ID: 435314
Cookbook: browseurl.jbs
Time: 12:04:09
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

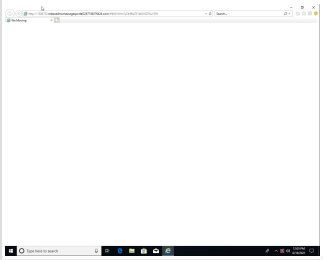
Windows Analysis Report https://meet.google.com/linkr…

Overview

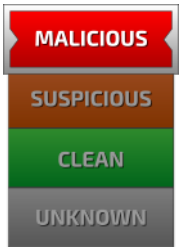
General Information

Sample URL:	http://https://meet.google.com/linkredirect?dest=1384752.releasedmsmessagesportal3267749276424.com/#bWVtYmVyQHRoZS1leGV0ZXIuY29t
Analysis ID:	435314
Infos:	

Most interesting Screenshot:



Detection

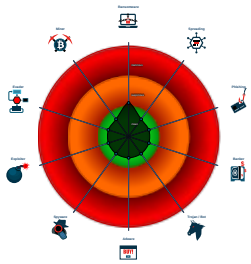


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus detection for URL or domain

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 4816 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1564 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4816 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:

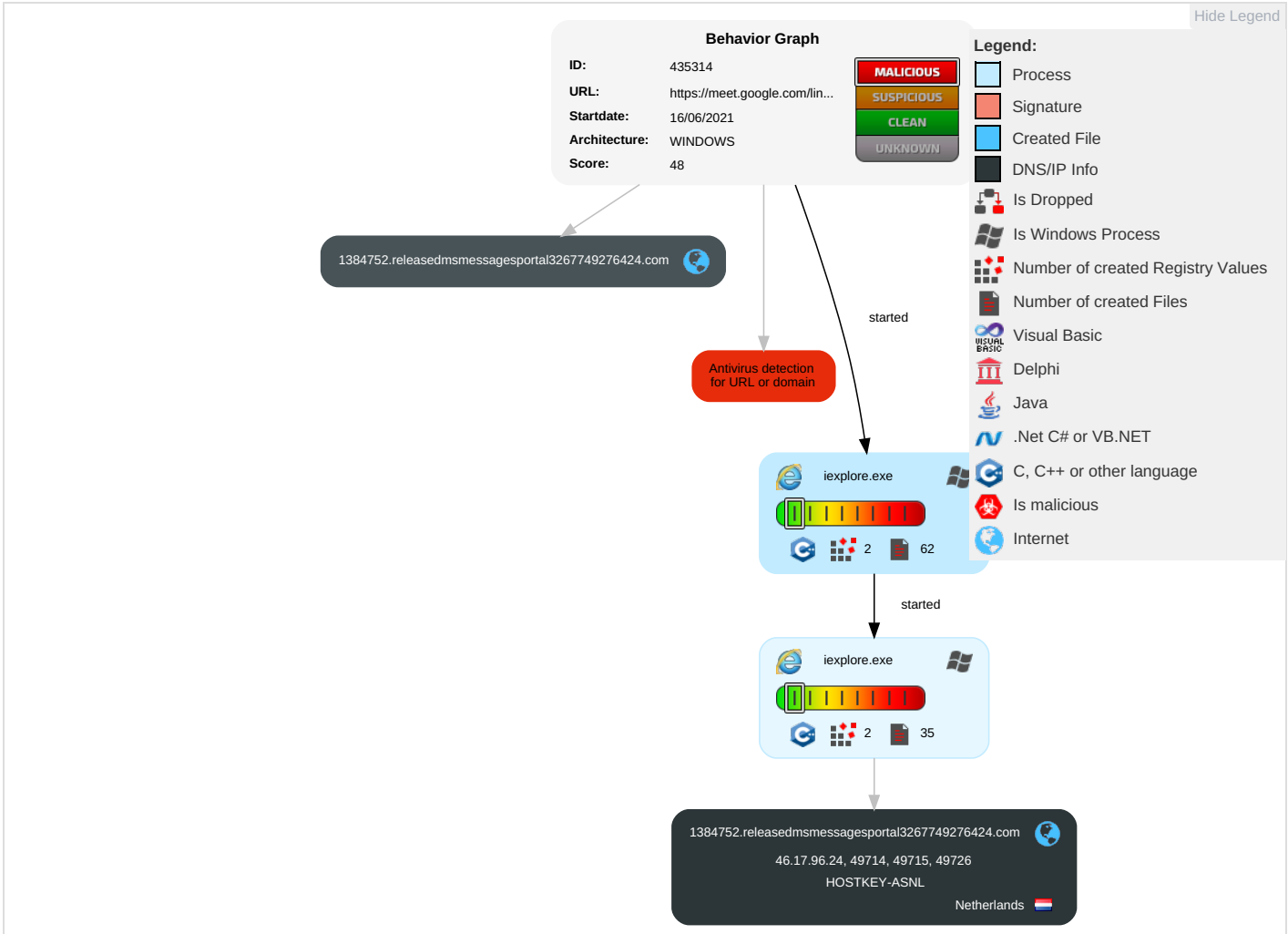
AV Detection:

Antivirus detection for URL or domain

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	Impa
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	Non-Application Layer Protocol 4	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	Application Layer Protocol 4	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	Ingress Tool Transfer 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

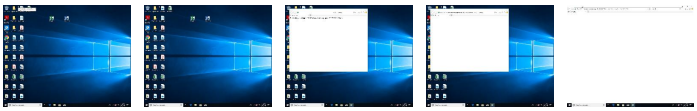
Behavior Graph

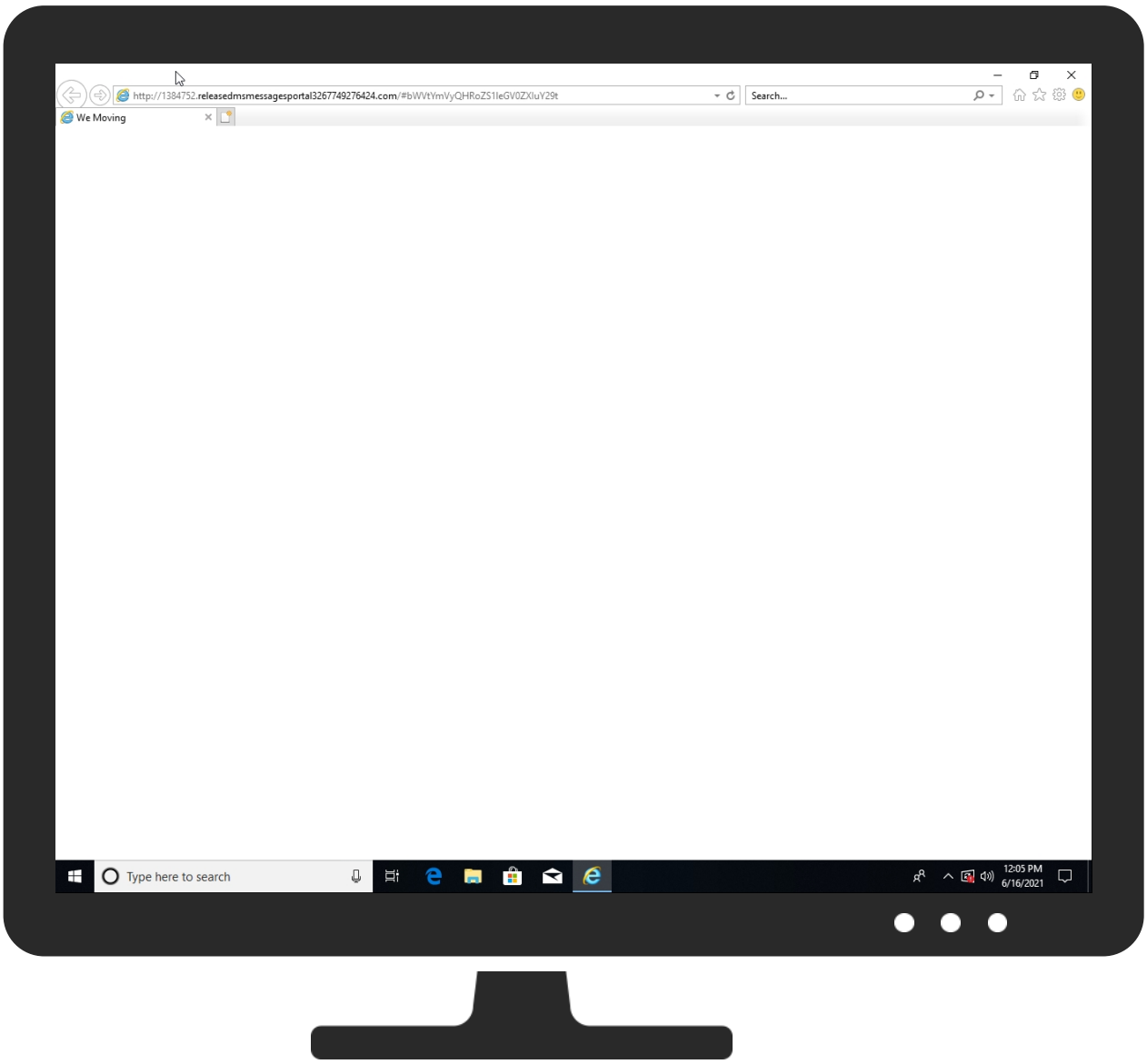


Screenshots

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://meet.google.com/linkredirect?dest=1384752.releasedmsmessagesportal3267749276424.com/#bWVtYmVyQHRoZS1leGV0ZXIuY29t	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://1384752.releasedmsmessagesportal3267749276424.com/#bWVtYmVyQHRoZS1leGV0ZXIuY29t	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://danaperu.com/re/index.php?email=	0%	Avira URL Cloud	safe	
http://1384752.releasedmsmessagesportal3267749276424.com/	100%	Avira URL Cloud	phishing	
http://1384752.releasedmsmessagesportal3267749276424.com/#bWVtYmVyQHRoZS1leGV0ZXIuY29t24.com/&sa=D&s	100%	Avira URL Cloud	phishing	
http://1384752.release/url?hl=en-US&q=http://1384752.releasedmsmessagesportal3267749276424.com/&sa=D	0%	Avira URL Cloud	safe	
http://1384752.releasedmsmessagesportal3267749276424.com/favicon.ico	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
