ID: 438535
Cookbook: browseurl.jbs
Time: 18:11:14
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

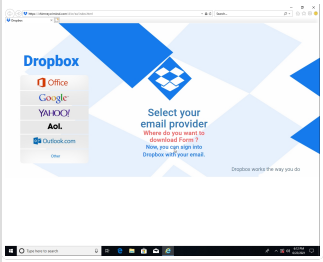
Windows Analysis Report https://chimneycriminal.com/…

Overview

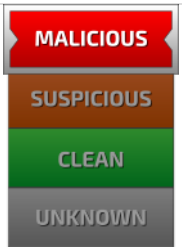
General Information

Sample URL:	http://https://chimneycriminal.com/d/er/ea/index.html
Analysis ID:	438535
Infos:	

Most interesting Screenshot:



Detection



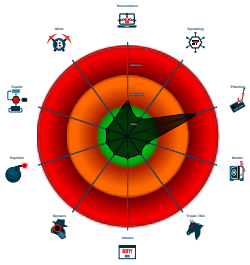
HTMLPhisher

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

Signatures

- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 6480 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6544 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6480 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

Phishing:

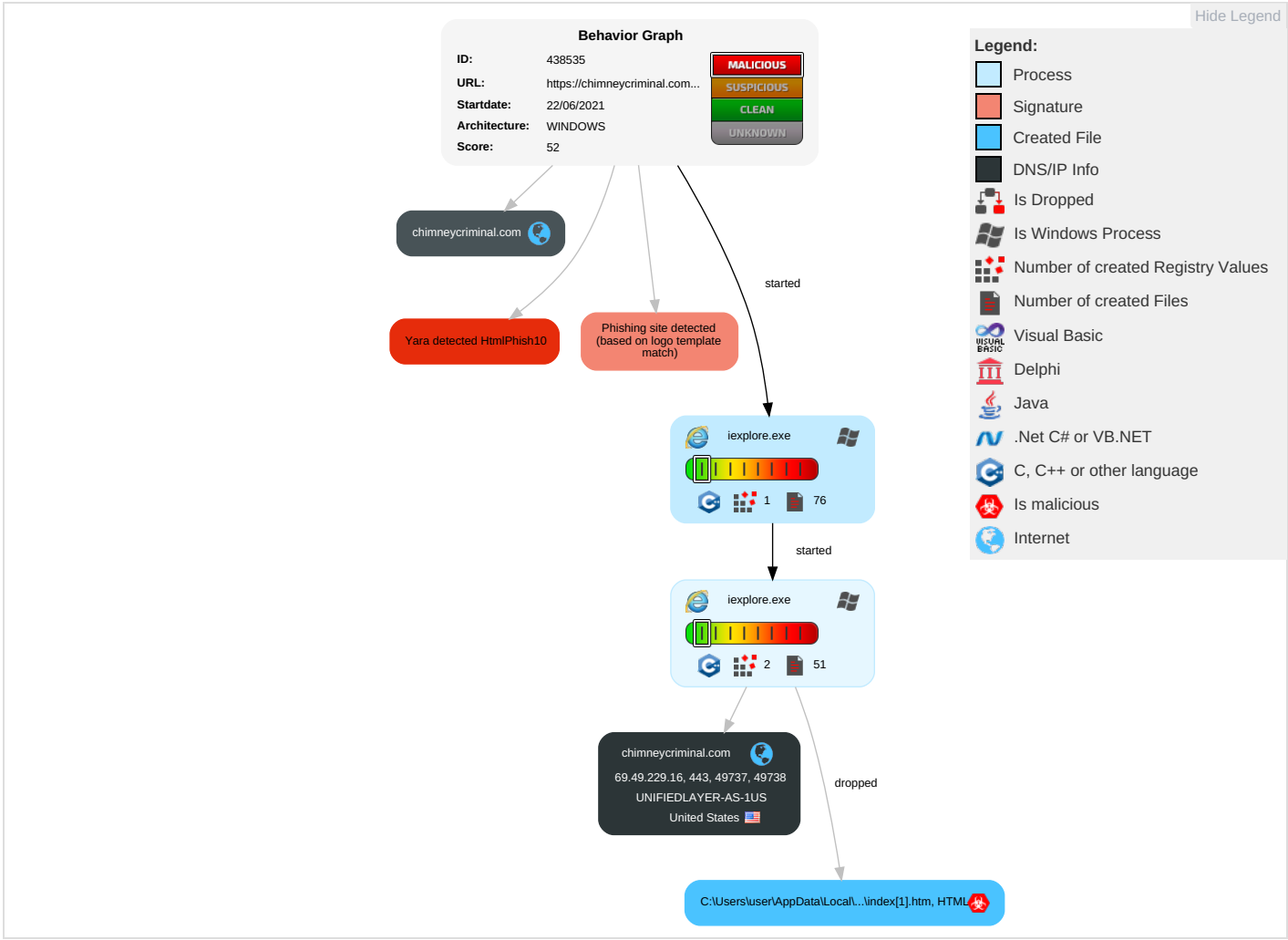
Yara detected HtmlPhish10

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	Impac
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	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
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	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
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	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

