ID: 655277
Sample Name: IP VM_8976544568.xhtml
Cookbook: default.jbs
Time: 20:50:22
Date: 30/06/2022
Version: 35.0.0 Citrine

Table of Contents

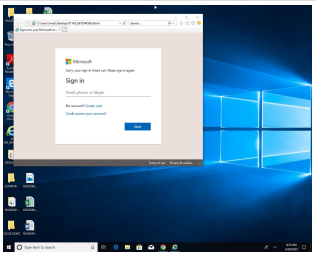
Windows Analysis Report

IP VM_8976544568.xhtml

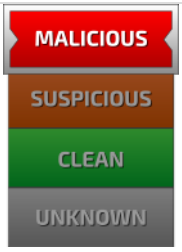
Overview

General Information

Sample Name:	IP VM_8976544568.xhtml
Analysis ID:	655277
MD5:	804a9bfbd0b974..
SHA1:	74af42444e8178..
SHA256:	ca479506434b4b..
Infos:	



Detection



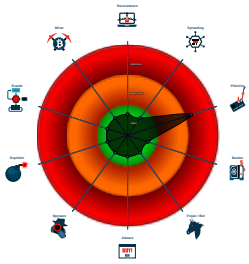
HTMLPhisher

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- JA3 SSL client fingerprint seen in co…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 6284 cmdline: "C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\user\Desktop\IP VM_8976544568.xhtml MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6352 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6284 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
IP VM_8976544568.xhtml	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

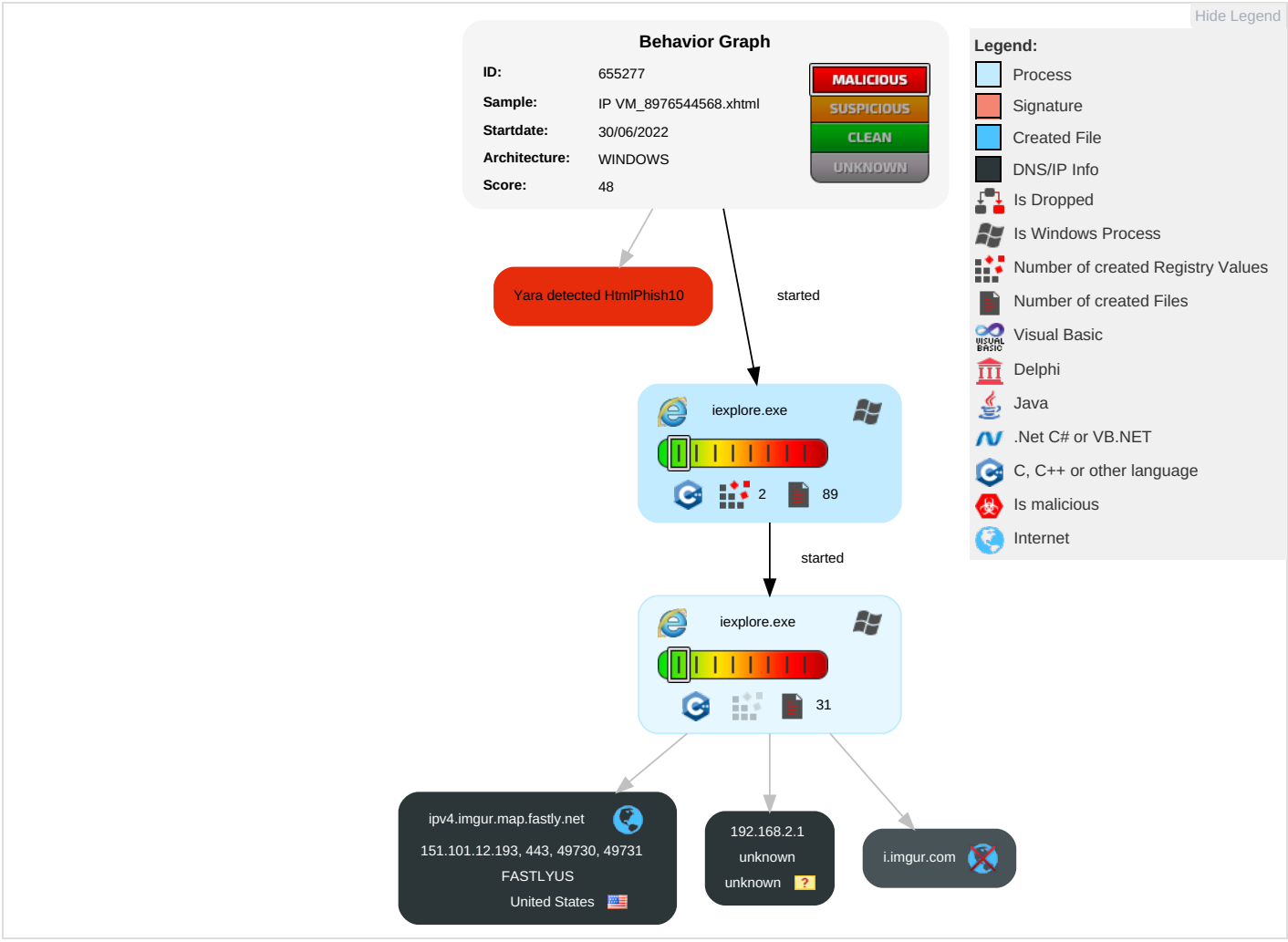
Phishing

Yara detected HtmlPhish10

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	1 Process Injection	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	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	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