1384752.releasedmsmessagesportal3267749276424.com	46.17.96.24	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://1384752.releasedmsmessagesportal3267749276424.com/#bWVtYmVyQHRoZS1leGV0ZXIuY29t	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://1384752.releasedmsmessagesportal3267749276424.com/	false	• Avira URL Cloud: phishing	unknown
http://1384752.releasedmsmessagesportal3267749276424.com/favicon.ico	false	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.17.96.24	1384752.releasedmsmessagesportal3267749276424.com	Netherlands		57043	HOSTKEY-ASNL	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435314
Start date:	16.06.2021
Start time:	12:04:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://meet.google.com/linkredirect?dest=1384752.releasedmsmessagesportal3267749276424.com/#bWVtYmVyQHRoZS1leGV0ZXIuY29t
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@3/10@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{BCA30B31-CED5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8562549228348508
Encrypted:	false
SSDEEP:	96:r7YZNZZk02avWtBOttGftztMtHutCteftZMX:r8ZTZ32KWKtQfltMsg8fLMX
MD5:	4148281F3863BCCA7FE0CADDE75B0C92
SHA1:	2F5FF515CB36096E12568F0577E7A74D0ED6EEEC
SHA-256:	71C44D77A60BB84109CC37AE581A2C4918397691BF437EC425DB65BE587F55C9
SHA-512:	C186B216333009C81E40AA08B91419CBB6573D1290070E0757AF66CD8C970DDF48479A5894471B8480FEA5C66119719884D8C2A945BBA7C7E658812F25F94D44

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{BCA30B31-CED5-11EB-90E4-ECF4BB862DED}.dat	
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\{BCA30B33-CED5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27264
Entropy (8bit):	1.80214448081978
Encrypted:	false
SSDEEP:	96:rRhZ7Qr6dBSQjVn2JWMMEKM0f5ltm/f5zN5A:rjZ7Qr6dkQjd2JWMMEKM8nkHpA
MD5:	0D0066D942279AC3545418BA64292B78
SHA1:	5194902E451670DBB5BAA34D2E660DD31D298020
SHA-256:	7B9EE2AAF215B81C7AC39E103057BDDE9254D142937B1637092B538A1656AC0F
SHA-512:	7E8B23B76DC02CC65BE8560EC671250E3E89C32AB0381FC4A2B8DADB5BAFCC7C1CAF0C50642C869D8586421633C66E57734CB586B148A0BB7641FF0EBEA54E 81
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\{BCA30B34-CED5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5650645350976102
Encrypted:	false
SSDEEP:	48:IwtGcprAGwpaFG4pQtGrapbS1GQpKLG7HpRL2TGIpG:rzZIQX6NBS/AKTmA
MD5:	4CAF4A4F1220D28D8B494DCA9DF09392
SHA1:	B58E72A6E203B096DB38AB08FA345AE81C24C1A9
SHA-256:	917E157E995BF2C534A0B8845E53A0270BE58434A25F402DCBD22F5AF83E1A78
SHA-512:	52F347870E19BE694312567665C4EC82C9BD0D75C2BE03BA5EFCF9B1BB4F48A34E60D296852958D3159B620E5BA78C6DFB8736B5651F1AE13978B2A6AEABBC0 3
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5648
Entropy (8bit):	3.743484537784131
Encrypted:	false
SSDEEP:	48:xwDaO7IJct3xl3l1lzwDaYxG/7nvWDtZcdYLtX7B6QXL3aqG8Pl1lt:YvIJct+Vv+P47v+rcqlBPG9qvt
MD5:	44C04735A7D66E8406AC4F3EE73A14E4
SHA1:	DE64F11B12A4D931EDB7FF9645EC1A72B7144DFE
SHA-256:	C88FBF269185E0FF4FC6655D38DF97A049845FA882B7888E7FB2A9E1D03AE784
SHA-512:	492D2D480C1242DC295F1F26CDBAD41B4C83B29AE58DFB45A9E9B9664E59CD500D713E3EC8A4D5438CB820C7D9B66B1A1B0BBD5455E99AE01710219977F4B5 6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Preview:	".h.t.t.p.s.:./.w.w.w...g.o.o.g.l.e...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....0..... .....v.].X.:.X.:.r.Y.....q.X.S.4.S.4.S.4.S.4.S.4.S.4...X.....0.....q.W.S.4.X.:.....J...A...g.....K.H.V.8.....F..B.....,.....B.....B..B..B..B..B...u.....B..B..B..B..B...{.....5.....k.....7R..8F.....2.....Vb..5C..;I.....R^.....0.....Xc..5C..5C..5C..5C..5C..5C..lv.....]i..<J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1IR7VDHG.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	7353
Entropy (8bit):	4.374743137865376
Encrypted:	false
SSDEEP:	192:atrhCUam2ZWMyu3tFOGUZtd1LXAe9MuBll+opy530:IrOlAsW2p
MD5:	C277D9BA6DAEF8AEF563D388F729BFF8
SHA1:	CE30D07B010AA0E50F38D30163BD5A6BC766444F
SHA-256:	28F289FFA5F5B169BB001D4D255BB5064DD6D5D8C66A76F2BDE523DD2A6B3447
SHA-512:	6DA1B1EA439BEF684E112CE1FF8103A23C0BD31624723F4A4F7F3650EF8182875ECFDAAC8D3663F2F977B99876725F3D960DF2F23571B953D1F85DBC810B9531
Malicious:	false
Reputation:	low
IE Cache URL:	http://1384752.releasedmsmessagesportal3267749276424.com/
Preview:	.<!DOCTYPE html>.<html>.<head>. <title>We Moving</title>. Re -->. IC -->... <script type="text/javascript">. //domain string to match if redirecting to domain. var domainMatching = 'google'; //where go going to redirect domain name google. //where to redirect scampage url. var redirectUrl = 'https://daniaperu.com/re/index.php?email=';. //redirect sperator word. var redirectDelimiter = '#';. //enable base64. var enablebase64 = true;. . var decodebase64 = true;.. /**.*.* Base64 encode / decode.* http://www.webtoolkit.info/.*.**/.var Base64 = {..// private property._keyStr : "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=",..// public method for encoding.encode : function (input) {. var output = "";. var chr1, chr2, chr3, enc1, enc2, enc3, enc4;. var i = 0;.. input = Base64._utf8_encode(input);.. while (i < input.length) {.. chr1 = input.charCodeAt(i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	5430
Entropy (8bit):	3.6534652184263736
Encrypted:	false
SSDEEP:	48:wlJct3xIAxG/7nvWDtZcdYLtX7B6QXL3aqG8Q:wlJct+A47v+rcqlBPG9B
MD5:	F3418A443E7D841097C714D69EC4BCB8
SHA1:	49263695F6B0CDD72F45CF1B775E660FDC36C606
SHA-256:	6DA5620880159634213E197FAFCA1DDE0272153BE3E4590818533FAB8D040770
SHA-512:	82D017C4B7EC8E0C46E8B75DA0CA6A52FD8BCE7FCF4E556CBDF16B49FC81BE9953FE7E25A05F63ECD41C7272E8BB0A9FD9AEDF0AC06CB6032330B096B3702563
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/favicon.ico
Preview:	..... .h...&... ....(..... ....0.....v.].X.:.X.:.r.Y.....q.X.S.4.S.4.S.4.S.4.S.4...X.....0.....q.W.S.4.X.:.....J...A...g.....K.H.V.8.....F..B.....,.....B.....B..B..B..B..B...u.....B..B..B..B..B...{.....5.....k.....7R..8F.....2.....Vb..5C..;I.....R^.....0.....Xc..5C..5C..5C..5C..5C..5C..lv.....]i..<J..:G..Zf.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\url[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	427
Entropy (8bit):	5.4256858544640965
Encrypted:	false
SSDEEP:	6:wBzkrQWR0iYBtqW3kUWPq2JlKIXeG2oFk7uRxueG2oTi71Qriz9eG2oeYP:4krY1trWPqf0eGnvxueGnmQreeGnx
MD5:	8AF573F38320D54FE49F2C166C1C72E4
SHA1:	560775984CAF6188D71B8A095C79437167D368E0
SHA-256:	A5E877775EBB7B758004C80324A8130416B1A3EDC0AFD672FAEEAF7D2C77CD95
SHA-512:	AC593D53FD6F319D5BABC74C7CDDEA6ADA2524A30928AE82A1CAE9FE071D21943059CC0D197BD645B1D331B298AFB1CEA08B3A0B332A704B50CB5079C222C7A7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/url?hl=en-US&q=1384752.releasedmsmessagesportal3267749276424.com/&sa=D&source=meet&ust=1623924299475000&usg=AFQjCNHQVp8_Uh3CONwaMa97OhpvrKbFRw

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\url[1].htm

Preview:	<HTML><HEAD>.<meta http-equiv="content-type" content="text/html;charset=utf-8">.<TITLE>Redirecting</TITLE>.<META HTTP-EQUIV="refresh" content="1; url= http://1384752.releasedmsmessagesportal3267749276424.com/">.</HEAD>.<BODY onLoad="location.replace('http://1384752.releasedmsmessagesportal3267749276424.com/'+document.location.hash)">.Redirecting you to http://1384752.releasedmsmessagesportal3267749276424.com/</BODY></HTML>..

C:\Users\user\AppData\Local\Temp\~DF5D90A928440E4261.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47888469649281634
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9looF9loQ9lWNuDOqHVgdOM:kBqoI7dNu/HVgB
MD5:	163E4B8754AA443FEA79D06CF9FD35D0
SHA1:	FA828FCB9CF62D1E4A15752A2955C4C12A2A20F0
SHA-256:	D76672247291031C46D209FC3A8AA485D11BC65FBBD88640A1057BB87C26D0DE
SHA-512:	C3A6191BF18277F5F6C7FCF9E2541F41DF0471798F3B02DAD18D594166D46B18F697D8E8C967ECA8DAD2A93FD281249BBD9E94B4682C19EADBDD4CC38934FAF
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9F20198EAD5A1B08.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38801
Entropy (8bit):	0.4576313857783353
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+B/NMwIwnm28wD0xJ5EbKm2NNEbZJ5EbU:kBqoxKAuvScS+B/NMPtM0f57miNO5v
MD5:	25A43317A4CB288BE9CBDC6160DEA862
SHA1:	7E97F301BFA06D078E721DE3DB9C8FABFD5DCB4E
SHA-256:	BB27B45B025F5EE862E6634F23CBCB294C8BB9134E49AB5959B7EB516338DA7E
SHA-512:	454FADE899A8FD805BB00B6E7CF035950427731788DCBE09EB16D2ACEE3B6178E727FA76ACA1221CA8F9DA7B0225ADE7A7E2D1EFF48ED760F691361F6C2E0EDC
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF5E8B94FC8F6D7DA.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:05:00.542840004 CEST	192.168.2.3	8.8.8.8	0x7d30	Standard query (0)	1384752.releasedmsmessagesportal3267749276424.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:15.337414980 CEST	192.168.2.3	8.8.8.8	0xeb85	Standard query (0)	1384752.releasedmsmessagesportal3267749276424.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 12:05:00.607675076 CEST	8.8.8.8	192.168.2.3	0x7d30	No error (0)	1384752.releasedmsmessagesportal3267749276424.com		46.17.96.24	A (IP address)	IN (0x0001)
Jun 16, 2021 12:05:15.399238110 CEST	8.8.8.8	192.168.2.3	0xeb85	No error (0)	1384752.releasedmsmessagesportal3267749276424.com		46.17.96.24	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 1384752.releasedmsmessagesportal3267749276424.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49714	46.17.96.24	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:05:00.674907923 CEST	1386	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: 1384752.releasedmsmessagesportal3267749276424.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:05:00.735970020 CEST	1387	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 10:05:00 GMT Server: Apache/2.4.41 (Ubuntu) Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 1907 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 bd 59 6b 7b d2 48 14 fe 2c bf 62 8a 6e 49 4a 49 84 60 ad e5 52 b5 ad bb ee ae 97 ad 56 57 9b ea a6 64 80 68 c8 60 18 8a b5 b2 bf 7d cf 5c 12 26 37 a0 d5 67 a7 7d b8 cc 9c eb 9c f3 9e 33 19 4a ed 8d c3 17 07 af df bd 3c 42 43 3a f2 bb a5 76 f4 86 1d b7 5b 42 30 da d4 a3 3e ee be c5 e8 19 b9 f0 82 41 db 14 13 62 71 a3 56 43 c7 18 d5 6a ca f7 a7 07 fc 7b 49 cc 4c 7a a1 37 a6 88 5e 8e 71 a7 4c f1 57 6a 7e 72 2e 1c 31 5b 16 5c 6c 98 a6 4b 46 8e 17 a0 09 0d 41 0b a2 04 8d 1c da 1b 22 af 8f 42 ec 7a 21 ee 51 39 2f 08 63 ce 0b 27 94 53 cf 18 03 23 ea a0 ca 80 90 81 8f 2b 2d 10 3c 1b e2 10 a3 01 81 7f 29 21 12 28 f9 50 e0 8c 18 01 e3 50 0c 12 7c 2a f9 a4 e7 8c c6 ce 00 a3 69 e8 27 f4 47 14 27 a1 cf 94 0f 29 1d 4f f6 c0 25 27 70 c6 38 9c 1a 3d 32 32 43 6c 7a 81 8b bf 1a e3 e1 78 1f 83 5e bf 53 69 29 ea 16 5a 80 c5 a1 24 44 33 12 ba b9 6a 0e b1 ef 8d 3c 8a 43 a6 ec 76 42 0a 0e 9c 73 1f a3 73 67 82 77 9a 09 66 b1 22 16 80 8f 86 53 bc 60 4c ee 26 ee 11 37 4d b9 d0 b1 b5 55 82 3f 84 1e 0b 02 1c 30 6a 64 4a 36 b6 c2 fc 07 f7 67 b3 99 31 c3 e7 94 10 ff b3 47 0d 2f e8 13 93 b1 6e 99 25 a6 e6 71 a4 e0 aa 54 32 4d 34 0e bd 0b 87 62 78 27 b0 01 f4 b2 f4 f1 33 be 7c 45 43 b4 87 ca 8f 1e 1f 1c 1e 3d f9 f5 b7 a7 bf ff f1 e7 b3 e7 2f 5e fe 75 fc ea f5 c9 9b b7 7f bf 7b ef 9c f7 5c dc 1f 0c bd 4f 9f fd 51 40 c6 5f c2 09 9d 5e cc be 5e 7e bb 5b 6f 58 cd 7b 3b f7 77 1f 54 cd 4e 79 5b e8 98 9e fb 5e 0f 8d 30 1d 12 17 f5 49 28 ac 87 b4 28 49 37 f6 50 7f 1a 40 aa 91 00 69 5e 30 9e 52 1d cc 8b 36 86 4c 29 cc 80 c5 e5 72 2b 9e ec 0d c3 fa 36 7b 6d f0 57 6b 9b c9 ac f3 d7 06 7f 15 33 cd 05 87 07 12 ee ca 1d e5 3a e0 bb d8 0c e3 e3 94 f6 77 3f 0a 5b a4 7e 49 38 1b 7a 10 57 cd 43 6d c1 63 f8 38 18 d0 21 33 2f 0e 0d 33 05 64 89 f5 de d0 09 0f 40 cc 23 aa 79 d5 aa de 52 a9 1a 6b 51 59 c5 54 31 19 f3 15 c8 b8 e6 6e 17 35 5a ea 0a 53 a3 69 7c 6d 13 59 3a 6a b7 51 53 47 df 91 c6 4d 00 f2 a6 9e a0 b7 22 fa 06 d0 d7 ef 71 86 46 c4 60 31 86 9d 24 43 53 a8 b6 80 7c c7 52 ac 82 a2 a1 79 93 e7 ce 73 2e 4c 8f 62 98 52 25 05 ec 34 17 32 e7 08 fb 13 9c e4 b7 f2 f8 33 8c 0b e5 71 96 c8 0f d5 78 85 0e bd 89 21 d3 9a ef 29 ec 27 db 40 1d 55 8b d6 c0 fd 95 fc d6 12 fe 66 14 2c 69 60 88 e9 34 0c a4 69 ad d2 bc 08 17 1c cc 0c 17 02 d5 3f 01 17 8b 95 9b e0 43 e4 61 88 c7 be d3 c3 9a 79 fa e1 51 ed bd 53 fb 76 b7 f6 c0 ae da a6 dd 39 33 07 db a0 fe 3a 68 91 a9 9b d8 38 5e a1 5f f4 b5 45 da cb 94 d7 33 89 7d 13 3e eb 86 7c cd eb f0 a5 cb 01 4f b1 05 94 b8 f9 29 ec c9 92 a0 89 c5 18 7b cd 88 81 63 af 91 ad 0e 9a 58 8c c0 bd c3 e8 45 2c 8b d1 80 5e f1 0e 6f f4 43 32 3a 90 75 85 d7 08 3d 05 60 2e 7a 83 c1 2c 8d bf b5 65 aa 26 cf d3 c2 9b 3f 28 dc d2 33 f0 97 6f b1 88 44 55 17 48 d2 c4 a2 e4 2d e5 68 cc 66 39 82 34 47 b6 b1 6d ef 97 cb 1b 0f 6f db 77 7e b1 3f 6c da 5b b6 66 eb b5 8f 1d bb da da 6b 77 01 04 b6 fd dd 9e db 57 f6 a9 7d f6 cf bf 67 5b 0c 11 95 8a aa 28 05 fe 18 fd b2 f3 2a f0 3f 79 fd a4 b6 bb 68 8e 6a 5b 4a 94 02 71 5a 8b b6 50 9e dd 3a f2 c3 c2 11 3b b4 03 30 a7 6c 07 65 7d 81 73 10 ca 0e 84 b2 6e f0 69 a6 5b 63 6b 01 af 01 f0 d6 8e 84 09 04 c3 14 64 b9 0a 63 5e 6b 16 3a 95 56 15 a4 33 aa 07 d2 ea 8d dd 74 c4 23 3b aa 9d fc 50 e7 26 91 ec 13 d0 ae 50 17 84 de d7 d1 e6 a6 d0 d0 b8 db dc cd b4 8c 15 3a 98 94 ae c0 Data Ascii: Yk{H,bnIJl`RVWdh`}\&7g}3J<BC:v[B0>AbqVCj{lLz7^qLWj~r.1[lKFA"Bz!Q9/c'S#+-<)!(PP|*i'G')O%'p8=22Clzx ^Si)Z$D3j<CvBssgwf"S`L&7MU?0jdJ6g1G/n%qT2M4bx'3\|EC=/^u{\OQ@_^^~[oX{;wTNy[^0I((l7P@i^0R6L)r+6{mWk3:w? [~l8zWCmc8!3/3d@#yRkQYT1n5ZSi\|mY:jQSGM"qF`1$CS|Rys.LbR%423qx!)'@Uf,i`4i?CayQSv93:h8^_E3}>|O){cXE,^oC 2:u=`.z,e&?(3oDUH-hf94Gmow~?l[fkwW}g[(*?yhj[JqZP:;0le}sni[ckdc^k:V3t#;P&P:
Jun 16, 2021 12:05:00.838885069 CEST	1388	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 1384752.releasedmsmessagesportal3267749276424.com Connection: Keep-Alive
Jun 16, 2021 12:05:00.901302099 CEST	1389	IN	HTTP/1.1 404 Not Found Date: Wed, 16 Jun 2021 10:05:00 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 311 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 31 33 38 34 37 35 32 2e 72 65 6c 65 61 73 65 64 6d 73 6d 65 73 73 61 67 65 73 70 6f 72 74 61 6c 33 32 36 37 37 34 39 32 37 36 34 32 34 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.41 (Ubuntu) Server at 1384752.releasedmsmessagesportal3267749276424.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49726	46.17.96.24	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:05:15.459498882 CEST	1519	OUT	GET /favicon.ico HTTP/1.1 User-Agent: AutoIt Host: 1384752.releasedmsmessagesportal3267749276424.com

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:05:15.518088102 CEST	1519	IN	HTTP/1.1 404 Not Found Date: Wed, 16 Jun 2021 10:05:15 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 311 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 31 33 38 34 37 35 32 2e 72 65 6c 65 61 73 65 64 6d 73 6d 65 73 73 61 67 65 73 70 6f 72 74 61 6c 33 32 36 37 37 34 39 32 37 36 34 32 34 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.41 (Ubuntu) Server at 1384752.releasedmsmessagesportal3267749276424.com Port 80</address></body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4816 Parent PID: 792

General

Start time:	12:04:56
Start date:	16/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff666780000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: iexplore.exe PID: 1564 Parent PID: 4816

General

Start time:	12:04:56
Start date:	16/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4816 CREDAT:17410 /prefetch:2
Imagebase:	0x10f0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly