ID: 412848
Cookbook: browseurl.jbs
Time: 01:20:01
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

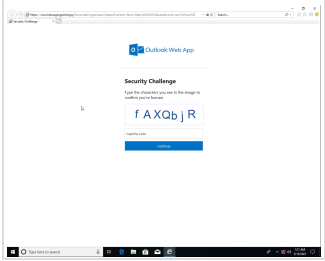
Analysis Report https://ciscomessagingportal.gq/authe…

Overview

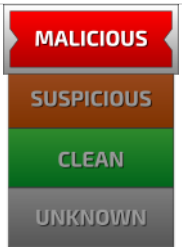
General Information

Sample URL:	http://https://ciscomessagingportal.gq/authen?error=1#owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fautodiscover.com%2fowa%2f
Analysis ID:	412848
Infos:	

Most interesting Screenshot:



Detection



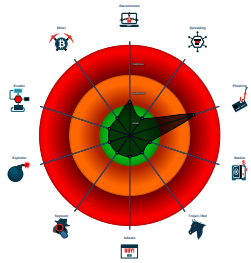
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish10

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6088 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5148 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6088 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

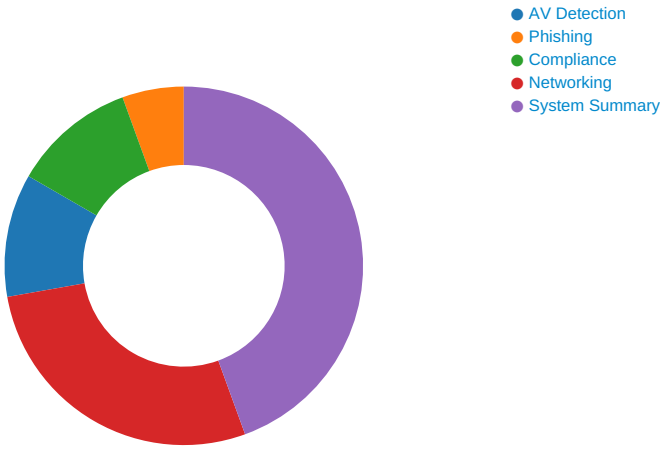
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

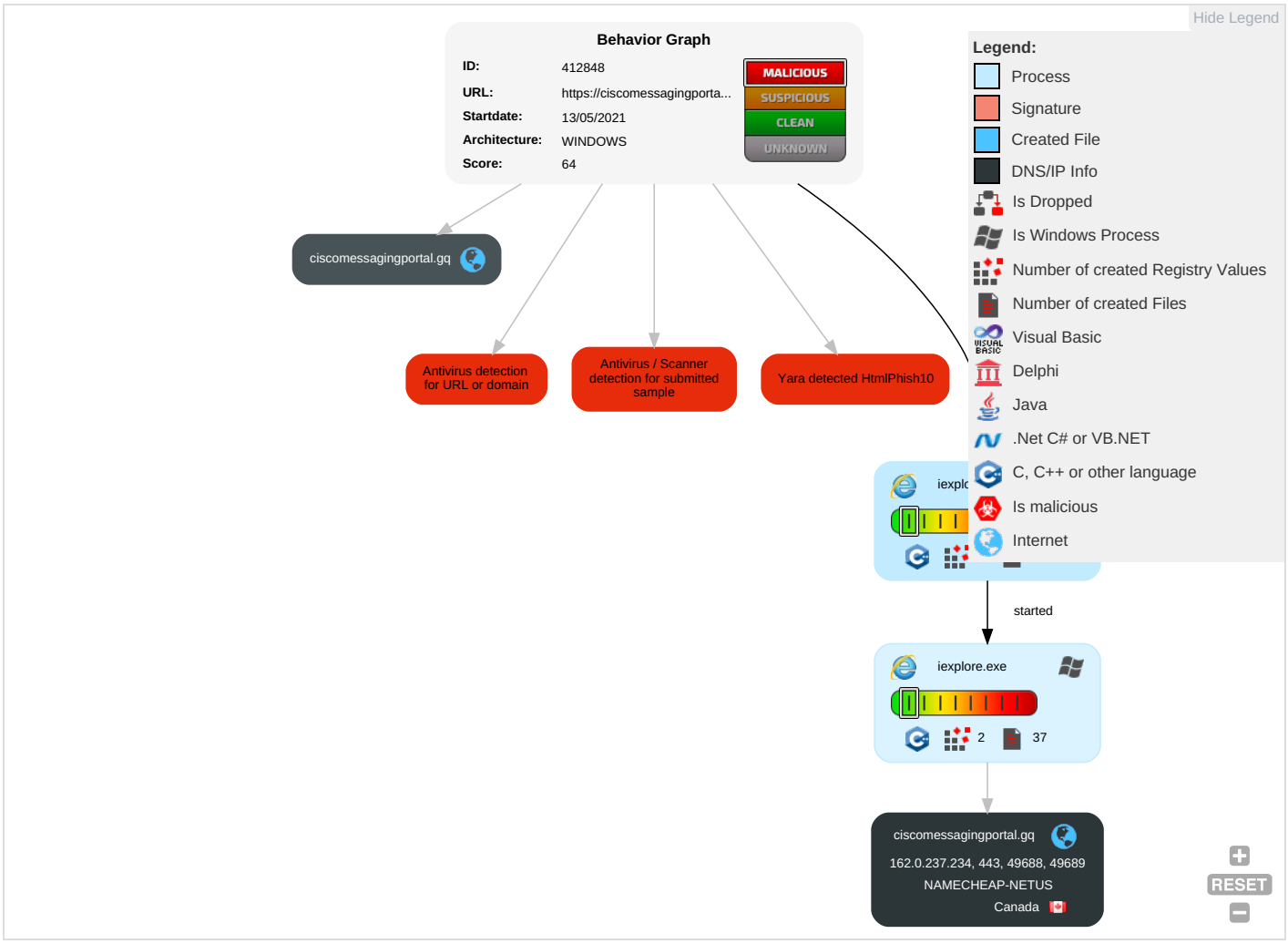
Phishing:

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	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	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

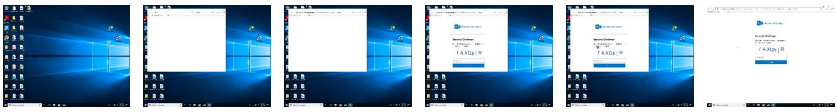
Behavior Graph

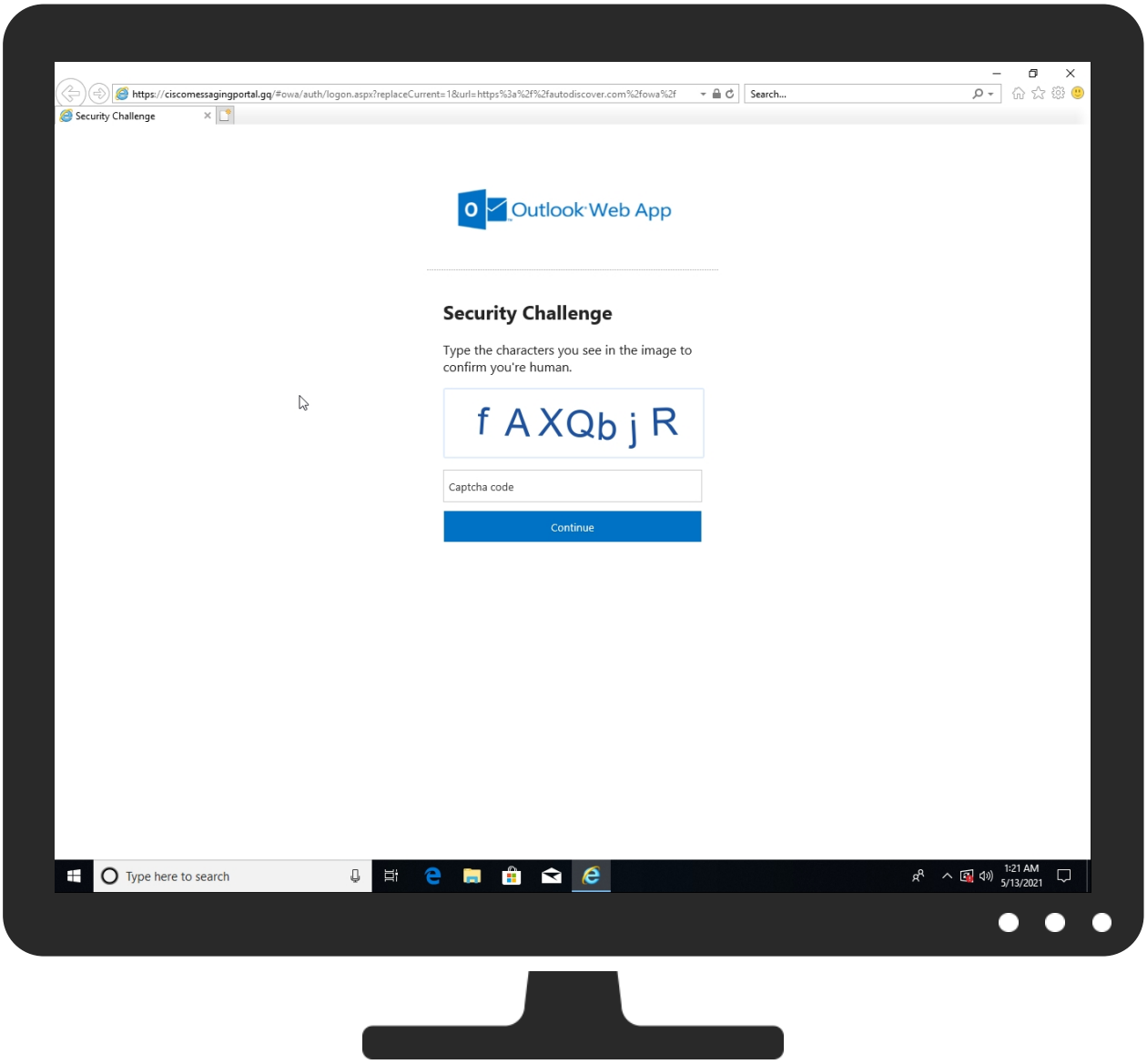


Screenshots

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://ciscomessagingportal.gq/authen?error=1#owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fautodiscover.com%2fowa%2f	0%	Avira URL Cloud	safe	
http://https://ciscomessagingportal.gq/authen?error=1#owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fautodiscover.com%2fowa%2f	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://ciscomessagingportal.gq/#owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fautodiscover.com%2fowa%2f	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://ciscomessagingportal.gq/images/favicon.ico	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://ciscomessagingportal.gq/images/favicon.ico~	0%	Avira URL Cloud	safe	
http://https://ciscomessagingportal.gq/#owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fautodiscover	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ciscomessagingportal.gq	162.0.237.234	true	false		unknown

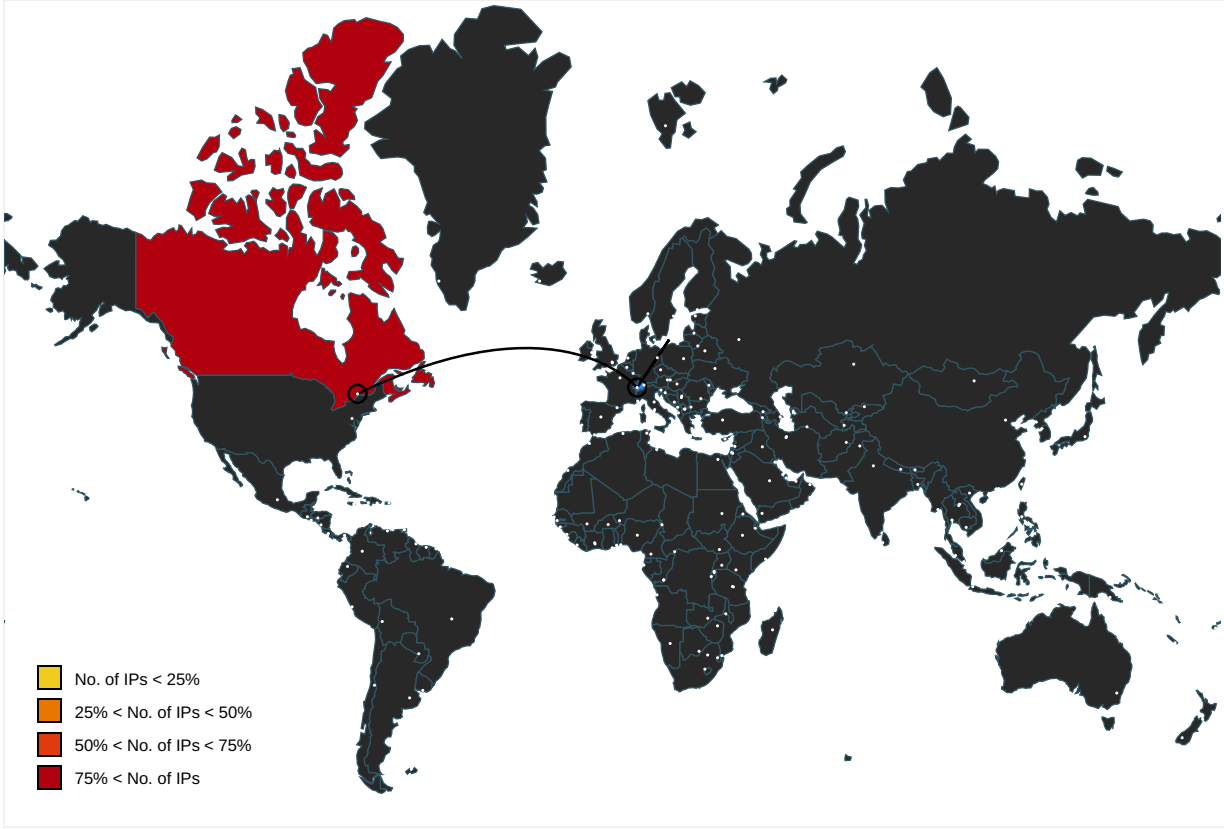
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ciscomessagingportal.gq/#owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fautodiscover.com%2fowa%2f	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ciscomessagingportal.gq/images/favicon.ico	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://https://ciscomessagingportal.gq/images/favicon.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://ciscomessagingportal.gq/#owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fautodiscover	~DFF7FAC163A929FC02.TMP.1.dr, {1E0C7D41-B3C4-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.0.237.234	ciscomessagingportal.gq	Canada		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412848
Start date:	13.05.2021
Start time:	01:20:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://ciscomessagingportal.gq/authen?error=1#owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fautodiscover.com%2fowa%2f
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:	11
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:	mal64.phis.win@3/20@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI

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.{1E0C7D3F-B3C4-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8520353872572572
Encrypted:	false
SSDEEP:	96:rkZCZn2LWyNtyQbfyT0jKMSbqnBQQtxfQSb0i6X:rkZCZn2LWIt1fIRMNSQfd8X
MD5:	FBF4C309903ECA841BF6E3975D408A0A
SHA1:	AF70D28FCE6851BB84109D69C69F8E6E95D03E77
SHA-256:	74F548A56041BAB810AA2D5BF969F15CFE00F5BA16EBF0B7122C69AABA07CD2C
SHA-512:	FC5D85EE162708BB7A9310FBB4269112177E71981425CA40B721FCEB0CFE9FDFC43CFC3ED6918852A3C8278F7EDF63483C316E386EBC54E901081C085A0D204
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\{1E0C7D41-B3C4-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24336
Entropy (8bit):	1.6610868435169408