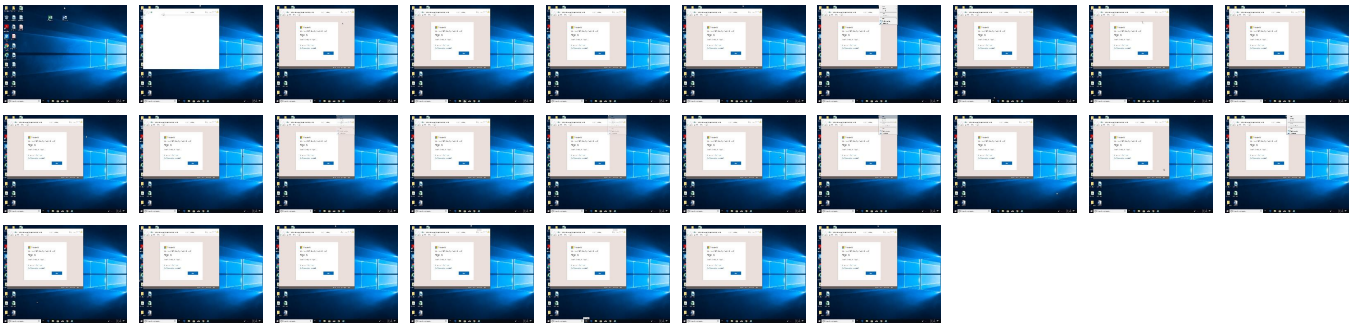
Behavior Graph

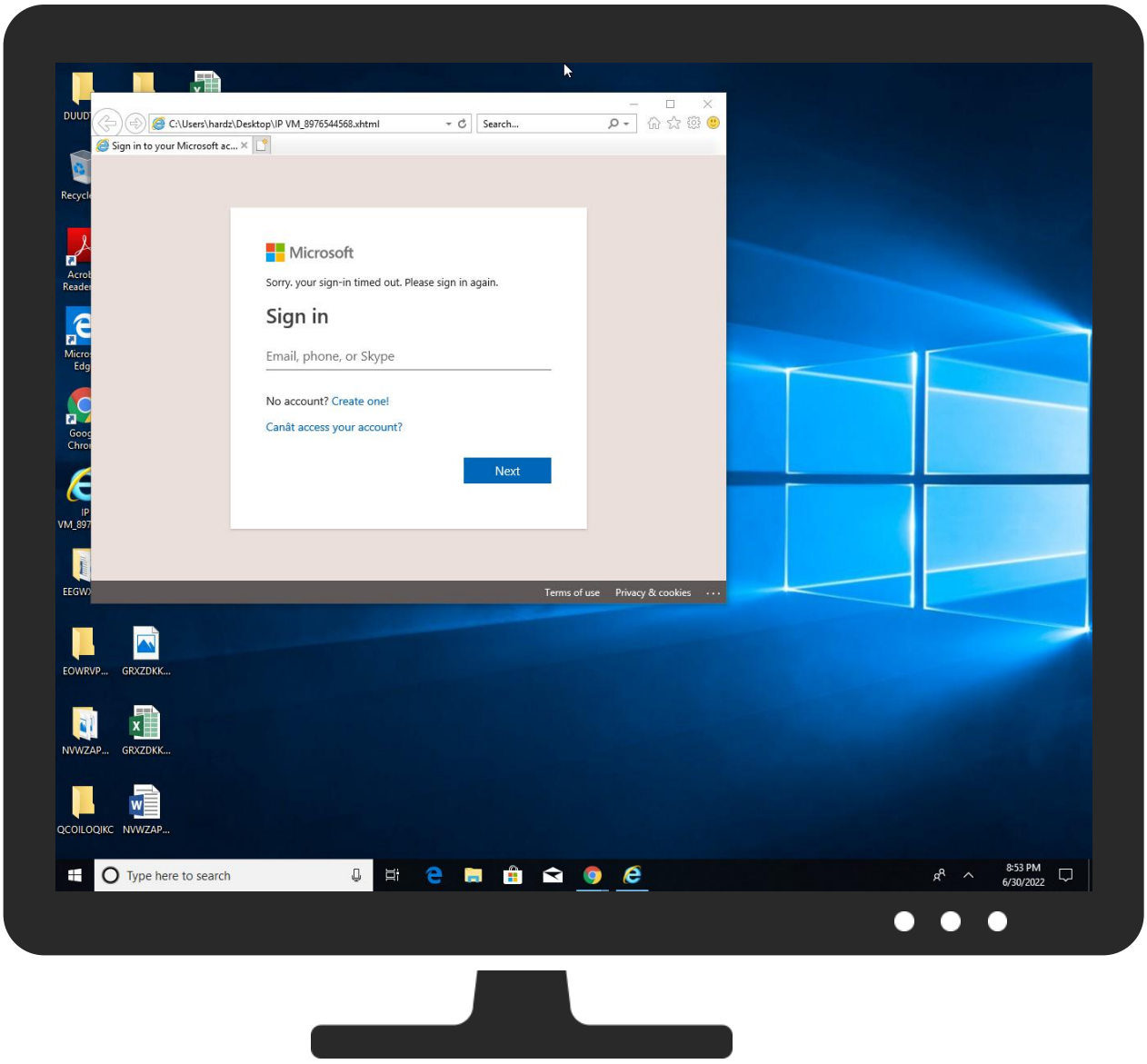


Screenshots

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
IP VM_8976544568.xhtml	0%	Virustotal		Browse
IP VM_8976544568.xhtml	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ipv4.imgur.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ipv4.imgur.map.fastly.net	151.101.12.193	true	false	• 0%, Virustotal, Browse	unknown
i.imgur.com	unknown	unknown	false		high

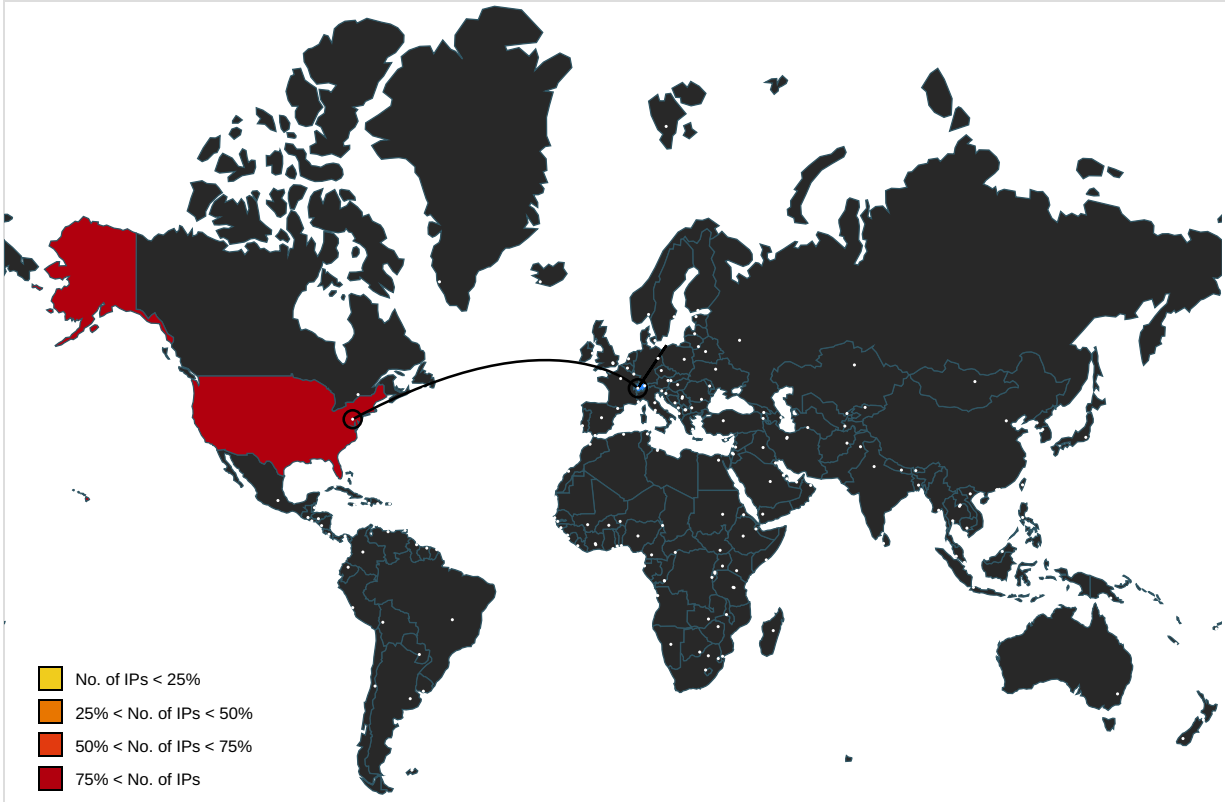
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://i.imgur.com/Jm3Kimw.png	false		high
http://https://i.imgur.com/NQUpBi2.png	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.0.dr	false	• URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.0.dr	false		high
http://www.nytimes.com/	msapplication.xml3.0.dr	false		high
http://www.live.com/	msapplication.xml2.0.dr	false		high
http://www.reddit.com/	msapplication.xml4.0.dr	false		high
http://www.twitter.com/	msapplication.xml5.0.dr	false		high
http://www.youtube.com/	msapplication.xml7.0.dr	false		high
http://www.google.com/	msapplication.xml1.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.12.193	ipv4.imgur.map.fastly.net	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655277
Start date and time: 30/06/202220:50:22	2022-06-30 20:50:22 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IP VM_8976544568.xhtml
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:	25
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:	mal48.phis.winXHTML@3/11@1/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xhtml • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 96.16.143.41, 152.199.19.161
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ie9comview.vo.msecnd.net, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, go.microsoft.com.edgekey.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, cs9.wpc.v0cdn.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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):	355
Entropy (8bit):	5.070196420426192
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc41EWnIM4TD90/QL3WIZK0QhPPWXpsVDHkEtMjwu:TMHdNMNxOEWnn4nWimI00ObVbkEtMb
MD5:	D96B5369AB2953E48EF3B8EBBCA85958
SHA1:	FC481FE79E82FC6667A041B8D653A5B48C029883
SHA-256:	433CF06E5B12C3C86AF7FBD8E0A868344DF1657C5638C8C8FAAF98E9FDEF1C4D
SHA-512:	2454ABD8E65AB6054B6B4A6576F735EBD6DEFD0C33C572552690A0EDB90EBD166BFE41317C61195227A3CEF9896D017F09F55C36BFA46B3FAD99DE23A5B023 7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xece9ebda,0x01d88cfd</date> accdate>0xed08e9b3,0x01d88cfd</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\T witter.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):	353
Entropy (8bit):	5.1293287195444135
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4fLGTklJlYeR2TD90/QL3WIZK0QhPPWXpskI5kU5EtMjwu:TMHdNMNxe2klzknWimI00Obkak6EtMb
MD5:	4284DF26200B52DA6C928EE94BDC82AF
SHA1:	9D1F93EB7C1F7B13044ACE13312F0A85C5533AB1
SHA-256:	BBA254ED4F65D0AB6DFCF175E879EF11665D7F6C9F6F4B582417922E369BE941
SHA-512:	E0CA353AF58610A3B161E1EFA0F62E31EB6297DEDEDD584D2B4633908F2B752AEAC764B6FA8A65B96E30ED02C1E8DED577DA3DC74414674436761FA68CE9C E47
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xeaccb599,0x01d88cfd</date><a ccdate>0xeaf2db35,0x01d88cfd</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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):	359
Entropy (8bit):	5.12610578801881
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4GLJ2zgNITD90/QL3WIZK0QhPPWXpsyhBcEEtMjwu:TMHdNMNxvL0zlnWimI00ObmZEtMb
MD5:	94D5A8FF581415663007824D8217ED93
SHA1:	6D1670801A272CE104707C482750434A4CFBBC80
SHA-256:	2D447B67481A1EB6FDE4EF290051B80BF23952FEAF3E694D1128F81382629164
SHA-512:	1E4B39392BA80B65C8DF5FBA87550FFB0CCD58E99CC13567AB1DE4A1C36BF5B448B35E183966137FA29FC4B879B9E1BB30F8856D214F2BCBA263874390FF700
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xed3d5d9b,0x01d88cfd</date> <accdate>0xed743390,0x01d88cfd</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):	349
Entropy (8bit):	5.102418865516137
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4Js+4oCDTD90/QL3WIZK0QhPPWXpsgE5EtMjwu:TMHdNMNxit4oCDnWimI00Obd5EtMb
MD5:	18C52A7FF2BC57FA114E4E9CCA4DADAC
SHA1:	E023C830411F953AB1442FA89C0BA17675FD355F
SHA-256:	37154FD9DE95D1D445E99E26029FA8A7B25FAE2F7A56A47D6D7BC0D201E23D70
SHA-512:	D13CCC089966547C2455682D0B24053F8C2329831CF60813A8616626BBF313EE49ED79FB15F4AA8B6FEEACB43BA827A3AE99AF58FA1C6097D341D0FF2F96308
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xebdee3b2,0x01d88cfd</date><acc date>0xebfde278,0x01d88cfd</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:	modified
Size (bytes):	355
Entropy (8bit):	5.103170991610456
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4UxGwinOTD90/QL3WIZK0QhPPWXps8K0QU5EtMjwu:TMHdNMNxhGwgOnWimI00Ob8K075EtMb
MD5:	52467B585B25E00E68EB91EA07F28F09
SHA1:	112DBA786D412994A063EED8CDEA33F2C000BD06
SHA-256:	14A375DA371C2B1F4E9F78FDF1812388CE678766695C6D134A18A315F814C6E9
SHA-512:	3888D91E9E5341642FA41EFC119E63FD1ED56344CE9A80826596A4DA0315870CA554B567432AFBE28439CFB468100365F432154217738BD504A4F84C4421C62B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xed93318e,0x01d88cfd</date>< accdate>0xedafce31,0x01d88cfd</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Y outube.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):	353
Entropy (8bit):	5.09826500603334
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4QunJ+JrOu5TD90/QL3WIZK0QhPPWXpsAkEtMjwu:TMHdNMNx0nm62nWimI00ObxEtMb

MD5:	0372FF80E5F1EB308CFD1B2CE79BBA17
SHA1:	075EB5E6C00ABBDA37719668BD31242C321841DE
SHA-256:	5B79B4BCE611763801C565CCF4B323B3F92A32643BF8E8F49F565C58F73AAE13
SHA-512:	D80A9E6FB7146AE686E6C8892298A3F2D26DE2010D4A351A8029B97981C3E6DD1DF04A7EC77909307EBDD61006496AE5AC732287F6F646114BCB6754D9B4505
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xec777a20,0x01d88cfd</date><a ccdate>0xecbc9e59,0x01d88cfd</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Re ddit.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):	355
Entropy (8bit):	5.180044543653231
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4oTgmBepimTD90/QL3WIZK0QhPPWXps6Kq5EtMjwu:TMHdNMNxxg2epimnWimI00Ob6Kq5EtMb
MD5:	CC768919453F6ADE14516F2EE1FB4308
SHA1:	F81B4D9D2484684C25A171E8F79627F8CD1F2F2D
SHA-256:	11EAD8B34AA868B229440547B6D5B91BC9C4396EB3EA8A3E6A10F6540A063B39
SHA-512:	6AAC6C8E6FD3914EDE3BD6A2ECF09437380B222145361A45F946140CB75DB89329B87A759114857EA0E86352FAB9C8706BB5D0891900740155C388BB9A537BFE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xec325664,0x01d88cfd</date>< accdate>0xec587bd7,0x01d88cfd</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\N YTimes.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):	357
Entropy (8bit):	5.124992959448571
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4YX2nrXvo5TD90/QL3WIZK0QhPPWXps02CqEtMjwu:TMHdNMNxcTv4nWimI00ObVEtMb
MD5:	BD2C76A9755F1BD8391CC9A8ACB4EED1
SHA1:	FC4CE7292D777E94FA5658D04EC86377D4D195F3
SHA-256:	AF3401064703C839E8DD3D2BF0A9BD0DB8DA8F9E59EB38CE2C258DA0A1683C3A
SHA-512:	72D74B94FEBE4ECD9E5D05295E29B47EA3405135879EC273505B48EACCA883A951D94EE66B04E2305EC15533ABD70450A38050C14F1B80C4C027698C5A7A3A7 B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xeb30d7ec,0x01d88cfd</date> <accdate>0xeb654bc9,0x01d88cfd</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):	353
Entropy (8bit):	5.088380797246651
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4InKs4IjVEDTD90/QL3WIZK0QhPPWXpsiwE5EtMjwu:TMHdNMNxfniIjV4nWimI00Obe5EtMb
MD5:	00A80571BEB1D90226E87312ED000A1C
SHA1:	8C00407C396E6193ABD51B32EF64E6A26771BF03
SHA-256:	646F5F92A1EEB4F2757142ACC6C94AC08DFAA07B75B8D9A9FE6295A3F00F989D
SHA-512:	87A358AEC5C32AD8F0320E64CA5D9F3175DB0A940887B46E07BE1C8BB385593F7335DB252AEEF53155B51DD2A37262D353444BAF1C440CF2CB24F973A45ED9 F
Malicious:	false

Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xeba348eb,0x01d88cfd</date><accdate>0xebbfe580,0x01d88cfd</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\PSUEOSZZ\Jm3Kimw[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 108 x 24, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1586
Entropy (8bit):	7.755536766236495
Encrypted:	false
SSDEEP:	24:Ss0JHVFE/OudK+QXOJ/BJX2/rproV8RXaRtKSRJsk6gpkexPnKNSE9SJpXuhS2dG:tI1q/OVuPupUjzKSPskCKWB9u8hS2U3
MD5:	3DEBDF39C16C7EC7446D2CB9864B24B9
SHA1:	B42C031518257E6474AD37C9BBEA372DCC9FD540
SHA-256:	83463B8064210A912F2D9A4A1600E5A0B0B9701F41A5B862EE95B5DD71A8785A
SHA-512:	2BCB2EEFDA76F0B2B215CF0EE18381A06B2A0461D91ADBBED53EE14AED501CE5E0FAEFB69F3A33306CC708E9B704221B2B25A422682425E447545E2DCD151D2F
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...I.....IDATh..ZMR#G...K.F.....p..]....;...(....k.... ".o...,N0..8Z.@#.V...25...11.t.....Y/_=.....H..^}z...Y.{..9.....C_.-..-a_../m...E.$-..[.....ai...k..U.....v.....YQ..CD"U=..._..4MD.}.7.....r/F.....^'kf.".....I.4..3...yf....n7&...H^.....fx!_E....$I....v.q ....,[....9af....E.....O.,.:.>UU.|._C....W...r.&..9..v.....W.R..@rZ.$.....8a$."r...+.y.;...Y".AU.....:U=.....^...q-...I.;..WUu\.....,;$..HDr*".<..Wm...}.....gYv.u.Vu%I.R.C..^|.....'.....iu.....|.m..3.....>.....Y,"'$..Y..h4.$.;.>.....,:....4M/Hv.6....^/2.....UU...h.H.s..y9.!....u...F;+..S..nt6.....iz%".>..+...g.../I.fUU..H..-.DU.f...{.E.-.....s..#.d..c3.....{.?x2:.@.XU'$....?..bG.I.+.....H.w.4#9.....s.....{...S6..G|...M..%....I.4..gY....0....4M.%.9w.....(.8.....G.z...R%.....8M..\..}E..af..(.sF...i..<.i.y>..'.pgg.....i..".OrZ.....<.q.o...m...~.....p..D.....`.e.LD.U..`..../..u....+d.}n.....BV...8...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\NQUpBi2[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	120
Entropy (8bit):	5.557874486268208
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lhkxn9gWZaBWaay1PkFJQllXuytDFexldp:6v/lhPR8bWVMYlxFejdp
MD5:	E7004A24D6E606CF714B8B06067FC8B2
SHA1:	9C49F10E5EB8B566E318EDEF67FD97C46F0C14DF
SHA-256:	895696E4A2FEFE97136406A427B805BD887B394272CB9178A2899366B02EBDCF
SHA-512:	BB08394916B9F33AF443B84135F0CB63472234263F828788190 47A309A182E18DB87E15C4F8DC29A431D8A15A6F45E46AC4AFFACE68CE6404178A14EA57C163B
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a...?IDAT8.c`....._..8.9.....P5..b.t.P..,P1F...%..c...X.G.@.../<..[i.....IEND.B`.

Static File Info

General

File type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.40728377889159
TrID:	• Scalable Vector Graphics (18501/1) 22.70% • HyperText Markup Language (12001/1) 14.72% • HyperText Markup Language (12001/1) 14.72% • HyperText Markup Language (11501/1) 14.11% • HyperText Markup Language (11501/1) 14.11%
File name:	IP VM_8976544568.xhtml
File size:	110240
MD5:	804a9bfbd0b974b9fd8f6910d46e45ae
SHA1:	74af42444e817841ef5a16ba9d055ca2f780c6f9
SHA256:	ca479506434b4bef9656293b03211a5bf01e854c3dea6802c2b4b3f6ab273cfa
SHA512:	566d99cb32369264d59c29a34393bb0a036d21cdf0161b6f68de05bfb7b6f4aa165967202d52e7a0342a7efdfe954fa5d3ce59cf898b0760b8155dcfa7b0f75a
SSDEEP:	1536:qqhuxk+Ex2azAFPWrR7qvwAFiGcpmKjaDmyUDqov:qqxXvyUu8
TLSH:	72B3D99459203C66D037873571C1BE8B62211503F637A9BFF6622DB9CF9968B0B31F89

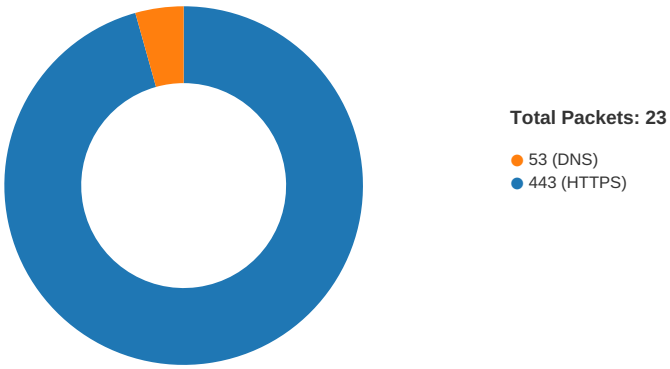
File Content Preview:	<?xml version="1.0" encoding="iso-8859-1"?>..<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">..<html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml">..<head>..<meta char

File Icon

Icon Hash:	e1e8ccdecccdf136

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 20:51:29.993369102 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:29.993419886 CEST	443	49730	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:29.993519068 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:29.994004965 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:29.994065046 CEST	443	49731	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:29.994143963 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.003549099 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.003587008 CEST	443	49730	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.003618002 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.003649950 CEST	443	49731	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.086260080 CEST	443	49731	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.086370945 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.086572886 CEST	443	49730	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.086673975 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.380017996 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.380054951 CEST	443	49730	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.380270958 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.380285025 CEST	443	49730	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.380633116 CEST	443	49730	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.380707026 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.387815952 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.387867928 CEST	443	49731	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.387893915 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.387921095 CEST	443	49731	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.388369083 CEST	443	49731	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.388472080 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.403979063 CEST	443	49730	151.101.12.193	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 20:51:30.404093027 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.404122114 CEST	443	49730	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.404151917 CEST	443	49730	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.404185057 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.404206991 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.405855894 CEST	49730	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.405885935 CEST	443	49730	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.419138908 CEST	443	49731	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.419282913 CEST	443	49731	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.419316053 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.419344902 CEST	443	49731	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.419394016 CEST	443	49731	151.101.12.193	192.168.2.3
Jun 30, 2022 20:51:30.419588089 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.419605970 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.440450907 CEST	49731	443	192.168.2.3	151.101.12.193
Jun 30, 2022 20:51:30.440496922 CEST	443	49731	151.101.12.193	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2022 20:51:29.954133034 CEST	57723	53	192.168.2.3	8.8.8.8
Jun 30, 2022 20:51:29.973680973 CEST	53	57723	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 30, 2022 20:51:29.954133034 CEST	192.168.2.3	8.8.8.8	0xbb70	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 30, 2022 20:51:29.973680973 CEST	8.8.8.8	192.168.2.3	0xbb70	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 30, 2022 20:51:29.973680973 CEST	8.8.8.8	192.168.2.3	0xbb70	No error (0)	ipv4.imgur.map.fastly.net		151.101.12.193	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- i.imgur.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49730	151.101.12.193	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 18:51:30 UTC	0	OUT	GET /NQUpBi2.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: i.imgur.com Connection: Keep-Alive

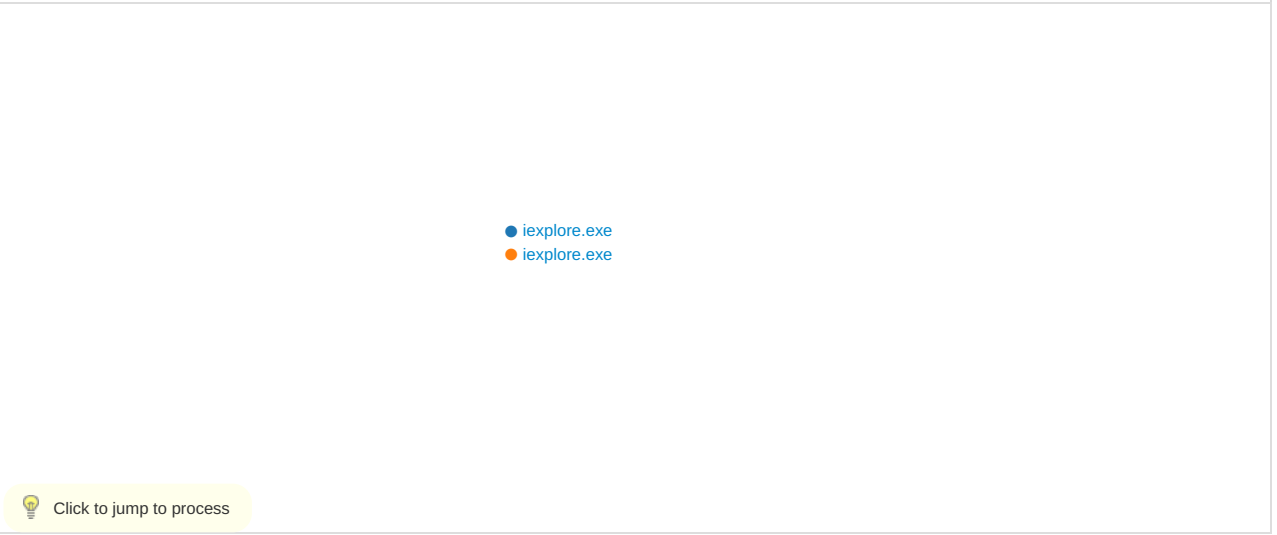
Timestamp	kBytes transferred	Direction	Data
2022-06-30 18:51:30 UTC	0	IN	HTTP/1.1 200 OK Connection: close Content-Length: 120 Last-Modified: Thu, 23 Jun 2022 07:34:36 GMT ETag: "e7004a24d6e606cf714b8b06067fc8b2" Content-Type: image/png cache-control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 30 Jun 2022 18:51:30 GMT Age: 645414 X-Served-By: cache-iad-kiad7000049-IAD, cache-fra19180-FRA X-Cache: HIT, HIT X-Cache-Hits: 1, 1 X-Timer: S1656615090.389343,VS0,VE1 Strict-Transport-Security: max-age=300 Access-Control-Allow-Methods: GET, OPTIONS Access-Control-Allow-Origin: * Server: cat factory 1.0 X-Content-Type-Options: nosniff
2022-06-30 18:51:30 UTC	1	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f f3 ff 61 00 00 00 3f 49 44 41 54 38 8d 63 60 18 05 83 04 fc ff ff 5f 00 97 38 1e 39 05 18 e3 c2 ff ff ff df c3 05 50 35 bf 87 62 01 74 cd 50 f1 f3 2c 50 31 46 1c 8e c3 25 0e 93 63 a4 c4 0b 58 c5 47 c1 40 00 00 c1 2f 3c 1e b7 5b 69 d4 00 00 00 00 49 45 4e 44 ae 42 60 82 Data Ascii: PNGIHDRa?IDAT8c`_89P5btP,P1F%cXG@/<[iIENDB`

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49731	151.101.12.193	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-30 18:51:30 UTC	0	OUT	GET /Jm3Kimw.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: i.imgur.com Connection: Keep-Alive
2022-06-30 18:51:30 UTC	1	IN	HTTP/1.1 200 OK Connection: close Content-Length: 1586 Last-Modified: Thu, 23 Jun 2022 07:35:17 GMT ETag: "3debdf39c16c7ec7446d2cb9864b24b9" Content-Type: image/png cache-control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 30 Jun 2022 18:51:30 GMT Age: 645373 X-Served-By: cache-iad-kiad7000070-IAD, cache-fra19156-FRA X-Cache: HIT, HIT X-Cache-Hits: 1, 1 X-Timer: S1656615090.403166,VS0,VE2 Strict-Transport-Security: max-age=300 Access-Control-Allow-Methods: GET, OPTIONS Access-Control-Allow-Origin: * Server: cat factory 1.0 X-Content-Type-Options: nosniff
2022-06-30 18:51:30 UTC	1	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 6c 00 00 00 18 08 06 00 00 00 1f d5 18 1a 00 00 05 f9 49 44 41 54 68 81 ed 5a 4d 52 23 47 16 fe de 4b b1 46 f4 05 90 c7 07 70 f9 04 5d de d8 de a1 d9 3b 02 f5 09 28 aa a4 ed 00 6b a9 aa 8b 13 20 22 bc 6f b1 1b af 2c 4e 30 ea 03 38 5a ba 40 23 bc 56 bd cf 0b 32 35 85 1a 19 31 31 04 74 84 be 08 05 95 59 2f 5f 3d f2 ab f7 97 92 fc d9 fe 07 b1 01 48 de ec 5e 7d 7a f3 af df f0 59 04 7b 9b ac 39 fb 11 b2 89 dc 16 9b 43 5f da 80 2d 9e 86 2d 61 5f 19 1a 2f 6d c0 16 ff 45 92 24 2d e7 dc 5b 00 cd aa aa 2e cb b2 9c af ca bc 18 61 69 9a 9e 84 6b e7 dc 55 bf df 9f ac 93 ed 76 bb b1 99 bd f5 c3 59 51 14 c3 a0 43 44 22 55 3d fb bb f5 5f 03 d2 34 4d 44 e4 7d 18 37 1a 8d 8f 00 c6 ab 72 2f 46 98 88 9c 86 eb aa aa be Data Ascii: PNGIHDRIIDAThZMR#GKFp];(k "o,N08Z@#V2511tY/_=H^}zY{9C_--a_/mE$-[.aikUvYQCD"U=_4MD}7r/F
2022-06-30 18:51:30 UTC	3	IN	Data Raw: 37 e9 51 8f 33 b3 36 c9 6b 9f 97 92 b0 d6 87 bb ab aa aa 92 9a 78 0c 60 58 d3 0f 92 ef 42 08 57 d5 36 c9 8f 0f d8 01 00 e7 f5 6a 70 1d 54 35 e4 f5 a6 aa 8e 48 26 2f e6 61 24 cf 1e 9a 17 91 4e a8 c4 ea f3 be 27 02 7c d8 ab eb 50 d5 a5 27 e6 79 3e f2 27 08 1d 5f ad cd 49 4e cd 6c b4 4e 4f 80 df ec 38 cb b2 b6 2f 1c 22 00 13 e7 dc a8 fe 6d c0 62 b1 98 a8 ea 3b dc b5 1d 11 80 89 99 dd ab 4c bd 7c e4 c3 69 6b 9d 2e 8f 21 c9 f1 aa 4d fe 64 e6 07 92 21 32 4c 04 bf de 6c da 06 df e0 97 bd 37 fc 37 3e 6f 5a 01 ca 4f db 9f 08 fc bf f1 aa 42 e2 16 8f 63 4b d8 57 86 2d 61 5b 6c f1 9c f8 0b c4 42 3c 72 4d 9a 36 f7 00 00 00 00 49 45 4e 44 ae 42 60 82 Data Ascii: 7Q36kx`XBW6jpT5H&/a$N'|P'y>'_INlNO8/"mb;L|ik.!Md!2Ll77>oZOBcKW-a[lB<rM6IENDB`

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6284, Parent PID: 1816

General

Target ID:	0
Start time:	20:51:25
Start date:	30/06/2022
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\user\Desktop\IP VM_8976544568.xhtml
Imagebase:	0x7ff7266f0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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: **6352**, Parent PID: **6284**

General

Target ID:	1
Start time:	20:51:27
Start date:	30/06/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6284 CREDAT:17410 /prefetch:2
Imagebase:	0x300000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

No disassembly