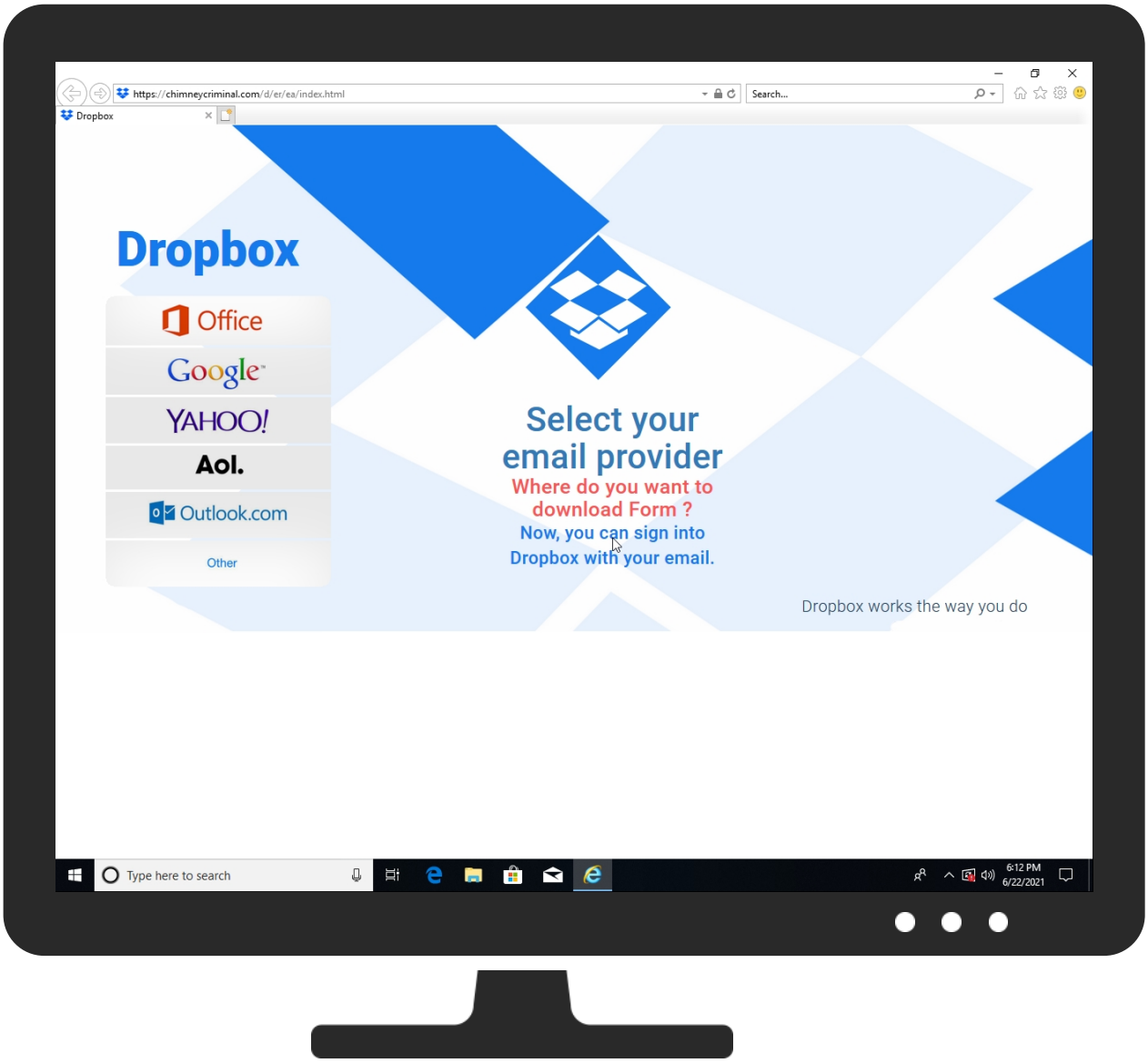
Behavior Graph



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

Source	Detection	Scanner	Label	Link
http://https://chimneycriminal.com/d/er/ea/index.html	0%	Avira URL Cloud	safe	

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	
http://https://chimneycriminal.com/d/er/ea/img/favicon.ico	0%	Avira URL Cloud	safe	
http://https://chimneycriminal.com/d/er/ea/index.htmlRoot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chimneycriminal.com	69.49.229.16	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://chimneycriminal.com/d/er/ea/index.html	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.49.229.16	chimneycriminal.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438535
Start date:	22.06.2021
Start time:	18:11:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://chimneycriminal.com/d/er/ea/index.html
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:	18
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 • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.phis.win@3/32@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI
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.{918DCD48-D374-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8490948885024991
Encrypted:	false
SSDEEP:	192:rnZIZm2vWht1ifQ5vxzMrpBkujDdsfOvcjX:rZIdeTaQIfkgw7
MD5:	1799B772F07E26E7A0A896A7D73F8654
SHA1:	8589BC37D0794F83847BE1C65AA019DD5D4C86FA
SHA-256:	29FF410939D5198B61A500831D4D532CBC4230ABDBC2398CA84B8BF4FFF6E571
SHA-512:	E24B7A9552BDEF2BB5B08A06A33C2FB4C4433290A66665B2C3050D391FB3706403963415CB0EB15B20044C1E466AEA8FDE51853733BFB176AF68D6704533EC98
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\{918DCD4A-D374-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24204
Entropy (8bit):	1.6348818389198676
Encrypted:	false
SSDEEP:	48:IwFGcprIGwpaEG4pQcGrapbSNGQpB2GHHpczTGUp8tGzYpmZLGopZ7pKHG+Xpm:rbZQQ06aBS3j12NWTMfvwg
MD5:	54E80617A53CBF9280256B3D56632F69
SHA1:	D1F6F8340D4BE63AE926CF9099861603AB5A196B
SHA-256:	09A9873F622D1934F3BBB4957BCC4E091B3D6A3635E18150C8839DF133A11FDD
SHA-512:	3D027E0971161C771E387E890DFFAC5953452A600B5B339DDE05B5CA88C71121F891D05A82BC969AA52C2A78F8EC1C76D53C59F1047055D2E112D35B4DB1574
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\{918DCD4B-D374-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565130010459196
Encrypted:	false
SSDEEP:	48:Iwx0GcprffGwpap0G4pQDmGrapbS9GQpKnG7HpRrTGIpG:r2ZRQq6MBSHAGTBA
MD5:	510A8F4AF47B7C85EA6433CAB71B4B25
SHA1:	F3B15EECD3A8A085FA2F90EB68D1AEE9F36156A2
SHA-256:	5984D6F5B47B7BD1BA2EE9CECD9819480522757997909 15EAF341BFFA2ADB60B
SHA-512:	2620ED407B317E46AB7D0C5EE16E9D1E31971990538D33710BF1A13CA8F8A43E2A6CA16AEE70FCC3A34D2750BBE64EEACB337D89015ACD6F650BCD5AFC6EA101
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):	5.102765894094325
Encrypted:	false
SSDEEP:	12:TMHdNMNxOELkUokUanWimI002EtM3MHdNMNxOELkUokUanWimI00OYGVbkEtMb:2d6NxOs2ESZHKd6NxOs2ESZ7YLb
MD5:	CB7B8DAA9E3A2C11C8FC1BEC18554BCC
SHA1:	FA33A63F486F5BF61F5CFA551AC8714B7DF9D680
SHA-256:	286E9E0266B3C26E0F8D09FA0EDCEA6B229EC5DE1653CA3A608885D9A2F327C1
SHA-512:	8523B511E6987A76F962263CE867196D3A904DD992D106DA457C4D5CF2689EC2083E5C6D0E396185B639C1BEBB23DE799D8B1E922025274FFE3812E1176EF41F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x6860d4d5,0x01d76781</date><accdate>0x6860d4d5,0x01d76781</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>0x6860d4d5,0x01d76781</date><accdate>0x6860d4d5,0x01d76781</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):	5.102337805208247
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SSDEEP:	12:TMHdNMNxe2kPUqUanWimI002EtM3MHdNMNxe2kPUqUanWimI00OYGkak6EtMb:2d6Nxr2SZHKd6Nxr2SZ7Yza7b
MD5:	466114D23CD944C11F953C285A821512
SHA1:	99E80F2708AA49C572AC9B45E55A8895F6D97B17
SHA-256:	084308ADE28DAEBBC679CE795D74AC8142E786A9078C199C62CB23AFF3C82CEC
SHA-512:	39C03DB1D6C9A1B243C3686814D4976E7291E48E3D73EB00967ACF050CC880B9A8DF1E6FA16266CF715CB1556FE1DA731DD942ABCD7A3B9BAA0FDF75B8866F9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x681bb0ba,0x01d76781</date><accdate>0x681bb0ba,0x01d76781</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>0x681bb0ba,0x01d76781</date><accdate>0x681bb0ba,0x01d76781</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):	5.1205417230873875
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLLkUokUanWimI002EtM3MHdNMNxvLLkUokUanWimI00OYGmZEtMb:2d6NxvP2ESZHKd6NxvP2ESZ7Yjb
MD5:	F6BCDBA75A06C131B314CE921AD9B3C2
SHA1:	B5917CD26D3C0F066E90F7FE1483008BB7D3760A
SHA-256:	61DAE02817D092236FEAE9729FD7F8E496395D93C7653D042EB7C0CB669399AE
SHA-512:	C57B2823196D6224F7942637538E8481C901951833A64E7EE18A11BF4B3FE762B24830516DF9884F2440F054EA8AD8777DBE3C7CCBF4F93F32505E17AAC6BB2F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x6860d4d5,0x01d76781</date><accdate>0x6860d4d5,0x01d76781</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>0x6860d4d5,0x01d76781</date><accdate>0x6860d4d5,0x01d76781</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):	5.115041143500923
Encrypted:	false
SSDEEP:	12:TMHdNMNxiTBlUGBlUanWimI002EtM3MHdNMNxiTBlUGBlUanWimI00OYGd5EtMb:2d6Nxk5tSZHKd6Nxk5tSZ7YEjb
MD5:	94957F1353B17562E8318A2074E36EF3
SHA1:	91921A44E1F367BE1DAE49E46E734FFED455FBF0
SHA-256:	78E32AA4DC63E9AE769782AE80ADE6295F9A5AB0306D8BC6FAA4B801B856B1A2
SHA-512:	59F217B3C9C79592CD1765E8FC61EFBA1E91C9FCA257D47902095E27907B0DC2496FC302D9729DFBFE876DC31B01CA940CB799138B0A9399C5C96AAC8401F0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x6841d64c,0x01d76781</date><accdate>0x6841d64c,0x01d76781</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>0x6841d64c,0x01d76781</date><accdate>0x6841d64c,0x01d76781</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):	5.137067347258585
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwLkUokUanWimI002EtM3MHdNMNxhGwLkUokUanWimI00OYG8K075Es:2d6NxQo2ESZHKd6NxQo2ESZ7YrKajb
MD5:	C5D8CB6EF61EE92BC53E72450BEB0505
SHA1:	DF270864EB3B53B9A7BCED0E188E69158D5A6145
SHA-256:	8874FFBB811A070F3D7CA7E7A0DC98D4CC2CB9666AEBF356BE5C4071BA9B71FF

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
SHA-512:	7E4CCEB4EC15B88E30109CB46478A9CABFA94C0ED1F72B428F3A6D85EBBD785D05C545F5575DE65A97C07708AEC9B58745A105358BA17EB1E0D6BCC6B3774E3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x6860d4d5,0x01d76781</date><accdate>0x6860d4d5,0x01d76781</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>0x6860d4d5,0x01d76781</date><accdate>0x6860d4d5,0x01d76781</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):	5.101882466910516
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nLkUokUanWimI002EtM3MHdNMNx0nLkUokUanWimI00OYGxEtMb:2d6Nx0L2ESZHKd6Nx0L2ESZ7Ygb
MD5:	907943E1CB436EF6931FEB106E82AD7D
SHA1:	E6E5081CADAFDE0F5A97029458993A4685986F26
SHA-256:	B69F311DBE6DE330912CAED144B0ED484C2A2C25EAC8383A6DEBCEBB3875E25C
SHA-512:	5EDA56FAC3D57E221842B3357941A3CC71734EC46F0EEBCEBE31A888AC8B091F8526ECFF6821D0F8D2A75DFE0ED479156DF066EB481367795A3CE7B39AFC2CD3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x6860d4d5,0x01d76781</date><accdate>0x6860d4d5,0x01d76781</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>0x6860d4d5,0x01d76781</date><accdate>0x6860d4d5,0x01d76781</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.1391368893868075
Encrypted:	false
SSDEEP:	12:TMHdNMNxxTBlUGBlUanWimI002EtM3MHdNMNxxTBlUGBlUanWimI00OYG6Kq5Ety:2d6Nx55tSZHKd6Nx55tSZ7Yhb
MD5:	CB30585B658768836FA7A5986A54A35A
SHA1:	9E7DFD577AE4D759C5623E0E5C9F1DAB428F1D59
SHA-256:	7F62B1902276AF56C681D75BE1ECDCDEA63630E1292172202526E2E2F1C44EB4
SHA-512:	909A0F9EEA179138DE2D56299882EA4622B3CD54BEFE1350FC7F6E0B0CAE85AF7750B14E27BAA8053605541E814001D616BBFCEDE016C3F17396A4C867F4CE6B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x6841d64c,0x01d76781</date><accdate>0x6841d64c,0x01d76781</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>0x6841d64c,0x01d76781</date><accdate>0x6841d64c,0x01d76781</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):	5.103998285610715
Encrypted:	false
SSDEEP:	12:TMHdNMNxc1UYUanWimI002EtM3MHdNMNxc1UYUanWimI00OYGVEtMb:2d6Nx2SZHKd6Nx2SZ7Ykb
MD5:	C42A48A5CF1B619C8D65C3DE7BDC33A1
SHA1:	454DA3092D48ACF87FA523D1375118948613DB38
SHA-256:	9C6CEE35CC8386FB53F383A46904DEF086242F1B8E76FFB72B37CEE65B9A3359
SHA-512:	BB7A12BBA3BDE165E33EF75E1E8385E137005127821E0B85A4836F5CC650C9077987EE146A3A5F210B466B27CF8F7F5B19A42A537A0FB18424E07647B02117A2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x683aaf4c,0x01d76781</date><accdate>0x683aaf4c,0x01d76781</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>0x683aaf4c,0x01d76781</date><accdate>0x683aaf4c,0x01d76781</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):	5.092938598648833
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn1UYUanWimI002EtM3MHdNMNxfn1UGBlUanWimI00OYGe5EtMb:2d6NxjSZHKd6NxTtSZ7YLjb
MD5:	291C4B7CD1CD4441933A54BD8751B799
SHA1:	9421E7D1CDEDC6FF06A32BEE25959B6CDB836E53
SHA-256:	D48F16BC3D2851E927B83B79C9B679E137B437646DA363E7861AF141E8A97B94
SHA-512:	9F4336CEF79D341CF4D5F320B94F9070ACC19962B50BE81C513C8312241DF0B66354709C735AC9AE2A80FF2D24AC42363E0F8DF671AFAF52875E577D49B7AEB
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x683aaf4c,0x01d76781</date><accdate>0x683aaf4c,0x01d76781</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>0x683aaf4c,0x01d76781</date><accdate>0x6841d64c,0x01d76781</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	527
Entropy (8bit):	6.751646743816944
Encrypted:	false
SSDEEP:	12:oU9pqLbpllUv/7iE2PNJG5VNe/ImCvF2L3rscIDgon+t:oUeL/xNJGNeAmBLbscIDlq
MD5:	817B26CE7C3220D8EBD0BFE40BA63034
SHA1:	E8E0B8AFF4A19267167FB1FEB0C4422776083837
SHA-256:	3192191338FA08DA75D5AE1CA1C8B03FD7EB5C491197D5387017B0C12D2496DF
SHA-512:	8269B1283493B9FF9AA582E67AE9D688DD2535B3B124D65ECB30215EBD19B9BB4D4C4B8C4AD0187A8C651FBC10ACDACCC27B63C9FEC4534CD8C27120AC61AE42
Malicious:	false
Reputation:	low
Preview:	3.h.t.t.p.s.:./.c.h.i.m.n.e.y.c.r.i.m.i.n.a.l...c.o.m./.d./.e.r./.e.a./.i.m.g./.f.a.v.i.c.o.n...i.c.o.....PNG.....IHDR... ... .szz....JIDATx...1N.Q..a#.;b.....hB...(....0..A;++u....-Ha.,.....!/w..&..bf.)&..ck3?.I...>.+...%....%...,...>.M..%.BK....1.Q.....)}.1a...].Q.....8.~.,._d.nV`.qL...z..ze....{..VM.....RRS..... ..cm..Ag4.Th.s...>.gJ.0X.....&.+.cu..h..c..U.....|...*{.~.p@.9f..Jo...<.CzW..>....z_;yga.m....WL..k>..U.?.....9m...+.p._g.+....IEND.B`. ... .`.....`....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\av022[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 163 x 50, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3450
Entropy (8bit):	7.911896239126936
Encrypted:	false
SSDEEP:	96:FGUTqNQMLoyyRKk7nvZJD/M+RCed8CSsnPdUKSS:TT/r7oexGJKdvSS
MD5:	E0251477F7131E1A46D0D8F4B19CE31D
SHA1:	F50354A61BD5A18E9FC273E58C586D63227A344D
SHA-256:	590F45556412336488FF1DB500B4E34104F30E7161E494992E4D0493A3D06DC6
SHA-512:	CAD1C1DF5F74AE1ADAE1883C3740F704F3B633F49D4342E28AB58BD67308B6ACB39B0282F4F977D60205B48862C665319E3619679CD8D57DC80A992BB18E1D6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/av022.png
Preview:	.PNG.....IHDR.....2.....0Vkf....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^...TU....R.W...MP.&..).I...IT...H.....Z..H.(U.wc...R,....7.....8.$..}.....w..d./.%+...@\..`Y..P.X0Z D.....3g.....3).....?K.!.G.x..MY.j..n.Z..-*....7.xC...('O.....>.H.o/[.I.....|..|Z.|.....O?I.-e...r..1./..)SF.....O.Y.f2o.<....oVi..R.JI.I...._....,XP.*R...J.*.x.....y.<...|..'./.9.....yj..y.<.W..}g...HL..f..od.}R.re....O.....8y..We.a.a.-[&W.\....@.K@.x..e.q.....%K..y..)..._..[.n.....8..s....?.X./.>(.....y/..2|...O.)^..^...g...`....J.1.}5b...F|+....r...".%.,Z.Hv..-.3...v..QV.X..-.....5*h.M..`.....W..7.....z,..4.H(..x...l.j....{....4.y...#..\g.I.e.)C..1c.\.pAz..!G.....7*...]*g..j.o...9n...e....E.o_.....6}..{.c<)o.|.O3..9R}.C...9.\..?^.....}...>.....*U...CC.....E.I."....6m*/...../...JOc....k...v.0.'O.b..K.d....L.4w.\a....h.n..M.)C..!oS.@.I.,.#..J..C.^..(..Oc.7...._.lz.N.Z5.M..7.4h....g.1.kW_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\av041[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 90 x 41, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1518
Entropy (8bit):	7.821266831682672
Encrypted:	false
SSDEEP:	24:HbYTr0bNc/0Wd0Qha9fEMBB3g2FsG2ftiifWgJgNg/7/wqoX2lSggc:Hqn70Q2F/2ftBfnJgiTuGFgc
MD5:	A93122D1F34261B94E07C3F1E7EF3F74
SHA1:	B2EED67DACFD8A4593C41738143EBF108583EE88
SHA-256:	B66A50616923E92B5B89FA4F2CA2F9A0281F5A27845885CF21DD397A0C1ABB07
SHA-512:	7D5FB6484B42B28B9BDFA262931A92CADF6459C59813C4C5A3FEEAA6E42ED9D0C53D343B6AEBADACEDF7F8D2AEC733B0EB683255D6A6326040823826536865 18
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/av041.png
Preview:	.PNG.....IHDR...Z...).....>m....sRGB.....gAMA.....a.....pHYs.....+.....IDAThC.[.OUW...,?...#.I..Ql.>L...0Bu.$B]4...B....&.F....n...s.6...AS...H.....l.....r9g.{.{O....w.....f .3...J$.....Bb.E .:O...'.Sq..w/.....6....P..]y:N83....v....=....7..).....t....~^.5...T...N...J.EEE..?#..%uLOMi.Y[]....#.`.(.....0.e.{ozz...;7#..E.....Bv...h.<6:..q..Q.....4.....(.....l..g## .9V.....Yu.n..n U.4...R.>#.....h.....G3.....V{...n.....,..=h...6:.v~..t..t...Q..%%.3!...ED.[...Z...d....14....BKh.....=....7..3.....,D....s.P@..8.-.h.3..<l.....U>..!.](...=.....SeU..L.0. {..c..s.`...B....\Tz..F5sQ.....jlj"|.j.....Z....+.....1..Sd.;.....3...3I.|:.~.....k1...EX...A?...4.x.p.....~...^....E.G..o.....k.F./.....N5..D'..\].....1..q..tM.o9 ...EX.s..-../2b.H.4.Z.. .....ns..;..k. u.D.YJl.....Y].....NU.....+..C.X.DG\k.@..KKKN.;..O...s^W..._0.....).a.....P...ml.../...E.;.[.....$..`C.....f..&....GQ.F)..o...Tc.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\av051[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 117 x 71, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2474
Entropy (8bit):	7.907961527557144
Encrypted:	false
SSDEEP:	48:N9Vi2jJTFGRWqD40OAmXZ4CxlrnaFKgw9K6yg7VbK4AGqN:N9VHNxGtUpJ4WWFKNhyg7VbKGm
MD5:	70FC0022C1F83253D04B7694EA34D4D5
SHA1:	53F9321D829A39C4C512B53946AA84288A2DDF9A
SHA-256:	A15B29FE61CDF379483582FE360B12868747042FA87BB40B0E9AF42CCFD548EE
SHA-512:	1E9543A375C7E9763CE6B6784417EF4226EC76AE1BCFD26117ADF1C317B34EB706A48E306ED43CFBD29B73720435BAD04CA69215F25993AB352A7AFB45EF98A F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/av051.png
Preview:	.PNG.....IHDR...u...G.....9.....sRGB.....gAMA.....a.....pHYs.....+.....?IDATx^.\]h.W.>.&5..$.A.....%.*(...iQ.R.P.m..Y..P.....b ....p.....H@.".,$...64.....]3.L&..... .s..w..-.D."e..".VFX f.....U3._..>...:iqiAi.>.....B&..+4`..kP...e...A.....R.X..o.*/...z..mS.={...[=.x.....utt.....g....k...;^.:k.x..].q.).....W...M....n.U....&..../<..<yB0.z&8,..{.n.....v.....[.B. .,..O=...vS.J...P[[.!..3=....B'N..C....s..5:..<=~.x}..t....K.....9C.....T...:"JU..s....?..#.d.m...J..DK.-*.....e...T*E.r.....1.....+GMe.tvv.c1....499)... ....x....|SSS.m.63..{.w..=....H.7o ...V.|..|hl.mZZZ.....1.x.....0..`.....b1ZXX.2www;l...*2..s...J...G.}.D...;.j..C..x.i$... ....R7...8...t.#.C..m.Fn..1^.7o.Y.r\.rE.%...h...0..y.....I..t.T....g_.y.[;..E.R..D....=..An..... .P8..#G..K..'*eBv....`2.W.^..b,..c./.ap.....k.?~...,....X.....=....&....T..5C?$.[.?.i...^.....g...".....<{...$.....o...=j..{8D.P.`B..L!..4v.n.....2..V4E...^.P<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bt03[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 301 x 43, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1143
Entropy (8bit):	7.6348521365854385
Encrypted:	false
SSDEEP:	24:y03EGiQw12bCGay0TLXi04JE9u9b2gGPeKqhYvajf/2xaQTG+m:yRYkm0LuJSP6CK3MG+m
MD5:	335F05C103766C7E3B78F6FA6EC13282
SHA1:	884DE5F276D676F35501B6B5F4D7F52EACBB794F
SHA-256:	9C93E8DBBB882FD57E533F32709D0A28F94E3C7CCE2FCAF1729DDC97E61979C3
SHA-512:	88338A6211A80F8E65F2E1CE4FBD89AD4012D5840AD96274B9BE7A96E87B3369153DC5CBF80B3D6104F73BEFC429DCA9A6E9D31201360711F3CBF20FD5F0744
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/bt03.png
Preview:	.PNG.....IHDR...-...+.....-..G....gAMA.....a.....pHYs.....+.....IDATx^.1hSQ..O2. mA.Xh'...A... .B...[....\.....P...C.P.t..Bp.....S...K}M.4-}...@.K...~..s...{..l{.l.....3?. ...d.. .....m3?v+|...w_.....@.0...fo.4..8..`1I ..l.....[...;.@..N`.g,Z,.....@.....b...#. ..&.D.....E...*\8... Z...@ (..VP..Y.@..b.@..A.@.....B....s.....T.p...@.....@P.....+..v+f.m.Yx....t...3[... .n..-..!.S..~..~.J...@.B.X.... ..f+7...C.d....q;.....>....ee.oK.[.yNr.6...-..tXR...2...qf.. Z..J.]Z|eVU..K}..hn.l]...".....U.....&bA.v%.....VuX..5..-....g.....%e[.+G...J.j:wR.....gH.'.*.j. .....Q..wD+...u....'m.z...>_.mH.....R..7[..|c...l..vz....GC.g...u..y.clfF..].R.5.].....E5~=e..\.. Z9...gF.:T.....Z..-.o..-9.....0.....uld.jP....4q..%J^<..s.z1/..u...E.^.r.....-.Bw.*..Vf4.....`. .)..+.=_9....U....NK.K..9...:.@...G..(3..y.~..u%.ZS....p...B.[...KF.....6.i...\.P...^.5.....C.3x2.`.....@.....@P.....".h.....-... ...D+.p,,. .h1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bt04[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bt04[1].png	
File Type:	PNG image data, 253 x 40, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1382
Entropy (8bit):	7.7926436378984665
Encrypted:	false
SSDEEP:	24:DMGC3j4Ci7NrclxmKNQiyj1pzWZchklaAs4RmCCTTQIqy/X5JOcHCWYg:DMlz4CelclxmjDWZchklwKmCgHDXfOMT
MD5:	C4E6C031CA581448898EC705EBD8E416
SHA1:	C564575BD210D4F3EC2EC3CDB074D252C47E7A90
SHA-256:	BFC52D51178C1FB22377B03C09C8479D611E2AFECBEB5D5A34988BBBBB60D08C
SHA-512:	CACDFD73962F9FA8A167FD8CD82F019711BEA377CBCE4B47B9414A63A2A2513AF21A02E6578A75F82989DA28FC9140FA91F6D324F9C0059CD50DCBB825EB51D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/bt04.png
Preview:	.PNG.....IHDR.....(.....5..`....gAMA.....a.....pHYs.....+.....IDATx^.mhSW...i^../...4k?.....*b....R..C.t.~..+..`..&.".}..66..a...`.C.C.."8.`V.%4m.....s...u.n.6...r.....=o.XFBsK_.2....H..J.....{k`y..GK.|.....@6.C.e.<;...C..{.:..S. ...E.~@.....8.%...}...#@.+.p.K..=...(F..W,.t..(z...P..E.X....P...$....^...]...7[...E....j.}j.8s.`.k.y.....E_ .fW..81...l...k.o..8.[n..`.(.....'..-xi...U9.05S..zS-.X!.P.mV].".n..4.\|..4.me..vx.C.L.ey..o.w]n...44..n@.OF...V..'...1.X...9..&..x;eG.#..2.7..;..>..Q....Q.._..W....7..hW.:...>.a.)\|~w.pU...].&.8=2.....3...F.V.&B.8.^...Q\x.(....;.....F..&m..E....0....8.&...C..q.c.w..\.....6..../..@OK.....y...}.PU._...0tE.LI...d.....,.....)..d...N.H.4.=2._/.7...c.....&CIL.....7.d$._..2..!.F.O..".j.'@.....^.,.4..'.?....F.....xgyzC.U0./..b,i.....t.....<.....8..8w]...+v..a...'...&.:.d..k.n.?.L.....!..w.=...{...!@...Vd-~6.../...._.o...d.M..=.^.g.....Ez:i.|Cf..K.^".....E.|.6l...Fc@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	9428
Entropy (8bit):	5.153338630383334
Encrypted:	false
SSDEEP:	192:3qxzBHwqz63upcFos8tKVm+6lC49DMoQ8bY9MxIOApvMMLUsyksM7of:EVQE63gs8PHCiegY8Aplfykw
MD5:	F86F436A4AA436CFDCB0E32C53838E5E
SHA1:	AC4E19DDA01E21D20F515CAD6562803D66F1C67B
SHA-256:	6C6A10E491B5D8B6588EFED6039CF6BDE74F64B406DAB0668FFCEEF81DA2E991
SHA-512:	A8FFA41822490A3E1B5C3BDC005CA3435B8ED492B96D63E346A2C6B05291F3DF8082A9BCEE04DA3C419C55601E2AA96ECFAAA37ADA394B385C7CE942BCF13E8F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/index.html
Preview:	<html>..<head>...<title>Dropbox</title>...<link rel="icon" type="image/ico" href="img/favicon.ico" />..<style>..*{margin:0px; padding:0px; font-family:Helvetica, Arial, sans-serif;}....body {.. background-repeat:no-repeat;..}../* Full-width input fields */..input[type=email], input[type=text] , input[type=password] {.. width: 90%;.. padding: 5px 5px;.. margin: 4px 26px;.. display: inline-block;.. border: 1px solid #ccc;.. box-sizing: border-box;...font-size:16px;..}..../* Set a style for all buttons */..button {.. .background-color: transparent;...padding: 14px 20px;...margin: 8px 26px;...border: none;...cursor: pointer;...width: 90%;...height: 40px;...position: absolute;...left: -12px;...top: 74px;..}..button:hover {.. opacity: 0.8;..}..../* Center the image and position the close button */...imgcontainer {.. text-align: center;.. margin: 24px 0 12px 0;.. position: relative;..}....avatar {.. ..}..../* The Modal (background) */...modal {...display:none

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\av031[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 123 x 109, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7197
Entropy (8bit):	7.965574434300428
Encrypted:	false
SSDEEP:	192:a35Vs7DFx1NlH5EgEdN4bIZlWbZxnPs8k3t/t/t/t/t/GNiZ:4Vs/r1rH5EgEdNQIub/n0
MD5:	517EE6558D4BFC71E59837D3DD13F64E
SHA1:	7B339DBAAD1D1349B153647217C10E80CC017D76
SHA-256:	137AA9734D8C02300502944ED1376D395A9F4BA97676E701ED32D07DBBF28BE6
SHA-512:	0A39251D27CAFC70028C1D5AE455F98DAC4ADD955F35B440FE54A16A86B2D24BAF90E102F60E2F63F0B04169D7BB32B25842B77B9217E42998F53A424DABB4D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/av031.png
Preview:	.PNG.....IHDR...{...m.....H.....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.].xTU.~g&....I ... ..MQ@0.]...D\.....jp]We.....@.....R.....P...Lz2...;...I2A./.=.>7..|....<*8j.....b..$y.d..@.A&..D.B....q..\|Dv.L+.=.^C..t.B."$.3.O.....!7?.....=..Z...E0.`3f...p..AK.w8.~U*..p..wREO...C..b....b.....=.N....."..1`../|1..)......H..4.n...>B..P.....8.u.zJ..M..Q..O_.{.5....OS6?Q..o.;H.0..M.([...&..s(.l.U*U... .....\7.&..q..N./.+w^.:....+...h..n...lv'..I#.....DY.....sw<..u...e..+p.k-j..`.....@..V+...=&.i..h.....`0....o..a.r.h..p..@W...n</.. ....ju*..vh|T..;.....w.v"H...Y....8.Y.....G.`..!... .x..v.../.:..A.x[/.y..z..../...DSy.B.|....C.E.S .....)N....."..5..]...=.....5w&.ium...Fd...8.x.K^..g.M.AV..T.N~.'Tg...2a..Xt....B.X,....c...1.. .1.....|$.8..n.P.....l.a..].O$.j.....qlO>...yd9.r.../.....c.=.qc..!.Yn...+C...../.=..").J.l..1I=.!:.....c.,++....z.1...H.....b.2.....p....>^z._.Z....].....C...F...f.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\av061[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 78 x 114, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9340247092335225
Encrypted:	false
SSDEEP:	96:kLG3W2yXiz+vd/3l1eGvp5BqnlP/9Sa/HjO0DHNL+xNjVFgZ:kr2lGwownzS+HD1OZVa
MD5:	3B97B73CEBF3BE8D46AEDF9553FA5486
SHA1:	B61499CF641E2540C511C01F68E7BD2C840F7712
SHA-256:	3FE2E6BEC88C9DFDA8A8A396EF687309FB6663B5DA176F5DCE730E44763E298B
SHA-512:	655C88653888CF99A2A12A1C6E22BC521EA47C68CFBF042ABC703C232044A6B1408B4ED76CF941223D082A8A03C52146C556B877766BD56DA787515B30AE8648
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/av061.png
Preview:	.PNG.....IHDR...N...r.....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.].p.U.> "bW....CU.u...l3RT`..(X..u@E,c.....G.....V 8.*.X.....v...n....}...}o_.wf.D...sO.k# .D9.F..v..uX.n.}....M.....>....S.}i.....D...l.W_}U.u.Q...s.G.W^y%..(.B...3f..-ZX.)..9..QYY.MK....z.!.Y3...^\w.u...l.....9..~.7.|..s.=%H....$@.v.....M.4....7.(.o..;.....?.!C.X\u..9 s.@y.G...k....K.....+x...a...W/...]..U.V...x.b.}{..../._..x....?...m.....Oj.Q.!.qc...h.Q.b...M.6.....G.M....k.(.....Neee.c.....O....b.B|....8{.....l...1p....=..S...l.....J.(.....e...?Gf.=.....s+.o. .....8.....@.^.p.l.o.e:(."..2../.\..4.@hs.8....9r.|R..|0.w.y.uk.-...*1..g..k..fq.w.l..rKJb....po.Ut..Er...*.,X.;D..|.l..A.c....^..V}.....RII...7.|S{..N>?..c...*.t.l....[.mh.g79.U....."E..Q. cj....B.T.d.....3DP.c'.... .{....C?...../../..d.#.....Qt..R.M.c=..t....{.9.8p..\...v....[..7)N.s'q4...Op....8m;n.....o...vX.b.(o..3T.....8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bt01[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 67 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	491
Entropy (8bit):	7.280592594167857
Encrypted:	false
SSDEEP:	12:6v/7ykF5N7Vy4KIVJ85EtBPwrN+g/7Qd+SsHQ6pYh1IH8dGgS7fR/N:sNKkEEtZ0+g/K+CyYhoWm7Z1
MD5:	3282AED98BA51D0B9F0E7C33936325B4
SHA1:	5B689D32AD29A0F9B34436BCF352EB51B493018E
SHA-256:	BC1A464CF269178D8C6E77030104427D6A443E56551A248E1BA2DD99E46C4967
SHA-512:	8B58CF3590622AA85262C5F2940D682DF6D9EBCE6E8BA9B3607495F201CF09B229BBA9604C2E0B074B990017AE375015800E154ACC9B9BED9036EDB7A94EDB6 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/bt01.png
Preview:	.PNG.....IHDR...C... .....I.....gAMA.....a.....pHYs.....(J.....IDAThC.Y[.. ..4..3x..k4^.....L.&F..(e.....k.....ZoN...`. <...S....i..3..0....2.L ..Dr.....Wb.I.....Ngb.....C.g.S..?7. _.'...../%(...r06.f....P&...K.x..Ht>\....D.;U.....&v..-...nX.....R.I$....t..`.~.;.....n....Yy`D..;...F...bF.....v7...~z.O$4....].S.'..N..8..E?.#fF.^...d..t...-3,..A.z.._.L.i.[..4....i.Lf....q...' &8e...*.....yi+.Fp.....c.-.F..K...x..K.^.$...g.=...N.v.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	387
Entropy (8bit):	7.315478699826133
Encrypted:	false
SSDEEP:	6:6v/lhPKq0iJ1IHHv7pbsyGE4G2VN5WtCLqwsNMYmmlHURuEu2tf910L3cgscIDga:6v/7iE2PNJG5VNe/ImCvF2L3rscIDgo1
MD5:	51E2DE798B41DB26B6A0EC187959D394
SHA1:	B55B0E80A4A533BE00E26D30756CB9B860AD76B1
SHA-256:	78F31552544922D7131FB218DD480A324E6EA9E9FA5E3134F446850B3238B103
SHA-512:	8702CCED8C0493B2546AB27B14836CA52C32A6FB6B0786CB22F7AC0D49374F026D233A11FA56B94E3DDE31E5D6E9D0599C764B52811ADCD5CF3228694392780
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/favicon.ico
Preview:	.PNG.....IHDR... ... .szz....JIDATx...1N.Q..a#.;b.....hB...(....0..A;++u....-Ha..,.....!/w..&..bf.)&..ck3?.I...>.+...%....%...,...>.M..%.BK....1.Q.....)}.1a...].Q.....8.~.,._ d.nV`.qL...z..ze....{..VM.....RRS..... ..cm..Ag4.Th.s...>.gJ.0X.....&.+.cu..h..c..U.....|...*{.~.p@.9f..Jo...<.CzW..>....z_;yga.m....WL..k>..U.?.....9m...+.p._g.+....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\av021[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 78 x 31, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1919
Entropy (8bit):	7.865043255831311

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\av021[1].png	
Encrypted:	false
SSDEEP:	48:Tb10R+cVmlbUOQJ5fcF80QOalO8GkAzWzGx+c:a/mlIOKeZQfYL3+c
MD5:	A2F0B50990F12B9077506CCC52223D19
SHA1:	8A91A072B821FCC239EC88791F7A3430EC6556E4
SHA-256:	24A8A365301768DDCF849160E1342D63B1FEAE4D5DACB1CB3D608C8CB6FA5994
SHA-512:	0580F64A5A4C2CAE904B43007514BA7C2292461245E018B604966DB8BB5946D68329FAEAE1494060BE92BC956CC1E5900CBE68431A3695640D2CFC9A864B468A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/av021.png
Preview:	.PNG.....IHDR...N.....Ix.O....sRGB.....gAMA.....a.....pHYs.....+.....IDAThC.Y[l.U..gv..v...B[...J..''..hAE).rQ.....KL....<.P.$FQ...P.,rM,H.H}.Bh5D*E...`.e.t....\|g.....l..E. .K&.9.....SIa.Q...y.=F;p.F.K..$.P..Q..5@M..t.3H^.:CI..J....N..R...3...l.....L..3qXF....#.....;.+.h.....6,.....[.R.o4s.t.`.....U...`_.iy.HT.....<N.....<L.'....1.....A.=.'.S.....v... ....O...Sm..3.@...T.9.HK...P....)..F(...9....F....4..k..''....)%D...@.y~.:.H...[_..}...{B}.j....,`..u.1x..>.G-.....OB.a...c.:..^.+.....{}4v.@7.[_!..>.;..o...HL....K?5....@.7,LgeT....yj...q. M_.g.n.u.kcH.7.*_...L.....^...P.y..0Lo.Y...U%..[.{.K.x{-I..RC.E.#.=.(p~!..c..6}.I...{...-..1.:..2#..x.<.X.&.O.''..M1C'.s..A...^b....5a.0q..h.#..$...0v..G.@.J.4...d.y..$O.Id....^|....;....P*. Z..e..'....._ *.i....{....1w>o....(;E.N....:.HX!?[..i.D_..+....o3...e.RDr.x.a9..jS.i...V...\v...irQ.....I.|.l%.Z..w.ox...j>[>;..Z:W.),,W.I...Y...;.....wr.$w..fc..x....C..@.....<..W....|..bu.P 1..a...[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bt02[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 90 x 37, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1066
Entropy (8bit):	7.746936094683425
Encrypted:	false
SSDEEP:	24:QeKS+ET4Bl26tq29UAWmSUFJU54IdYnn361t:QQaXlSUFJULe361t
MD5:	114CCB5EF1213328E648AE75A41321D4
SHA1:	AFE2D1EC8F00CD8C51429D15217EFE418252536F
SHA-256:	0CA9497A9E2C19628EF30C1405A682B5EEFAB5A38821D35C563642E1E79A62A0
SHA-512:	539C746F73A88C5057DC150FD8DCF960A3F883C21DE649089FC44E0891760DA719BB7FAE7C5D18C6B0DD77BDDB8E6CE29D2306E5F752DB8A542D87DA0AAE6 87
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/bt02.png
Preview:	.PNG.....IHDR...Z...%.....gAMA.....a.....pHYs.....+.....IDAThC.KlLQ....1..)%f4...''...GSDB''UB.`E''....k...XXy.TDB...x5.....j.Z.....wM.LK2.9...$....}.w....).....i.....J. c....m....H...400`.;o...2..''....%.jk..L.h{).D.''@I...zP.v.!..[.....!.&..c.m.$.....a.....!.H....d @...pJ#.....eo.....%..&+h..G..(..6~W...2..m&.4.pt..E..:...q...Us}.....1\}d:....ES.<d.s.@apx ...p..7..!.o.u...@...n...5uX...L..OL.k1p...h.s.\..,.m..I.>G....4=.....lJK.....x.hs..Y...a.....Y&.....%.K:^}.Q.b.}.....yf:.?rMO...W.qv.#.S...bh...@.G..m....6.....z,\f..5...Y(.....|. .]St+.. ...l._.g..n..%..peO.3.w.`...vCP...#.)...x.@O.W.....p...YS.B..AR=:.[..$..{Dq..wo!].M.>u[g.i..u...CI.zt.....a...O.6.O...T1c..K....Z..v.!D...Pzj\P...T...;.:...e....<?].M.....b.}...<6u.....*j.h .se.&.....>.u..a..U..X3OM.C._.:hZ.....^.ed1^U.....&.2...<g%zf:.....tZ..e>.....~2...y....''.....C..$.b...4'....E...pJ#.-@s".).P4/.$![.....y''..%..(.>~..E..E.[b,...Ms#.3.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bt06[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 67 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	491
Entropy (8bit):	7.280592594167857
Encrypted:	false
SSDEEP:	12:6v/7ykF5N7Vy4KIVJ85EtBPwrN+g/7Qd+SsHQ6pYh1lH8dGgS7fR/N:sNKkEEtZ0+g/K+CyYhoWm7Z1
MD5:	3282AED98BA51D0B9F0E7C33936325B4
SHA1:	5B689D32AD29A0F9B34436BCF352EB51B493018E
SHA-256:	BC1A464CF269178D8C6E77030104427D6A443E56551A248E1BA2DD99E46C4967
SHA-512:	8B58CF3590622AA85262C5F2940D682DF6D9EBCE6E8BA9B3607495F201CF09B229BBA9604C2E0B074B990017AE375015800E154ACC9B9BED9036EDB7A94EDB6 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/bt06.png
Preview:	.PNG.....IHDR...C... .....I.....gAMA.....a.....pHYs.....(J.....IDAThC.Y[.. ..4..3x..k4^.....L.&F..(e.....k.....ZoN...`. <...S....i..3..0....2.L ..Dr.....Wb.I.....Ngb.....C.g.S..?7. _.'...../%(...r06.f....P&...K.x..Ht>\....D.;U.....&v..-...nX.....R.I$....t..`.~.;.....n....Yy`D..;...F...bF.....v7...~z.O$4....].S.'..N..8..E?.#fF.^...d..t...-3,..A.z.._.L.i.[..4....i.Lf....q...' &8e...*.....yi+.Fp.....c.-.F..K...x..K.^.$...g.=...N.v.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\001[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1588 x 630, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	208099
Entropy (8bit):	7.812129836950512
Encrypted:	false
SSDEEP:	6144:csjwctXG0/pc5b1xhX7xIdJ464L/pRdXrOQW4N:csj/XG0/8GA6cRpZ
MD5:	C23B576DD1E0B96E2AB82334FB914788

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\001[1].png	
SHA1:	24922CF88A290EEB3E1D2A26534FC7D8B0D2A4FC
SHA-256:	5CF4F5D46E721802446659D5D6A04435C8062EBE4A92EDF2DE0F62DCC093EED5
SHA-512:	D64A15F923BC6A3F67D93CAB9772075867C043BDB1B480B17B038F7936B5DE0BF0342C18452273A616E214659BFDFC849DA34F08BCEE67BA90AA0BD0244DC17
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/001.png
Preview:	.PNG.....IHDR...4...v.....k.... cHRM..z%.....u0...`..:....o._.F....pHYs..$...$...c....8'iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNT czkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 ">. <rdf:RDF xmlns:rdf="http://www.w3.org /1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/ sType/ResourceEvent#". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2017 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2018-10-07T02:47:17+05:00</xmp:CreateDate>. <xmp:ModifyDate>2018-10-07T02:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\av011[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 264 x 113, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5170
Entropy (8bit):	7.834208354489188
Encrypted:	false
SSDEEP:	96:Y7Z8J92iag0FRe/6KDGG75aWUECgDjeCgZJjsdiM145bOn1/VO:Y7yfA1eR7vUECAj1gZpCifxO1/VO
MD5:	438C039278D5F8E502ABB4D18039FCBA
SHA1:	FCA04AFA0344E8A24312D38B3F7DD545868F0E25
SHA-256:	A609042B1CA43D30D0006C66A1417FEA56B42766FEEAEBA8B20803A43E6DFF09
SHA-512:	A29140CE57C6BD6FF36B9492DC90A58D56DB326A4FBAB4321A04FC2870EBC409067C75EC93E81EBC0375D5C6D81E06E5EBD9226A043C48B19C8518757418BA6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/av011.png
Preview:	.PNG.....IHDR.....q.....).=B....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.]=plG.n=..c...j..m....IU.D.IF..5.....v.$...Rf0.#..i..}.`.U..J..b\..I.?^.....s{.....O=Iso.s....9..^ oM.96"@..@..w... .D..... ...l.2.....7.....O.O=}..y...}....F..@Z.,M....W.._..}..{n....?..O.G....8t.....G`!.....@. .....:.....z"...N.aS.U...W.."lD..l....6.X.4....>".~.J.b.....C;..S .M$.DJ6uz.[...w...w.F." FA.....A,.B.n.....$(@.....V.. .....wdRw).....fu..O.....H.....Z..."..bS..7`..V.O,.)g9.....g..{.J.@.....zs,..d|.....W.@.O....c.....42.}w$...<.7.. . ...N0..rD.../Oe|..8.....v>..W..R]....7.^.|@..a.....U-.....huP...$.....?.....O..'?`.W...I...O.=6m..O....WW..~..)9.;. Z.+q.Uyl(jo...t..`I....&>:.6.>.t..K.U.,...N,.ww.ZE.]C.uG. .....`.....t.....ei...>....[Q.$..AC4..w_.C.....k..6k..}.(d...@. .4D..8,..>."..4.H..<..w*G.&..}.=.w.. 6...Nro.....|..`..$.WB.`....Rsl.R6...?...>4...r.....z.gD>.;..C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bt05[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 36, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	923
Entropy (8bit):	7.502613620123825
Encrypted:	false
SSDEEP:	24:HzKFD7vQF//UgYCt/bUjakSDLZeD78HC/t:SDwYVvAfC/t
MD5:	435E789B609BC7D66120D6F5BD2BA5FC
SHA1:	195F2FCDE90F797737FEA71CDC72CCB2ED23E3DB
SHA-256:	6BDD77A0448306EF0F6AEA95131560C6FC2C81AAA25158BF975C91906616A237
SHA-512:	25B6254B4CDE607A38B8EBC80B13390AE024227029E8E69108F5FC1333EDB5137B6F1FA56DE4D0B1299E0BAA11C45B2E75E972D5FC381525EA29167DA4E552D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://chimneycriminal.com/d/er/ea/img/bt05.png
Preview:	.PNG.....IHDR....,...$.....3Y.....gAMA.....a.....pHYs.....+.....=IDATx^.1K[Q..._.. B.C)T. ....B.K.....f..._p.A.-.f....]T.....C.:H.$C.Q..!.....}..r9..<.....9..>~.... .....D.@.....E"@..f.` XfB.P.@..". ..3.0,3.B(. .a.....P!.....@.....L.....`X... `...e&T....0,r.+...{.Y.f.v[.gU...z..!.....Z.m..VfaV.Q.X.S....Q....."...V.*.92. ?..2..#.a.\H,.*kj.\/R....\_&.].y...z>...B...MXR..... G.i!).....R....Q}x.L.)...im.....2KW&.Q....Q-6Vi..IeT.Zp.\..K..o./|.....E..L .....7.i.....m4G(.x.z....k~.".UZ..=..c..`Xq.n.s.9Pp.....V.9.,..wZ..6Qa..n.V|..iY.;Q.....`X.#...7...6...,.. .J.....#..-...,Di.5..6...u.....M..Z.f.Y..Km}r...=..@O.q}&.a..x,.kl.gR.....+.o....U...tt..}...S.....+9.. .7.o1q.}.$.u.!..Z.o.o..~Vx*...}.;.ec....Z... 0..". ..+.XaY..:!...a.....H<..+.) ....!.a..J!.x..V.S....C...+.B ..0.... `...e'V(.@..`X.O..@.....N.P.....xt...!.4....IEND.B`.

C:\Users\user\AppData\Local\Temp\~DF41DA1EA9355D0F2A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.474561157917097
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loG9lo29lWWlN2fH:kBqoIhnc2fH
MD5:	A989F7B1ADDB80C386049B37299E3667
SHA1:	666876EF4E36297F973AF35AF3AFAA382B89BCAC

C:\Users\user\AppData\Local\Temp\~DF41DA1EA9355D0F2A.TMP	
SHA-256:	6B80F5C7309BD5BAF11BE979A1BFFA072964E0A0C5FCCE4089EAC172E5C5A4F2
SHA-512:	199F9E0F9996699D999DFDDBAB1C116C9E565982775CF2FB567D8DA2AAA4639A3BF32526CBBDC46565BA83E8AC3E4E7D1D59260160A4AAFF2A4082035E2F4B 0
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF81E8D53A1AD6C473.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34397
Entropy (8bit):	0.3559107352954691
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw/9lw/9l2h9l2h9l/ZQ:kBqoxKAuvScS+4+UlZlZT7pt
MD5:	9581BA2B54CCC83EF17C876E29B20341
SHA1:	6083B7150DB676C3DACA940A66705305DA41B4EA
SHA-256:	8D3140ABC88A4B5A09D48289C1605199D5E61FA30A95E6107E4870AB2BA197C9
SHA-512:	211A8C2FEA2164B18159AE3D6CD8B300E91A216B63660782FA14D55ECF41CA3FEF1F8049E9B3C6CDBC6F253839ACA0486A8DE341AA63C323BBCC5C4790A8D0 61
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF999385913C23802B.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
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/22/21-18:12:46.874069	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 22, 2021 18:11:59.748761892 CEST	192.168.2.4	8.8.8.8	0xb455	Standard query (0)	chimneycriminal.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:12:16.154983044 CEST	192.168.2.4	8.8.8.8	0xf836	Standard query (0)	chimneycriminal.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:12:00.186328888 CEST	8.8.8.8	192.168.2.4	0xb455	No error (0)	chimneycriminal.com		69.49.229.16	A (IP address)	IN (0x0001)
Jun 22, 2021 18:12:16.217266083 CEST	8.8.8.8	192.168.2.4	0xf836	No error (0)	chimneycriminal.com		69.49.229.16	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 22, 2021 18:12:00.535674095 CEST	69.49.229.16	443	192.168.2.4	49738	CN=chimneycriminal.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Jun 21 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Sep 20 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 22, 2021 18:12:00.538959980 CEST	69.49.229.16	443	192.168.2.4	49737	CN=chimneycriminal.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Jun 21 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Sep 20 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 22, 2021 18:12:16.561695099 CEST	69.49.229.16	443	192.168.2.4	49754	CN=chimneycriminal.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Jun 21 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Mon Sep 20 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6480 Parent PID: 800

General

Start time:	18:11:58
Start date:	22/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7e80e0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 6544 Parent PID: 6480

General

Start time:	18:11:59
Start date:	22/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6480 CREDAT:17410 /prefetch:2
Imagebase:	0x1320000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly