510A3C238D48F2B047BD5B1A3AC5B97CE94A168334393178FD6EFFEA429A3D134BEC256D7AF8E09E5930E2F2C70A19BB961CC538032E671C474D57F9B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</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>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.1063824171621395
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwZnWimI002EtM3MHdNMNxhGwZnWimI00ON8K075EtMb:2d6NxQ4SZHKd6NxQ4SZ7uKajb
MD5:	2121880B007B38FCD239C030239FBB6E
SHA1:	A623B9E129EC1C4836FDAAEAE06566AD116958AF
SHA-256:	369922DA314F0FE1BD8945A8CBEFE78A46D871A56E5C51AB07D46DF5669CDEC7
SHA-512:	6A70BF4B9C870D7E779E0D341DC10A11DC37D9BF34ADA92E28327931AD620C1BC81EE5DAF9C8E31DA0B1AB2EA2B3343750CB7115E5D21C7E2C6646897924439
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x1a869d89,0x01d75eed</date><accdate>0x1a869d89,0x01d75eed</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>0x1a869d89,0x01d75eed</date><accdate>0x1a869d89,0x01d75eed</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-6757900\msapplication.xml	

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.016133600134568
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n3LUELUwnWimI002EtM3MHdNMNx0n3LUELUwnWimI00ONxEtMb:2d6Nx07v3SZHKd6Nx07v3SZ7Vb
MD5:	6C1CBF011C6109C4F085ED8D43BD369C
SHA1:	65DAB39FC3488E44AC89EC1B6BE8AA1102D1C32D
SHA-256:	8B8EAC0BB5F8F5C5B0108B88EBBB7C34797D7112C7BA9ED57D191FD6E36E3682
SHA-512:	4BCA7B4CFA88B52485F3CE477F285CF42C289803AC65851D4376280BCA395D326DA64A23E31C12A7035FFFFF3F49263B45EA17B2991844CF5D7A20AECD57FC3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</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>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.056992239173104
Encrypted:	false
SSDEEP:	12:TMHdNMNxx3LUELUwnWimI002EtM3MHdNMNxx3LUELUwnWimI00ON6Kq5EtMb:2d6NxRv3SZHKd6NxRv3SZ7ub
MD5:	4ACF79F0E1C175105942202C2D752681
SHA1:	B12FBA5514D0301E2F6A2CE98A0E5E8AE6A656BA
SHA-256:	09C8720131E700D052113A000530EFD78B5F9A7B94E28EB9F6037F6D93EF9ECE
SHA-512:	909773AA625506D24F5744649F83498980B3BE5BC4A1976FEA87CCC1F254E1D7693D51F75585F3F8F575FD286530DBF42EABA7041DCB5B1D6DC2AF750CEBAE7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</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>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.037541494186377
Encrypted:	false
SSDEEP:	12:TMHdNMNxc3LUELUwnWimI002EtM3MHdNMNxc3LUELUwnWimI00ONVEtMb:2d6Nxiv3SZHKd6Nxiv3SZ71b
MD5:	E4AA3632C9AE1E1651E21AC3912F4364
SHA1:	30208868F92F06102BA8B86E20B7E6DA6D4B16BC
SHA-256:	6AD1DB34AA10CA7ED308D277A538D459F83850B7A9E8B269EAED31396137AA46
SHA-512:	3068A5C0F0D79858DED24B35CC185EEA856940D08CEE15EC2399448392A02763F6851633D007166930B43F1A238B7A5ADF046A9D693DEB24D10F461D2F1EEF2A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</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>0x1a7d1410,0x01d75eed</date><accdate>0x1a7d1410,0x01d75eed</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.017511107114451
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn3LUELUwnWimI002EtM3MHdNMNxfn3LUELUwnWimI00ONe5EtMb:2d6Nxjv3SZHKd6Nxjv3SZ7Ejb
MD5:	3F79EE03F22073372B47B2E38B2D4B57
SHA1:	C93A256BBCE66C02DD67014C4ECE4C6117867FBF
SHA-256:	981B531B4E2804097FFABB407AF1F502F85D435B54946E0F1E0FE2561D14C985
SHA-512:	E83D30A8513ECC0B98BD28B7691C652762EF72C1618020934AEFA0BA25744774D351AFA411E5562B29313F65A9CC204565843D1667DFCA3EFEED33F3D908C54
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x1a7d1410,0x01d75eed</date><a ccdate>0x1a7d1410,0x01d75eed</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>0x1a7d1410,0x01d75eed</date><a ccdate>0x1a7d1410,0x01d75eed</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Temp\~DF230B8C90068586DB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48232140842757887
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loT9loT9lWV0ylYYH:kBqoIUKV/Ye
MD5:	F75B5D1916A687B6E8766B1A742B6781
SHA1:	9C43A4EF27E3D7508BB2796CBD97696B7CFE136F
SHA-256:	FB193BE961DAAEABAA580E7E1DC6EDF69BDD8F7F5AE9654828010ADDA06DAF46
SHA-512:	826311FE2A14FD120053D0F0665FC9BCF98ED8A01DBC308FBA9674BA1B418632928B26CF55A2052F2D26932D9D61EE059584C11B4D2952550224F50B9E101ECF
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF691E1308E941992B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3950516366741589
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAggttFqveaP:kBqoxxJhHWSVSEabtjqvS7zHEN
MD5:	E1ABE93EE632C016A19F2E71192398C0
SHA1:	51EF11D38262EBA73C6934308665FB69B340669A
SHA-256:	78A3981B2F4A3C8AAEB3030DA7FDBFAE6E8330AB2B29761926CE8FD3BA853E65
SHA-512:	4C0029EDB366DA4C74B3473654AC2B23C53C3EFBBA475EAEEAE1DCD0B42DFBE271A8FE4E04847FCB41D07EC6CBF013B1F93DEEC4EB7E782EAC210D239781 7148
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE05AA1654C2D9938.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	36111
Entropy (8bit):	0.6162514532113428
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+zN/2SISrsfSpPfYc2XfYchiS4STSx0V:kBqoxKAuvScS+zN/2dqt2Rhf

C:\Users\user\AppData\Local\Temp\~DFE05AA1654C2D9938.TMP	
MD5:	AAED3F6C69EF6A2B722EAD33702306DC
SHA1:	81A8C3813871D746EF9109D668F05881941A8CFF
SHA-256:	D15114E44F716C8A6EC859F94525F16035CC65B5A04A4EE32A239484838763AA
SHA-512:	EDF446513B9710B2F289B7C779A96D2FFA635927E27F32B29141BD31C8764B8BF5F7392D4A523C9DEF81AC2FD0615E1937C591518271F47E91DD569D9481B8FB
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):	5.953912123128076
TrID:	• HyperText Markup Language (6006/1) 54.56% • Synchronized Multimedia Integration Language (5002/2) 45.44%
File name:	Payment Data.html
File size:	431095
MD5:	c3334584ded66141a0c2b1c95e69086e
SHA1:	d10d17599c325e85ce8a43c70d7dfa419d2590db
SHA256:	6ea0976949a655738926cbb9072e3abd0be3e3d3779a75 c028dc88b888e736a1
SHA512:	1cccabea29e6e5efc7ebbc85f94dc7948ce2a564404acad ffe0c53a1a5279f418579ebe746428e413bacba1925231f 450d3bb35daeca42dd67d050cff32a2b6a
SSDEEP:	12288:qGDKhf2yW1MBoU2DY77S4C6Nu1xlvm2Jm+jf: HKhfvWAl/SOupg7
File Content Preview:	<html>...<meta http-equiv="Content-Language" content ="en">...<title>Sign in to your Microsoft account</title>... <link rel="icon" type="image/ico" href=" EAAAAAAA6A0AAM4oAAAwMBAAAAAAAGgGAAC2N gAAICAQAA

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5108 Parent PID: 792

General

Start time:	11:10:15
Start date:	11/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7d1480000
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: 5888 Parent PID: 5108

General

Start time:	11:10:16
Start date:	11/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5108 CREDAT:17410 /prefetch:2
Imagebase:	0x12e0000
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

Registry Activities

Show Windows behavior

Disassembly