ID: 385482
Cookbook: browseurl.jbs
Time: 15:25:18
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

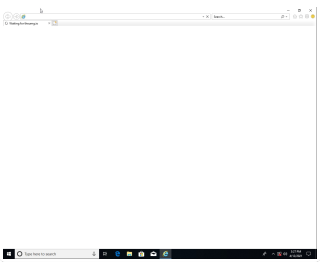
Analysis Report https://theumg.io/sendy/l/VW1gAgapdP…

Overview

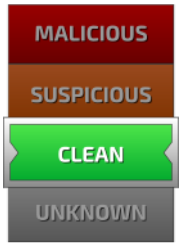
General Information

Sample URL:	http://https://theumg.io/sendy/l/VW1gAgapdPzbdYRlrDKGfg/jkZXej7lRHyHDOvMzNt5kA/8v8Gu9q6f7m64yYP6Fjp4A
Analysis ID:	385482
Infos:	

Most interesting Screenshot:



Detection

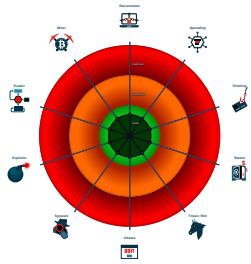


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5328 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5444 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5328 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

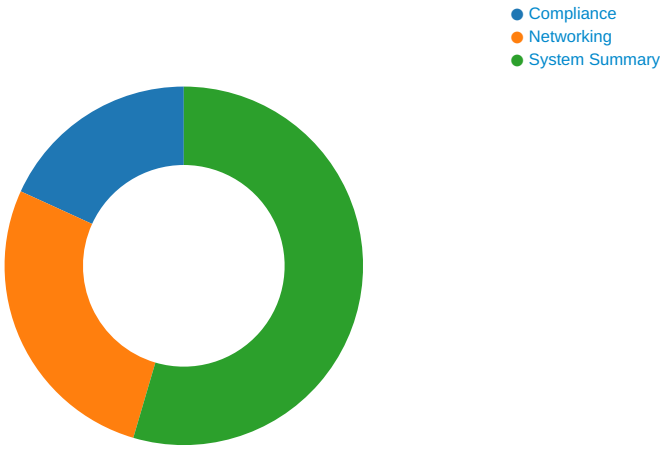
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



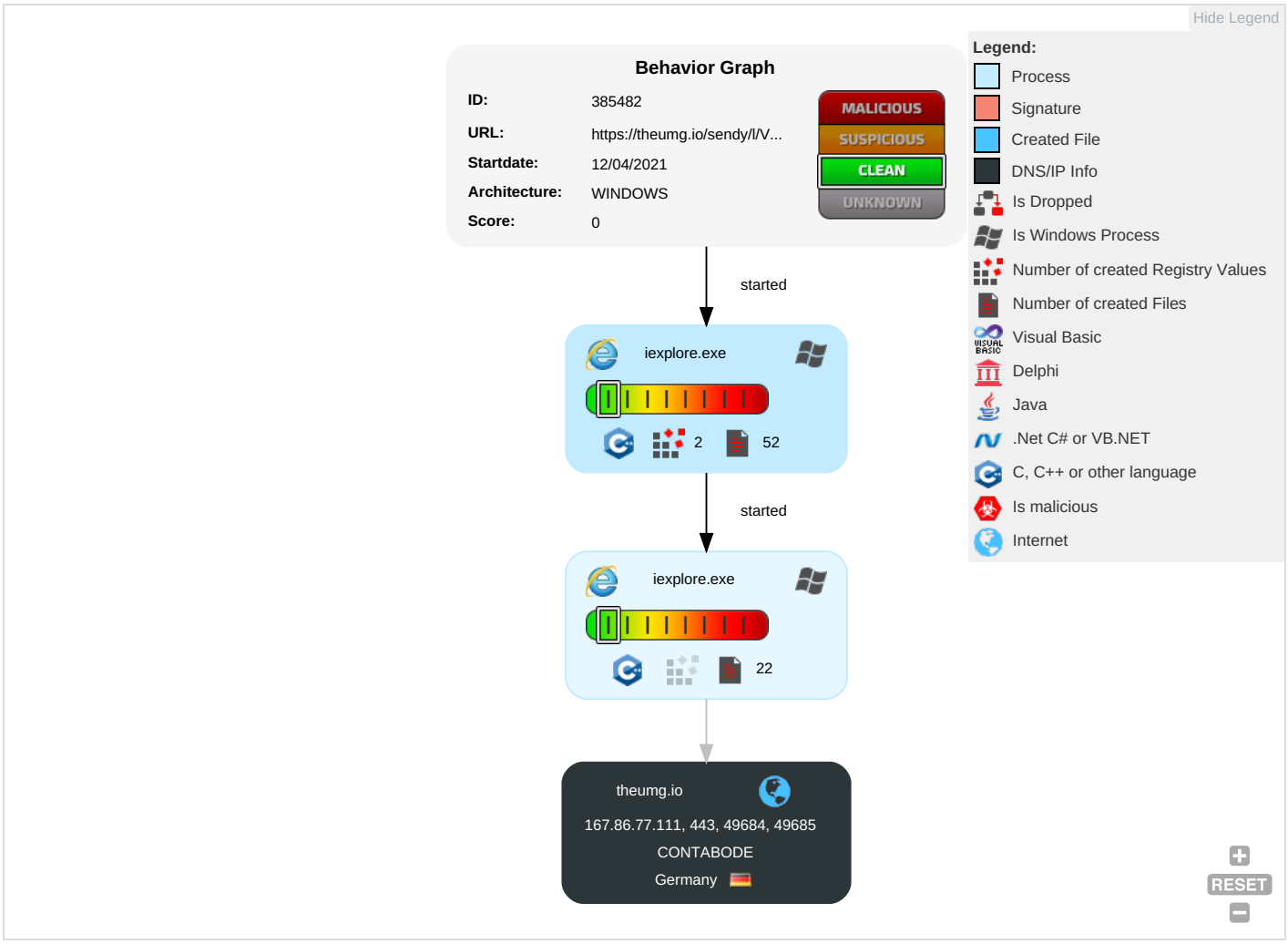
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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

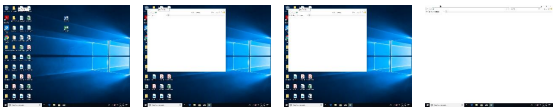
Behavior Graph

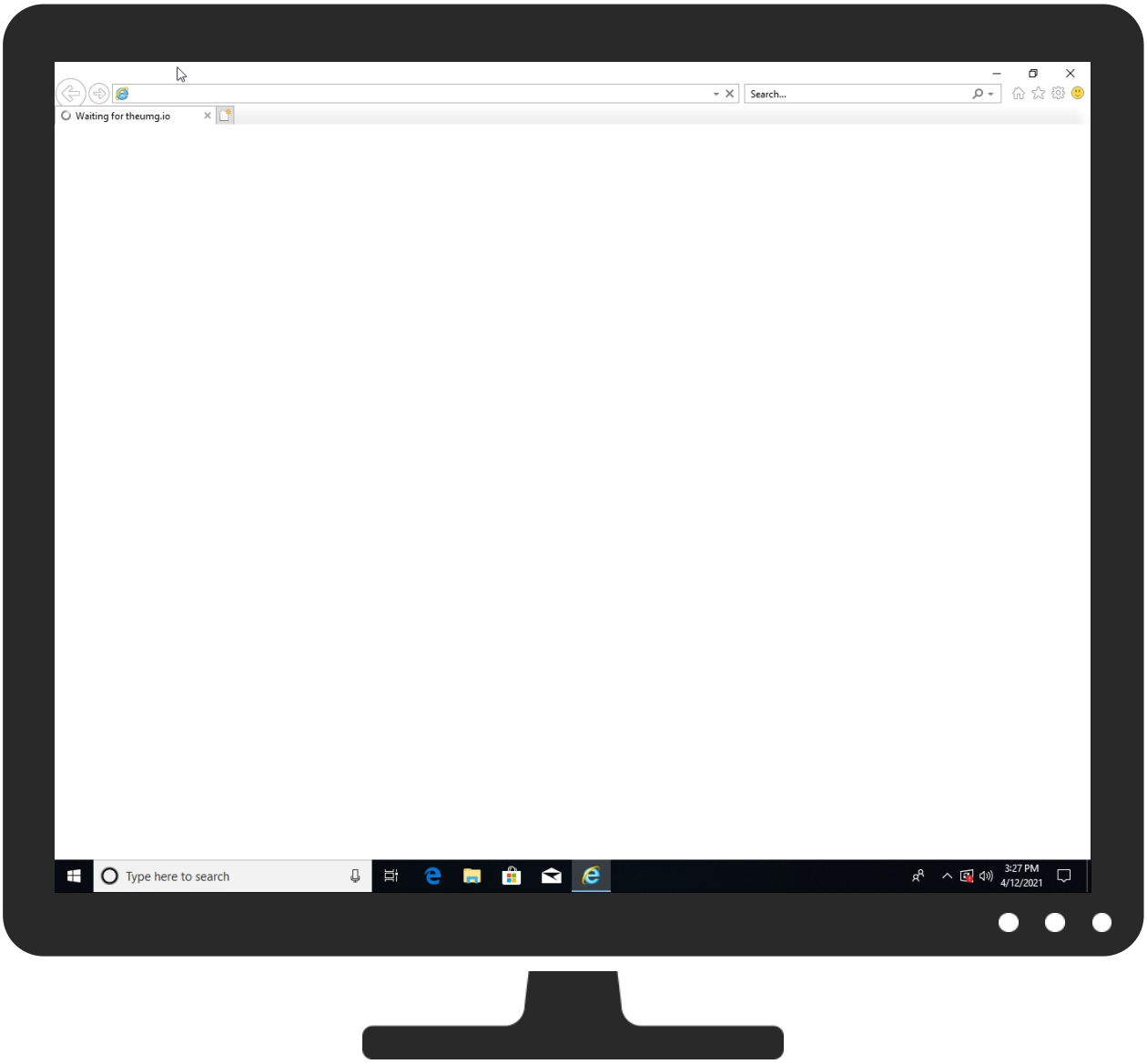


Screenshots

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://theumg.io/sendy/l/VW1gAgapdPzbdYRlrDKGfg/jkZXej7lRHyHDOvMzNt5kA/8v8Gu9q6f7m64yYP6Fjp4A	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
theumg.io	167.86.77.111	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	false		low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.86.77.111	theumg.io	Germany		51167	CONTABODE	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385482
Start date:	12.04.2021
Start time:	15:25:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://theumg.io/sendy/l/VW1gAgapdPzbdYRlrDKGfg/jkZXej7lRHyHDOvMzNt5kA/8v8Gu9q6f7m64yYP6Fjp4A

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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/6@1/1
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, SgrmBroker.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 88.221.62.148, 104.42.151.234, 92.122.144.200, 13.88.21.125, 152.199.19.161, 93.184.221.240 • Excluded domains from analysis (whitelisted): fs.microsoft.com, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wu.azureedge.net, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net, cs9.wpc.v0cdn.net • VT rate limit hit for: https://theumg.io/sendy/l/VW1gAgapdPzbdYRlrDKGfg/jkZXej7lRHyHDOvMzNt5kA/8v8Gu9q6f7m64yYP6Fjp4A

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.{15DB888A-9BDE-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.860342039145661
Encrypted:	false
SSDEEP:	192:reFZ8cZ5201W0Ct02if0kwKzM0niB0m8D0Tsf0vwjjX:rAdo0M060H0V060h0e0o
MD5:	38302F01D0C3C9000B97BF1EF1DC7AA1
SHA1:	A2B4BEE234DF29902CD2E08FF3AB852F343645D1
SHA-256:	0AE80F566D95889734CC4F5B44C3E74D67E5FC1C5CDEB53A275BE6BB2F945C29
SHA-512:	286E0B69F5180474CF5D7AA6ACEE66FB202AF4AA6FDDB0701864DECD8E4883A1DBC005133B0B616F7CADB9D8D5AE2105AA334ED2C8FC37DB128984D0A1BCA553
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\{15DB888C-9BDE-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.575479620360812
Encrypted:	false
SSDEEP:	48:IwhGcprQGwpa4G4pQUGrapbSvGQpBWGHHpcR7TGUpG:rXZ4Qo6iBS5jV2RVA
MD5:	82C03C0947B82AF7052BD762CF62F832
SHA1:	FD57ECFF33F94D5B47D73AE6EDA0975E186C9C2B
SHA-256:	BB040D405EEA98138592598DFC948E329808C2AE5418675DBFFD9E1E087450F8
SHA-512:	FFB0856FA1DAD84F76C37DC5E5F6C4BD0022150F82F49EC3BF6D41810FB7222DD6990B35D7D738BB6D58A12448A17F3AEA66E141467E3909210C34C7C978D78
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\{2017BF91-9BDE-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5643849310728324
Encrypted:	false
SSDEEP:	48:IwMGcprBGwpavG4pQjGrapbS6GQpKPG7HpRUTGlpG:rQZbQh6HBSCAeTwA
MD5:	0424413DF6B69E83CA907AFECA6777B7
SHA1:	98AB3074805AEC7B0E76BEF30F4FE6F43EF5A4E7

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2017BF91-9BDE-11EB-90E6-ECF4BB82F7E0}.dat	
SHA-256:	909B0A68451A5441BE6DA9E54CCBAD7F8667539A73D92476D167B3ED3F402231
SHA-512:	C9D96428446CF03E021FEACCE39262179F7CBDF8CD5797D50ADDD9598605C3CAAD4568BC11DBCD99C17D45196611E41B78B843E1F89433629C13F99DB6B912
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Temp\~DF7972584DD7ADBB05.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48204116742501196
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRi9l8fRS9lTq0Cje:c9lLh9lLh9lIn9lIn9loi9loS9lW0Cje
MD5:	35290613C30117128C8267604E2850A8
SHA1:	99BDBE8EBAF4B20E9DB860E3E183525506C40AC1
SHA-256:	04428BEE8648F44FAE21C205757BA948E3C52F94E2051232C018E42D5CD22DF1
SHA-512:	33244BEBC8A047765876F34B656EFF9E27D748D6C904AA5F3D5B1F0E112A8E588BD5D201DB311691D5A5F2BA0BDFDC9BB9918DC208960E297CD6F3CCC5E08E FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF7FE99D633414C1A7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	25441
Entropy (8bit):	0.3717884046375479
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAuxynlPty9g:kBqoxxJhHWSVSEabuxAJtg
MD5:	D1F328849F0A560A9AD6205F51180CAA
SHA1:	8728CE85CBD849C8AC8395E664D991AFCABB6A23
SHA-256:	61664DA9735BCA0D494E1ABF653D44CF7AC4AB8DA390A7CD9BF9661D5B866490
SHA-512:	5ECBCD884515C5C3D037FFD4D9D62C26A2789375C378DEEA0B1B7B3DC3CDDCD7B037E543A5C8E9266073BC2F0B44AD717CD1C4977AC97A1A7E7E4A942BDE CAC
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFDBED20CF3A1B55E5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.31383355293505655
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw0F9lwdi9l2X:kBqoxKAuvScS+XZX
MD5:	C4E65D21A4A29963AA099427CCBACDD2
SHA1:	160B3D9FF2AA0BB99ECB2FA6BDEEFEEF480F3627
SHA-256:	E068CFA02B933A13BCA649EEC7AE9EB78AAFD53EC1DECAD96FEF3F36A20A8CB5
SHA-512:	ABC782227B24B86F34F3C74328A3172F189603ACFA93F8700FAA380027AEA03465B79075433BF3898DE164E11316D005B34060F7DA42FD348A23A3AF69478DF3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFDBED20CF3A1B55E5.TMP

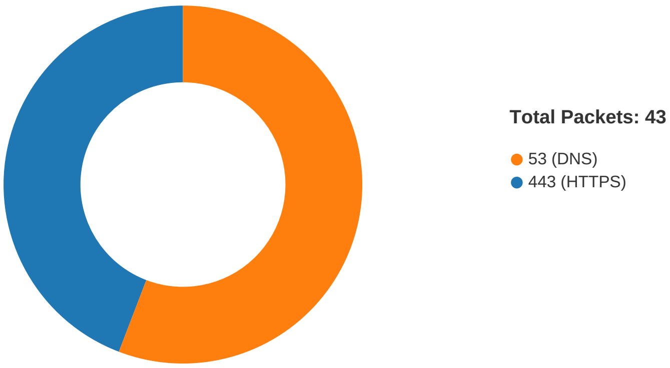
Preview:	...............................*%..H..M..{y..+.0...(.................... ....*%..H..M..{y..+.0...(.................... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:26:14.628031969 CEST	49685	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.628032923 CEST	49684	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.677937031 CEST	443	49684	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.677988052 CEST	443	49685	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.678071976 CEST	49684	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.678126097 CEST	49685	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.688148975 CEST	49684	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.688389063 CEST	49685	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.737566948 CEST	443	49684	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.737615108 CEST	443	49685	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.738245964 CEST	443	49684	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.738292933 CEST	443	49684	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.738332033 CEST	443	49684	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.738359928 CEST	443	49684	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.738440037 CEST	49684	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.738500118 CEST	49684	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.738508940 CEST	49684	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.739209890 CEST	443	49685	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.739253044 CEST	443	49685	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.739291906 CEST	443	49685	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.739306927 CEST	49685	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.739319086 CEST	443	49685	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.739336967 CEST	49685	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.739372969 CEST	49685	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.741316080 CEST	443	49684	167.86.77.111	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:26:14.741450071 CEST	49684	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.745129108 CEST	443	49685	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.745255947 CEST	49685	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.825424910 CEST	49684	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.825449944 CEST	49685	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.833261013 CEST	49684	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.877960920 CEST	443	49684	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.878098011 CEST	49684	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.878536940 CEST	443	49685	167.86.77.111	192.168.2.7
Apr 12, 2021 15:26:14.878637075 CEST	49685	443	192.168.2.7	167.86.77.111
Apr 12, 2021 15:26:14.923826933 CEST	443	49684	167.86.77.111	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:26:05.556762934 CEST	61952	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:05.608333111 CEST	53	61952	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:06.590923071 CEST	56217	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:06.640914917 CEST	53	56217	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:13.020711899 CEST	63354	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:13.079252958 CEST	53	63354	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:14.551573992 CEST	53129	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:14.608679056 CEST	53	53129	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:16.363504887 CEST	62452	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:16.415154934 CEST	53	62452	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:17.274507999 CEST	57820	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:17.323411942 CEST	53	57820	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:18.392263889 CEST	50848	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:18.442234039 CEST	53	50848	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:25.258238077 CEST	61242	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:25.316812038 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:33.793570995 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:33.851911068 CEST	53	58562	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:36.572417974 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:36.634529114 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:38.550019026 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:38.599642038 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:43.036808968 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:43.085717916 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:43.891110897 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:43.942683935 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:44.024004936 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:44.072813988 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:44.885077953 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:44.936530113 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:45.040888071 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:45.089589119 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:45.899224997 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:45.951215982 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:47.038572073 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:47.087255001 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:47.914132118 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:47.965745926 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:51.054426908 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:51.111895084 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:51.934000969 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:51.985559940 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 12, 2021 15:26:54.233516932 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:26:54.282211065 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 12, 2021 15:27:01.200623989 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:27:01.259236097 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 12, 2021 15:27:24.825371981 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:27:24.874473095 CEST	53	54640	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:26:14.551573992 CEST	192.168.2.7	8.8.8.8	0xbdf7	Standard query (0)	theumg.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:26:14.608679056 CEST	8.8.8.8	192.168.2.7	0xbdf7	No error (0)	theumg.io		167.86.77.111	A (IP address)	IN (0x0001)

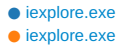
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 15:26:14.741316080 CEST	167.86.77.111	443	192.168.2.7	49684	CN=theumg.io 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	Tue Mar 23 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Jun 22 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		
Apr 12, 2021 15:26:14.745129108 CEST	167.86.77.111	443	192.168.2.7	49685	CN=theumg.io 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	Tue Mar 23 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Jun 22 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		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5328 Parent PID: 792

General

Start time:	15:26:12
Start date:	12/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff73b3b0000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 5444 Parent PID: 5328

General

Start time:	15:26:13
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5328 CREDAT:17410 /prefetch:2
Imagebase:	0xc20000
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	Completion	Count	Source Address	Symbol

Disassembly