ID: 385480
Cookbook: browseurl.jbs
Time: 15:23:51
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report
https://theumg.io/sendy/l/VW1gAgapdPzbdYRlrDKGfg/jIGbD9oIL71s0OhPRyHYIA/8v8Gu9q6f7m64yYP6Fjp4A
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Startup 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Signature Overview 3
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
Contacted IPs 7
Public 7
General Information 7
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 11
No static file info 11
Network Behavior 11
Network Port Distribution 11
TCP Packets 11
UDP Packets 12
DNS Queries 13
DNS Answers 14
HTTPS Packets 14
Code Manipulations 14
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: iexplore.exe PID: 6472 Parent PID: 800 15
General 15
File Activities 15
Registry Activities 15
Analysis Process: iexplore.exe PID: 6564 Parent PID: 6472 16
General 16
File Activities 16
Disassembly 16

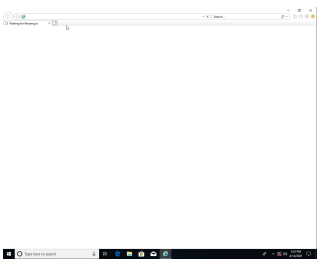
Analysis Report https://theumg.io/sendy/l/VW1gAgapdP…

Overview

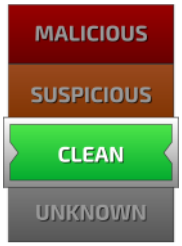
General Information

Sample URL:	http://https://theumg.io/sendy/l/VW1gAgapdPzbdYRlrDKGfg/jIGbD9oIL71s0OhPRyHYIA/8v8Gu9q6f7m64yYP6Fjp4A
Analysis ID:	385480
Infos:	

Most interesting Screenshot:



Detection

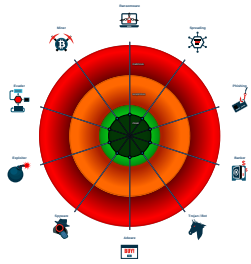


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6472 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6564 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6472 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

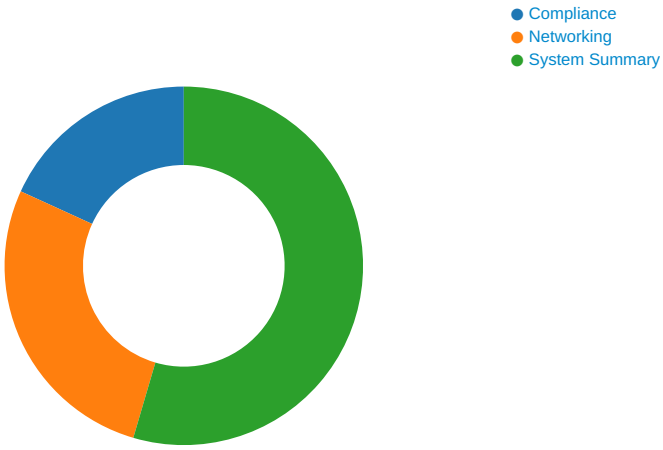
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



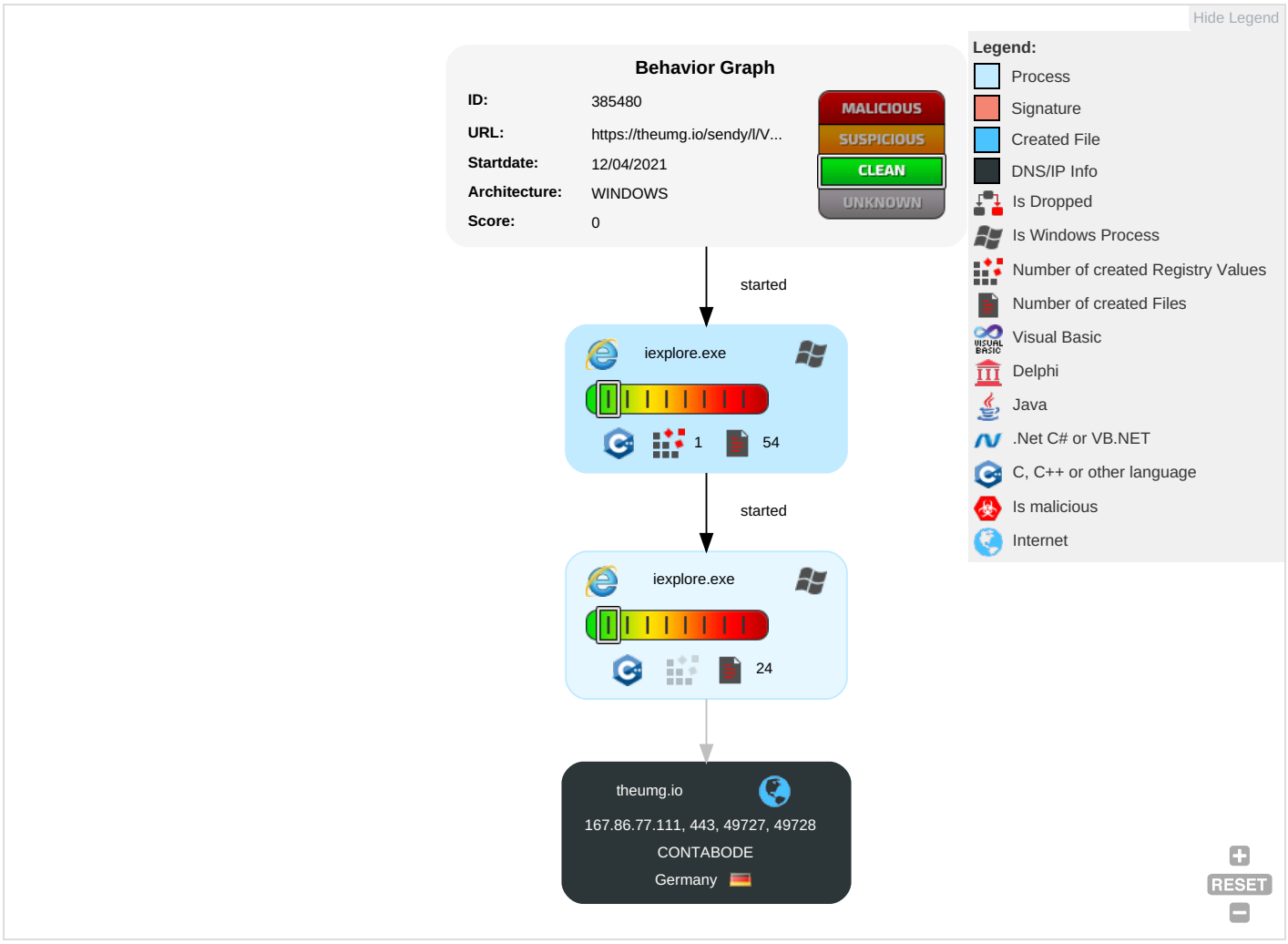
Click to jump to signature section

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

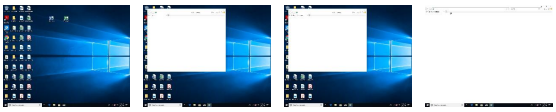
Behavior Graph

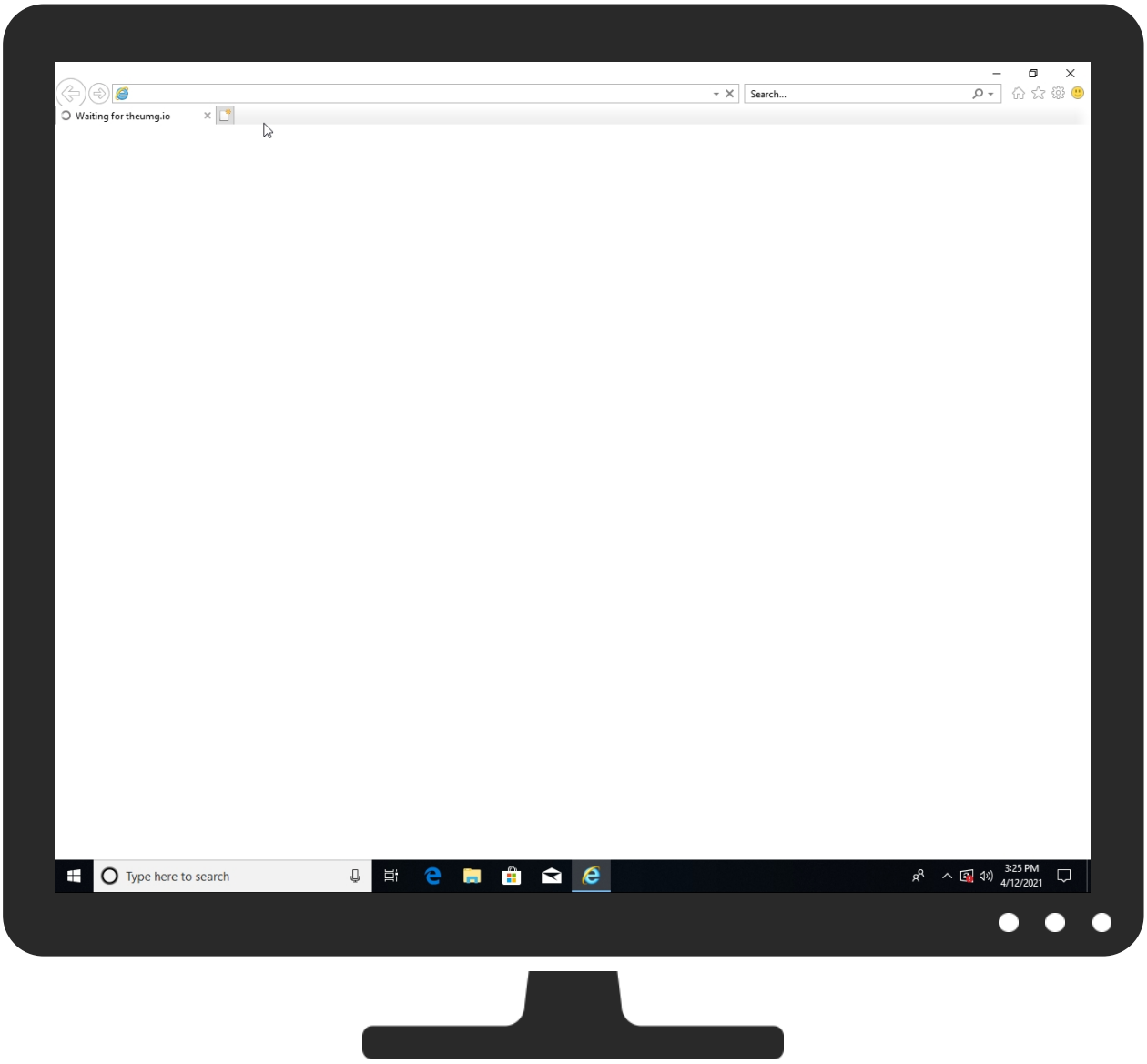


Screenshots

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/jIGbD9oIL71s0OhPRyHYIA/8v8Gu9q6f7m64yYP6Fjp4A	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
theumg.io	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

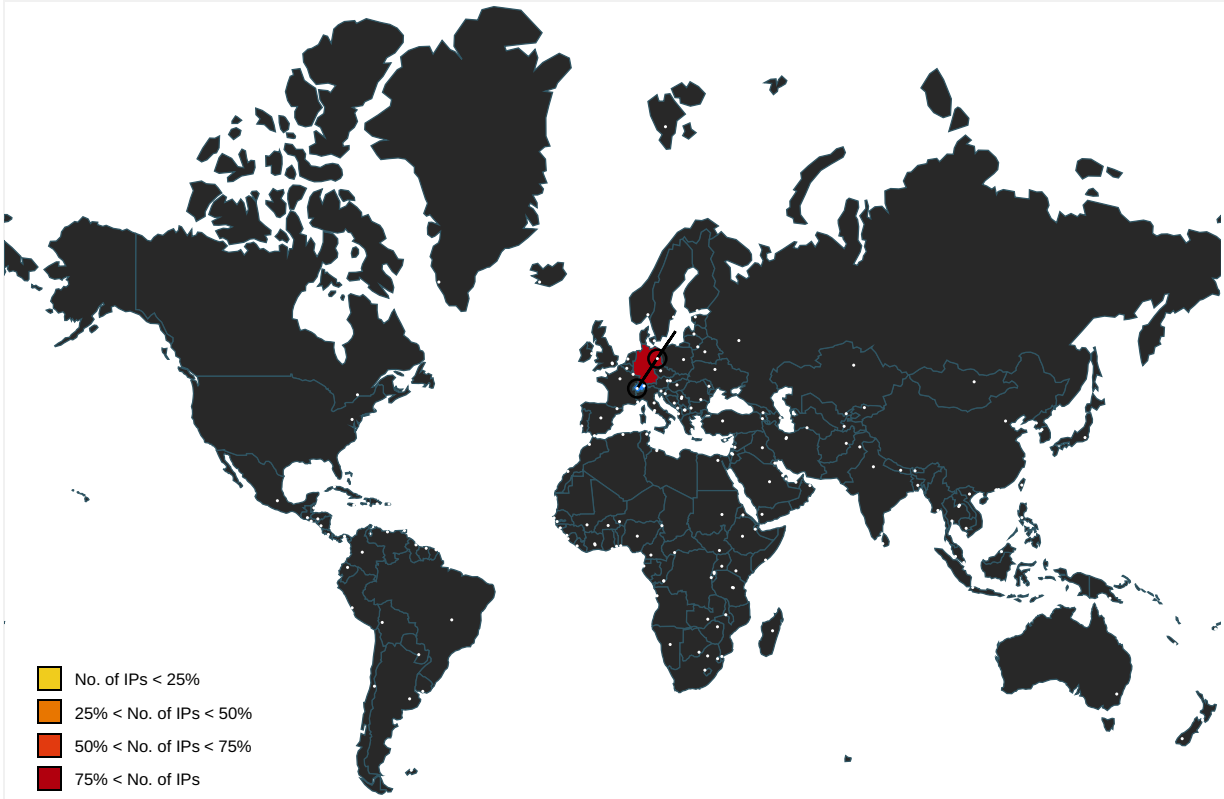
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
theumg.io	167.86.77.111	true	false	• 0%, Virustotal, Browse	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:	385480
Start date:	12.04.2021
Start time:	15:23:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://theumg.io/sendy/l/VW1gAgapdPzbdYRlrDKGfg/jlGbD9oIL71s0OhPRyHYIA/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:	17
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): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 88.221.62.148, 13.64.90.137, 20.82.210.154, 92.122.213.194, 92.122.213.247, 152.199.19.161, 52.147.198.201, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129, 104.43.193.48, 104.43.139.144, 20.82.209.183, 52.255.188.83, 104.42.151.234 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net

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.{6E19B87B-9B92-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8556033511143781
Encrypted:	false
SSDEEP:	192:r7Z4ZD2FWGtZifgiYzM9QBtoWD0sfviVjX:rNY68G29KtZjI
MD5:	EE323ABCBFA9B6748C1BE5D27C8BE1C8
SHA1:	306190C4DDAE8770CE5251CC3AEB23BFB974661E
SHA-256:	B5F99567746FA815C7088DC31CB5EAE37E3B754883A7CAAECA983EBC89F8E28F
SHA-512:	FCC12C19B860DF46716C95E0DE8810D646ADCAEE41C3FA88FE65859BCDBEFE2031125DCE647701CA4994FDD695BC2F79B81F34108291876EEA405434B24B09 9
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\{6E19B87D-9B92-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5747221128373639
Encrypted:	false
SSDEEP:	48:IwIGcpr+GwpaWG4pQ3GrapbSCGQpBOygXGHHpcOy+TcTGUpG:r8Z2Qm6LBSKjdgC2d+TUA
MD5:	36D1F00B600963EA3153020E70782D68
SHA1:	FD210F48BA0DE8F01B21DD869788FC6CB335AFE6
SHA-256:	CB233A857DA24C7571B4CBD6721BD44BBA94495F88ECBCD5A46F9C90E051480E
SHA-512:	2C0895065A8D0657A8D20337924E75044E68DB8FB27E328DBE50A78877A891066BA35A3DA0BF4C8F7E3FCC80DF63E5F10D395BD7CA3F857713AB0FCBDF8F595
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6E19B87D-9B92-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{78453E96-9B92-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.56550724784434
Encrypted:	false
SSDEEP:	48:IwiGcprrGwpaKG4pQ6GrapbSlvGQpK5xG7HpR9TGIpG:rWZlQq6sBSI5A6T7A
MD5:	EB7636769FEBF328D2D64E74A04B1D96
SHA1:	35EBDCB0273D791E308C8A04BF53FF4A593FC50C
SHA-256:	A25D47485877C2E8B0247EC222382572EB35E5A1D53037FD31A863A857D8F13C
SHA-512:	A1506BA6C89BCA70BFBACB8F7FA8C5C154438BA26771E77517E98C78B89701F01C3491FFC36E09722BE6559FEBC2F3D46B3F21A3EE04B146F67E4468816C7FE
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Temp\~DF003F897782CA72CD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.31425763153041986
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwOyRF9lwOyki9l2Oy6:kBqoxKAuvScS+OyMOyqOy6
MD5:	E3D50B70EBA6AE403518F620EB46958C
SHA1:	54C872A00781AC82EC12A0AA5EA01EEA85124CF0
SHA-256:	22A8E79B8D8BC28C7901CD09BFE37BAF74607F21EA49037470D045455502C3C0
SHA-512:	CA1DE13F8144A9ED4F77AB444965F9802FBB12A1B4E473A29639950AAE2A6E29CC298F4B172A72F7A704F91BDC9561BF663A549787F046544998BF3F6E57395A
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA5F4A0DB13383F94.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.39662400487867816
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAgg4sc9nX7:kBqoxxJhHWSVSEabm9nr
MD5:	BFFFD37A1F7462AC356FABB8A60E015E
SHA1:	76C6EF97273F8DFB115E43C466630160726A9A5B
SHA-256:	736B17CEF1470365790398 52EEAE19403EB07DF9E633DF60EDEE96281CD23BF4
SHA-512:	4300501914E09BAA01A2E3E514036C9703287FDBEC8D56D37F6345DE5AC05F4698FA81EBCE6224E7DB1247437056C57A3D863E83116642E1A7E5799B46814670
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFEDC4065D0C93F2A6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

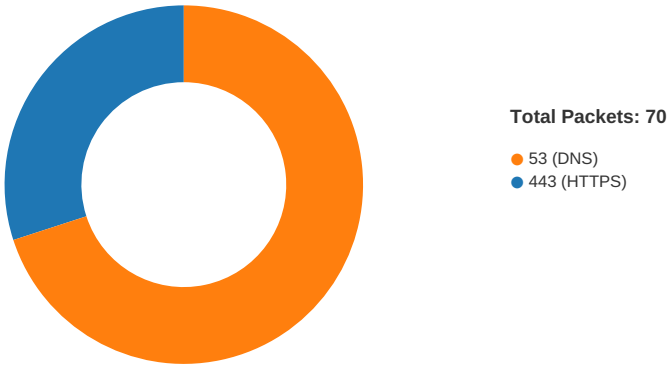
C:\Users\user\AppData\Local\Temp\~DFEDC4065D0C93F2A6.TMP	
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47785172102793116
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRPF9l8fRN9lTqB7dGw:c9lLh9lLh9lIn9lIn9lot9loN9lWB/
MD5:	420F37FEE1FA439DD0EA413B1F08512D
SHA1:	85439D17CD90EF7C83EA419953A9DB5ED03E30D8
SHA-256:	E345DEC29604447DE323C3E4047A5BAB40B7371D320FEB1621B99ED0149C732C
SHA-512:	A6052D96A755B26954B319657ED207DFA276BD67BB38310B51F681081204A6ECAF9B7C4543A2059A513E77E1CC2C358F8F97771163B090C1329FED09CBEA5B65
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
Apr 12, 2021 15:24:40.056375980 CEST	49727	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.056488037 CEST	49728	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.106163025 CEST	443	49727	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.106259108 CEST	49727	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.107008934 CEST	443	49728	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.107089996 CEST	49728	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.114501953 CEST	49728	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.114599943 CEST	49727	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.166860104 CEST	443	49728	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.167282104 CEST	443	49727	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.167525053 CEST	443	49728	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.167565107 CEST	443	49728	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.167592049 CEST	49728	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.167632103 CEST	49728	443	192.168.2.4	167.86.77.111

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:24:40.167653084 CEST	443	49728	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.167685032 CEST	443	49728	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.167695999 CEST	49728	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.167722940 CEST	49728	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.167987108 CEST	443	49727	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.168030024 CEST	443	49727	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.168059111 CEST	49727	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.168100119 CEST	49727	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.168128014 CEST	443	49727	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.168154001 CEST	443	49727	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.168176889 CEST	49727	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.168195009 CEST	49727	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.169327021 CEST	443	49728	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.169379950 CEST	49728	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.170838118 CEST	443	49727	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.171000004 CEST	49727	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.241101980 CEST	49727	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.241307974 CEST	49728	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.256354094 CEST	49728	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.291162968 CEST	443	49727	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.291188002 CEST	443	49728	167.86.77.111	192.168.2.4
Apr 12, 2021 15:24:40.291241884 CEST	49727	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.291280031 CEST	49728	443	192.168.2.4	167.86.77.111
Apr 12, 2021 15:24:40.343307018 CEST	443	49728	167.86.77.111	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:24:32.601421118 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:24:32.660427094 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 15:24:38.865060091 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:24:38.925349951 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 15:24:39.986875057 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:24:40.043977976 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 15:24:41.585099936 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:24:41.635663033 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 15:24:43.203046083 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:24:43.256880045 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:01.863862038 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:01.915560007 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:08.133441925 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:08.192301035 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:08.872595072 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:08.921139002 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:09.523650885 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:09.575313091 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:09.861428976 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:09.910173893 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:10.538281918 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:10.589951038 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:10.875091076 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:10.924734116 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:11.531547070 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:11.583125114 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:12.307475090 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:12.356336117 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:12.889933109 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:12.951776981 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:13.546377897 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:13.597896099 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:16.905910015 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:16.955691099 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:17.566126108 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:17.618634939 CEST	53	52991	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:25:26.726852894 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:26.789138079 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:28.588733912 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:28.714356899 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:29.261965990 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:29.399616957 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:30.020826101 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:30.080955982 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:30.614722967 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:30.672751904 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:31.022929907 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:31.080384970 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:31.390405893 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:31.447743893 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:32.037245989 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:32.116092920 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:32.743554115 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:32.800792933 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:33.576845884 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:33.641896963 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:34.491087914 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:34.552495956 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:35.123694897 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:35.180953979 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:43.323940992 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:43.380925894 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:46.135184050 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:46.184914112 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:47.464237928 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:47.515913963 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:48.248893976 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:48.310995102 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:49.202990055 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:49.262852907 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:53.259340048 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:53.307904959 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:54.299331903 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:54.349534035 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:55.583808899 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:55.632605076 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:58.929923058 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:58.978615999 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 12, 2021 15:25:59.826695919 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:25:59.878268957 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 12, 2021 15:26:00.824055910 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:26:00.874188900 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 12, 2021 15:26:11.999092102 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:26:12.047916889 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 12, 2021 15:26:12.639292002 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:26:12.704540968 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 12, 2021 15:26:13.480106115 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:26:13.529021978 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 12, 2021 15:26:14.397496939 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:26:14.461102009 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 12, 2021 15:26:15.198265076 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:26:15.250041962 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 12, 2021 15:26:16.284897089 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:26:16.337925911 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 12, 2021 15:26:20.943973064 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:26:20.995501041 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 12, 2021 15:26:21.869045019 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:26:21.917728901 CEST	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:24:39.986875057 CEST	192.168.2.4	8.8.8.8	0x4c3b	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 15:24:40.043977976 CEST	8.8.8.8	192.168.2.4	0x4c3b	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 15:24:40.169327021 CEST	167.86.77.111	443	192.168.2.4	49728	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 15:24:40.170838118 CEST	167.86.77.111	443	192.168.2.4	49727	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: 6472 Parent PID: 800

General

Start time:	15:24:38
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:	0x7ff610960000
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: 6564 Parent PID: 6472

General

Start time:	15:24:39
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:6472 CREDAT:17410 /prefetch:2
Imagebase:	0x80000
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