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1E0C7D41-B3C4-11EB-90E5-ECF4BB570DC9}.dat	
Encrypted:	false
SSDEEP:	48:IwwGcprRGwpa5G4pQNGrapbSQGQpBiGHHpcnTGUp8wGzYpmr8GopFBkZ67CGCwpm:r0ZLQb6tBSYj52xWEMQrq6zg
MD5:	5069FA8E4FCB0A2085959DB8888B3584
SHA1:	AC9B9FBFF8A377C42F4A410FA6A29947C3A7E466
SHA-256:	25232D4065B793923886ACDA5D4000B2F5725DC2C0071EF74B785649B23FD3B6
SHA-512:	A8DB6A6097CA33F07406ED407F7FEA2D9397853FA451F3890B583C66F6FCE972E18B3016ECB9E4E34B4BCC7BE418AAADFCB9F297B32C87A3FD409736D63C636
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\{1E0C7D42-B3C4-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.564735526617303
Encrypted:	false
SSDEEP:	48:IwsGcprpGwpaTG4pQXGrapbSrGQpK9G7HpRvTGIpG:rwZDQl6rBSFAcTNA
MD5:	66C0887139DD2EF9E312A5ADE209C783
SHA1:	158DD15F8A3DB50EBAAEA2EAFB89828BA9E56FA4
SHA-256:	CAE7532B2CC5313EDEC9843440A0A6B997120FDEDEFEBD36EDF1E61FBF883E16
SHA-512:	4C85BFE50DD3C27A4999B0910826A7A7DE4C5E73DEACE659767CB278204A7EBBE6664507CFDE0E8AA2D116F7250312D3B67126B6CE0D351274F18A0E95B2692C
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):	5.073469900016691
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEOB/B8nWimI002EtM3MHdNMNxOEOB/B8nWimI00ONVbkEtMb:2d6NxO5B+SZHKd6NxO5B+SZ7Qb
MD5:	587D9A2943FA45CA627EC4B2AB07F1CB
SHA1:	A4366D903EE1FAD7B63DEE6BD04053878613FFB0
SHA-256:	ADEFB78CDCF89E92C9F75E1F0A02F2DA4DE909387E0F3E3F0F5F14EE6FEBD3C3
SHA-512:	E86E97E8EFCA9F09CFAB8EF5AA24E133AA9E3888EE6E27BE60186831DFF7F30280523DB662AC6E4BA0F08A5E3693C86F57E11CB91A65A1013DACE8832DA0F08F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xf4c8066f,0x01d747d0</date><accdate>0xf4c8066f,0x01d747d0</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>0xf4c8066f,0x01d747d0</date><accdate>0xf4c8066f,0x01d747d0</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):	5.056360238226398
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kznWimI002EtM3MHdNMNxe2kT5+8nWimI00ONkak6EtMb:2d6NxrGSZHKd6Nxrk5+8SZ72a7b
MD5:	D1DBD5AA48B1BDB3F3B7D41F2B6011A4
SHA1:	3A7F1E45B07D8B73FF4161442A5C5F8F71166200
SHA-256:	CDC3D73FD14D2A44ED6EC90C2904015E841422CCA97F52856C99E2B0339D046D

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SHA-512:	5C9DE9905F07F1FF57D46D728BA220AA54EDA4ADEC9602AE1699CBB55708E6634FB3C7B687E70B8A946D6A799888AAB9D647A354A45C7DC6B783AC7FB438EC38
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xf4c0df7c,0x01d747d0</date><accdate>0xf4c0df7c,0x01d747d0</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>0xf4c0df7c,0x01d747d0</date><accdate>0xf4c341dd,0x01d747d0</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):	5.07478628934543
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLBnWimI002EtM3MHdNMNxvLBnWimI00ONmZEtMb:2d6NxvdSZHKd6NxvdSZ7Ub
MD5:	7BBBCE30F856BC5BF2C47CFEB8C93E44
SHA1:	C558ECA02703839FE451359BF6C527078CD04674
SHA-256:	5EA1AA65E627819CF814BA0DDF4ADA9677C49B03D2968B09BACDAA5767012572
SHA-512:	DEDF603CD9958F077F251643831506F85CAA7943EF84262E9BE50203D7AFBB3C07E55291664DC6BB19AB24B679BE9F0F980479322BF243403A8CA035BFDD2F64
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xf4ca68d0,0x01d747d0</date><accdate>0xf4ca68d0,0x01d747d0</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>0xf4ca68d0,0x01d747d0</date><accdate>0xf4ca68d0,0x01d747d0</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):	5.106852042094574
Encrypted:	false
SSDEEP:	12:TMHdNMNxiZomo8nWimI002EtM3MHdNMNxiZomo8nWimI00ONd5EtMb:2d6Nx+P5SZHKd6Nx+P5SZ7njb
MD5:	E2A8A3714081CC1FA5AC4076B249BC44
SHA1:	D4A7C6887965ED1E1C887E430D16848BF647395E
SHA-256:	72F209C41181BC1A3FAE57080A9B8B839B89783787B488453742F349B064431C
SHA-512:	E04C1B6EF3102047526C85076AD49191E33665368E110B431E4222395200370D4C00A72397B1E02507A5A05676E85BC76D36B1CBB5BBCF8A37EB13BEBF478727
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xf4c5a426,0x01d747d0</date><accdate>0xf4c5a426,0x01d747d0</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>0xf4c5a426,0x01d747d0</date><accdate>0xf4c5a426,0x01d747d0</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):	5.091950347490606
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwBnWimI002EtM3MHdNMNxhGwBnWimI00ON8K075EtMb:2d6NxQESZHKd6NxQESZ7uKajb
MD5:	22B53FFAFD648424527DF54A4733DC40
SHA1:	E2B3BDC59066E2A3AFD443CE1C27E9379889062B
SHA-256:	1DA5A413C899E2B2B7A33A09F5FA3155CC9134750210ECFE3650D2CD8E482D67
SHA-512:	92460F2F2811C1EEBFF3FC5C15DF8BF92107438FFB4714593100F3671BDBC02E995FABF9A81DA7C15D8953D7B0D008DDFD6A2C8F7D933082BE4C6089F47C0B1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xf4ca68d0,0x01d747d0</date><accdate>0xf4ca68d0,0x01d747d0</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>0xf4ca68d0,0x01d747d0</date><accdate>0xf4ca68d0,0x01d747d0</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):	654
Entropy (8bit):	5.074575975501992
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nOB/B8nWimI002EtM3MHdNMNx0nOB/B8nWimI00ONxEtMb:2d6Nx0OB+SZHKd6Nx0OB+SZ7Vb
MD5:	8A8E727C7A92F0A6534A66C7740A3DBD
SHA1:	71AB469C0E8886E182311D1C4EE1A6F268DDD1C8
SHA-256:	1C5334A6AC6974CD5A8AF1A22B8509D17C427867DC593A5C149FCC13F960E00E
SHA-512:	2C7F703838611C1401145C6F7C135AF9D9A5BA96BBC28A2EEA71E205D99B2728418897F5F1CD9F0F626001A20010E0356B99BF1AC8753A93966F6A5EBE1F2CA6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xf4c8066f,0x01d747d0</date><accdate>0xf4c8066f,0x01d747d0</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>0xf4c8066f,0x01d747d0</date><accdate>0xf4c8066f,0x01d747d0</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):	5.1130448516742755
Encrypted:	false
SSDEEP:	12:TMHdNMNxxOB/B8nWimI002EtM3MHdNMNxxOB/B8nWimI00ON6Kq5EtMb:2d6NxIB+SZHKd6NxIB+SZ7ub
MD5:	972A7DF2E5254161059D908B8C767454
SHA1:	98E92F1EE82FDD55CD4FB9D9FE371B0024F4BD40
SHA-256:	980FE86A06AC575ED529732A17E4A8C27C27CEA3CE85C7A7653EF34B5371F953
SHA-512:	8F8D8561A49150A4526EBFAC148E8A18464A697AB12A245082D3381A0C02E4D5958F31DC627EB5994633ED4C740D9E73622A71C3E16231FC8A07B2B7A4B9C9AF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xf4c8066f,0x01d747d0</date><accdate>0xf4c8066f,0x01d747d0</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>0xf4c8066f,0x01d747d0</date><accdate>0xf4c8066f,0x01d747d0</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):	5.109466262635702
Encrypted:	false
SSDEEP:	12:TMHdNMNxcZomo8nWimI002EtM3MHdNMNxcZomo8nWimI00ONVEtMb:2d6NxAP5SZHKd6NxAP5SZ71b
MD5:	A9E8FBD36C868A722FC1ABDF71706002
SHA1:	5A2D7D4D18AA91FE3F966064B4CE7D87D89603BB
SHA-256:	1E70562901C0715AE7FBE7D0477C8948FE612A3969A7E0622828E84079505DBC
SHA-512:	2EEC1CC600DF0B990B01EF52A4EC1CD7BF1649D8DE040FBE563EF52C8908CC994874004A12C39B2E6AC890CCF5FBD091D76E2F64432FC281BA92B00C6652115
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf4c5a426,0x01d747d0</date><accdate>0xf4c5a426,0x01d747d0</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>0xf4c5a426,0x01d747d0</date><accdate>0xf4c5a426,0x01d747d0</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):	5.092150975574755
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnZomo8nWimI002EtM3MHdNMNxfnZomo8nWimI00ONe5EtMb:2d6NxxP5SZHKd6NxxP5SZ7Ejb
MD5:	2145B6DFC991DAA987E9643D63F2453F
SHA1:	6B8BD80E39C5ABD56BC5118B718D21147C9F95BC
SHA-256:	694E0A7F771DFB141F06F9A304E26EB19CD19AE63E0A58CE504F653F2F54B1B3
SHA-512:	1EBE411B2F1224BAC2FDB55F7C52AC2CCCED9F9C3D8EF63C4888194AAE932F80F22711CEA64E61B0BBE15E729816162338D99A82A022815492C9D1F1DF15265
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf4c5a426,0x01d747d0</date><accdate>0xf4c5a426,0x01d747d0</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>0xf4c5a426,0x01d747d0</date><accdate>0xf4c5a426,0x01d747d0</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\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	8312
Entropy (8bit):	4.219070295022647
Encrypted:	false
SSDEEP:	48:hSPLLLLLLBWj2P+W3DS4E4U4R7454y4aR+BddHCISilFgWSsjfQeiFzm22TISO3O:BjQDdNKevXCWl/a6aZPs
MD5:	481CDC9C0D6D078F8B2FE376E0F7B9AA
SHA1:	B83142869D12B9584DEE559B05C8D05D188D38B4
SHA-256:	A60D7EF83F39AAF25772CDF7B353A1C96FB00B5D81DA04BF69CB1D4CDBFC3722
SHA-512:	EBCA3943662127B905476ADF4340FAC583439CB11FAD7CB9E4B537CC06DDBC3FA551D047B199D7391DF4E9CF302FDD76B3A4D0355B86EFDB42A54A7EBD044 B7
Malicious:	false
Reputation:	low
Preview:	2.h.t.t.p.s.:././.c.i.s.c.o.m.e.s.s.a.g.i.n.g.p.o.r.t.a.l...g.q./.i.m.a.g.e.s./.f.a.v.i.c.o.n...i.c.o........... ....(... ...@..... ....(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..'.....................................(.....~......................................(.."......................... ...."..(..(..(..(..(..(..(..(..$.....}..y...y...y...y...y...y...y...y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\2134651[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 355 x 142, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9883
Entropy (8bit):	7.801042498548808
Encrypted:	false
SSDEEP:	192:6SC7FhkniL/BM4az1Xy96YbZ1Bs265JYAhpovdwyOI6+mXAAgNYWH99999999990:1CYniLJM4az1Xy96k1Bsdnzpo2Ihz79y
MD5:	9A2AE3B67B7001B6BB4BF3E1903B59F2
SHA1:	DB0A1994B15E971FCF943D731D5D1BDEE9AC7D52
SHA-256:	FF2294F85AD59D6D537BA92D2C8054C8F824736F946714688C1F51A6A6577BD3
SHA-512:	9B4C667847814F16F0294DB85E048C0A1A6C51EA0BE41D1389F9C424512F7364BEDD6E101224499C110B537423C18C9C070085E7DF80FF43B5EFBBA0BAE94AB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ciscomessagingportal.gq/2134651.png
Preview:	.PNG........IHDR...c..........oi.....pHYs.................iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <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:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmp:CreatorTool="Adobe Photoshop CC (Windows)" xmp:CreateDate="2021-01-26T01:03:01+01:00" xmp:MetadataDate="2021-01-31T00:32:58+01:00" xmp:ModifyDate="2021-01-31T00:32:58+01:00" xmpMM:InstanceID="xmp.iid:caeca533-2501-8b4b-a025-a2e004d62f2d" xmpMM:DocumentID="adobe:docid:photoshop:e03756b9-90f8-654a-8649-9e5d92c4e96a" xmpMM:OriginalDocumentID="xmp.did:ed01d8e4-1071-e546-8af0-c7fb433cafc4" dc:format="image/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\HXBTAIX6.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\HXBTAIX6.htm	
Size (bytes):	476
Entropy (8bit):	4.954301751982787
Encrypted:	false
SSDEEP:	12:hPEhkACy7C/GE0fM0VcFBULfuNQGj3CQZLVMWPGb:hPRCrt+F6aNZVMf
MD5:	C974D480C952F8B46D4A2E2B1735CD6A
SHA1:	535D38C41CD9D9FD0045EC577E58FBE0E203DB72
SHA-256:	64D95DD0058B02B2BA12F890111F0970818C47C8C771FDBA38C098163ECA0C20
SHA-512:	8042D654DB5921C683942409470AA91CB91AEA2673A98C08EDB5D7A95D5754AEE505F40D9F3DA646F948A0ECEF1F5D59C0925D3FC658FFEB901ED3B795B9CB 6
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>..<html lang="en">..<head>.. <meta charset="UTF-8">.. <meta name="viewport" content="width=device-width, initial-scale=1.0">.. <meta http-equiv="X-UA-Compatible" content="ie=edge">...<link rel="shortcut icon" type="image/x-icon" href="images/favicon.ico" />.. <title>Security Challenge</title>..</head>..<body>.. <div id="app"><captcha v-if="active" link="./"></captcha></div>.. <script src="./assets/js/captcha.js"></script>..</body>..</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\captcha[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	120620
Entropy (8bit):	5.261604717159396
Encrypted:	false
SSDEEP:	1536:bYEJXUrIFqE9pVnSdomZNiPFoTMrU3utV1yjgYqiwP/Pb:bYE9Fv9HnWomZoSTMri0VOQj
MD5:	61A1D827694190E20912D77413C59AC2
SHA1:	6CB409C67EEF9846CC2F412018CA58157AE81840
SHA-256:	E1678E66939660787D297768B442CC31EE07265FCACB6384E3603CFAAED7C39F
SHA-512:	8D68A2B3969CB714874B8DCEAE51237E0289080BB5FB3928E3B03790D57E1B5253FF98777E6A84596812588718D318E59776ABB9C9B2B7FB6278D600129D8752
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ciscomessagingportal.gq/assets/js/captcha.js
Preview:	!function(n){var r={};function o(e){if(r[e])return r[e].exports;var t=r[e]={i:e,l:!1,exports:{}};return n[e].call(t.exports,t,t.exports,o),t.l=!0,t.exports}o.m=n,o.c=r,o.d=function(e,t,n){o.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},o.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},o.t=function(t,e){if(1&e&&(t=o(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var n=Object.create(null);if(o.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var r in t)o.d(n,r,function(e){return t[e]}.bind(null,r));return n},o.n=function(e){var t=e&&e.__esModule?function(){return e["default"]}:function(){return e};return o.d(t,"a",t),t},o.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},o.p="/",o(o.s=12)}([function(o,e,t){"use strict";var i=t(4),n=t(20),r=Object.prototype.toString;functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 3 icons, 32x32, 32 bits/pixel, 24x24, 32 bits/pixel
Category:	downloaded
Size (bytes):	7886
Entropy (8bit):	4.14434000076088
Encrypted:	false
SSDEEP:	48:gFLLLLLLBWj2P+W3DS4E4U4R7454y4aR+BddHOlFgWSsjfQeiFzm22lhCa1I/CPP:tjQDdNKevXOl/amZP
MD5:	AC16FA7FC862073B02ACD1187FC6DEF4
SHA1:	F2B9A6255F6293000F30EEE272ABDD372A14E9D3
SHA-256:	E35D94B76894D6ECA96FF5B1A12D94DFE73485EF3C52CB5B4395BE8FFAC1CB45
SHA-512:	FF0884F9F3DED38191C7D1F214545509E80DE614BC824395F3C9412AED8D81DB95BA7E761939AC1F1798C1D39A7969A3DBF373D03A88404345714EDD8165F19D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ciscomessagingportal.gq/images/favicon.ico
Preview:	....6......... .... .h...f...(... ...@..... ....(..'...................................(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(..(.....~.....................................(.."... ... ...".(..(..(..(..(..(..(..(..(..$.....}................ ....y...y...y...y...y...y...y...y...y...%..(..(..(..(..(..'.....|............................

C:\Users\user\AppData\Local\Temp\~DF0DA9C130E8F06E70.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47978011525978576
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loD9loD9lWnpYDnSr:kBqoIkaSTSr

C:\Users\user\AppData\Local\Temp\~DF0DA9C130E8F06E70.TMP	
MD5:	FE05C607B87BB675B2C28943317098BC
SHA1:	36A14B9C05B16B7109B81A51E6C6BEF7C6E42CC1
SHA-256:	4412AAC9608FFF860DEF2833D78DFB9204C7A1CEC3CF8BA1FCBCCE96C1C753D2
SHA-512:	43589C233F2233DF90CB61EC6060B867EA5098D47E6D8694EB5894A0A5F53354D244EEB1ED79AD57A32D315553400247A329B3D2B645C108FE4EE245DBD15DA
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFAC0AF7A12B20718B.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...(.................. ....

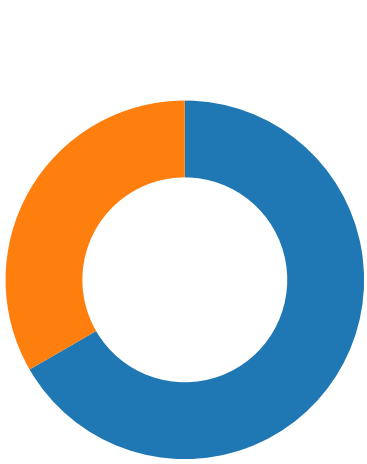
C:\Users\user\AppData\Local\Temp\~DFF7FAC163A929FC02.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34529
Entropy (8bit):	0.38063022380275835
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwrF9lw+i9l2P9l2P9lb:kBqoxKAuvScS+iEOnrIrHBkZ67c
MD5:	720575E0C9160FE34CBA0C36E8B74BAE
SHA1:	94375E7BF7371422692DAF36C3531841E970D6C2
SHA-256:	C6954CDD8B1EC9280B602494B301DE83F8776AF9608950FEA9512FD4B3EECD32
SHA-512:	BA123BD1EA80E0032DC15CF8D4047FA6F1162A5089DA12D512582AE6C3949F7CCA0DD85E7F35DC2D8A45207C85200C075977583C96D25478ECD158E1F48B165
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 01:20:50.546936035 CEST	49688	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.547090054 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.736149073 CEST	443	49688	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.736336946 CEST	49688	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.741277933 CEST	49688	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.742418051 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.742551088 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.743716955 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.930849075 CEST	443	49688	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.931399107 CEST	443	49688	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.931442976 CEST	443	49688	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.931468964 CEST	443	49688	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.931487083 CEST	443	49688	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.931520939 CEST	49688	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.931567907 CEST	49688	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.932476997 CEST	443	49688	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.932615995 CEST	49688	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.939289093 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.939644098 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.939670086 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.939692974 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.939703941 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.939768076 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.940766096 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:50.940820932 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:50.940861940 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:51.010142088 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:51.015520096 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:51.017494917 CEST	49688	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:51.207288980 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:51.207477093 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:51.208055973 CEST	443	49688	162.0.237.234	192.168.2.5
May 13, 2021 01:20:51.208118916 CEST	49688	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:51.252228022 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:51.517637014 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:51.517807007 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:51.521012068 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:51.719865084 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:51.745419979 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:51.745580912 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:51.860970974 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.070621967 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.070667028 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.070689917 CEST	443	49689	162.0.237.234	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 01:20:52.070704937 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.070724964 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.070743084 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.070755005 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.070763111 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.070771933 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.070789099 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.070806980 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.070871115 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269516945 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269555092 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269579887 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269599915 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269604921 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269629002 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269630909 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269649982 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269659996 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269675970 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269685984 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269710064 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269711018 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269736052 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269737959 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269756079 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269763947 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269781113 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269789934 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269799948 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269814014 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269835949 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269835949 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269865990 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269867897 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269892931 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269897938 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269917965 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269943953 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269959927 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269968987 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.269973993 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.269979954 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.270009041 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.270030022 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.468897104 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.468941927 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.468971968 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.469000101 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.469026089 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.469048977 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.469065905 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.469162941 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.469208956 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.592984915 CEST	49689	443	192.168.2.5	162.0.237.234
May 13, 2021 01:20:52.796770096 CEST	443	49689	162.0.237.234	192.168.2.5
May 13, 2021 01:20:52.796832085 CEST	443	49689	162.0.237.234	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 01:20:41.490374088 CEST	53183	53	192.168.2.5	8.8.8.8
May 13, 2021 01:20:41.543404102 CEST	53	53183	8.8.8.8	192.168.2.5
May 13, 2021 01:20:42.786076069 CEST	57587	53	192.168.2.5	8.8.8.8
May 13, 2021 01:20:42.843065023 CEST	53	57587	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 01:20:43.647454977 CEST	55432	53	192.168.2.5	8.8.8.8
May 13, 2021 01:20:43.727080107 CEST	53	55432	8.8.8.8	192.168.2.5
May 13, 2021 01:20:44.486845970 CEST	64936	53	192.168.2.5	8.8.8.8
May 13, 2021 01:20:44.542133093 CEST	53	64936	8.8.8.8	192.168.2.5
May 13, 2021 01:20:45.405225039 CEST	52704	53	192.168.2.5	8.8.8.8
May 13, 2021 01:20:45.457607031 CEST	53	52704	8.8.8.8	192.168.2.5
May 13, 2021 01:20:46.892407894 CEST	52212	53	192.168.2.5	8.8.8.8
May 13, 2021 01:20:46.954514027 CEST	53	52212	8.8.8.8	192.168.2.5
May 13, 2021 01:20:48.435457945 CEST	54302	53	192.168.2.5	8.8.8.8
May 13, 2021 01:20:48.490430117 CEST	53	54302	8.8.8.8	192.168.2.5
May 13, 2021 01:20:48.923835993 CEST	53784	53	192.168.2.5	8.8.8.8
May 13, 2021 01:20:48.987654924 CEST	53	53784	8.8.8.8	192.168.2.5
May 13, 2021 01:20:50.093610048 CEST	65307	53	192.168.2.5	8.8.8.8
May 13, 2021 01:20:50.289335012 CEST	64344	53	192.168.2.5	8.8.8.8
May 13, 2021 01:20:50.347174883 CEST	53	64344	8.8.8.8	192.168.2.5
May 13, 2021 01:20:50.536627054 CEST	53	65307	8.8.8.8	192.168.2.5
May 13, 2021 01:21:07.331670046 CEST	62060	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:07.394896984 CEST	53	62060	8.8.8.8	192.168.2.5
May 13, 2021 01:21:10.755594969 CEST	61805	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:10.836894989 CEST	53	61805	8.8.8.8	192.168.2.5
May 13, 2021 01:21:18.913017035 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:18.973469019 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 01:21:19.658793926 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:19.720187902 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 01:21:19.905740976 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:19.966099024 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 01:21:20.669929981 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:20.722023964 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 01:21:20.903912067 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:20.964276075 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 01:21:21.685110092 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:21.737261057 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 01:21:22.928184032 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:22.988727093 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 01:21:23.685396910 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:23.745969057 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 01:21:26.936197042 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:26.998286009 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 01:21:27.701541901 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 01:21:27.756062984 CEST	53	49557	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2021 01:20:50.093610048 CEST	192.168.2.5	8.8.8.8	0xf492	Standard query (0)	ciscomessa gingportal.gq	A (IP address)	IN (0x0001)
May 13, 2021 01:21:07.331670046 CEST	192.168.2.5	8.8.8.8	0xc957	Standard query (0)	ciscomessa gingportal.gq	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 01:20:50.536627054 CEST	8.8.8.8	192.168.2.5	0xf492	No error (0)	ciscomessa gingportal.gq		162.0.237.234	A (IP address)	IN (0x0001)
May 13, 2021 01:21:07.394896984 CEST	8.8.8.8	192.168.2.5	0xc957	No error (0)	ciscomessa gingportal.gq		162.0.237.234	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 13, 2021 01:20:50.932476997 CEST	162.0.237.234	443	192.168.2.5	49688	CN=ciscomessagingportal.gq 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	Thu Mar 25 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jun 24 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		
May 13, 2021 01:20:50.940766096 CEST	162.0.237.234	443	192.168.2.5	49689	CN=ciscomessagingportal.gq 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	Thu Mar 25 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jun 24 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		
May 13, 2021 01:21:07.799256086 CEST	162.0.237.234	443	192.168.2.5	49690	CN=ciscomessagingportal.gq 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	Thu Mar 25 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jun 24 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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: 6088 Parent PID: 792

General

Start time:	01:20:47
Start date:	13/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff799c40000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5148 Parent PID: 6088

General

Start time:	01:20:47
Start date:	13/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6088 CREDAT:17410 /prefetch:2
Imagebase:	0xc30000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly