ID: 413042
Cookbook: browseurl.jbs
Time: 06:51:59
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

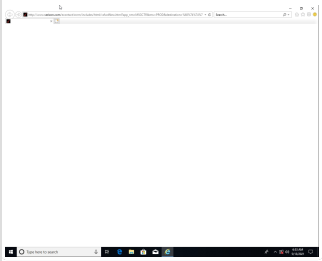
Analysis Report http://www.verizon.com/econtact/ecrm/…

Overview

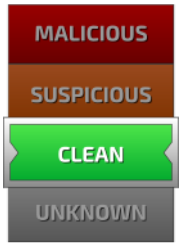
General Information

Sample URL:	www.verizon.com/econtact/ecrm/includes/html/vzfwdNew.html?app_nm=MSGCTR&env...6abea7e%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5
Analysis ID:	413042
Infos:	

Most interesting Screenshot:



Detection

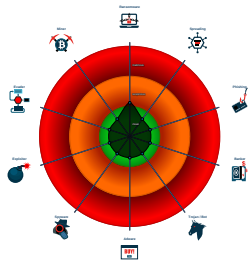


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 2924 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5524 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2924 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

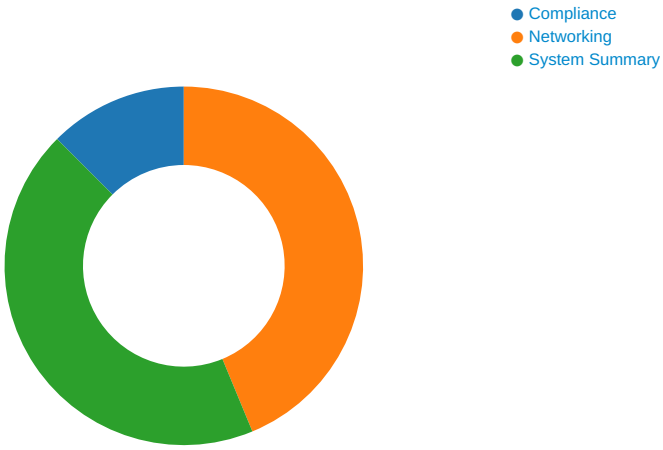
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



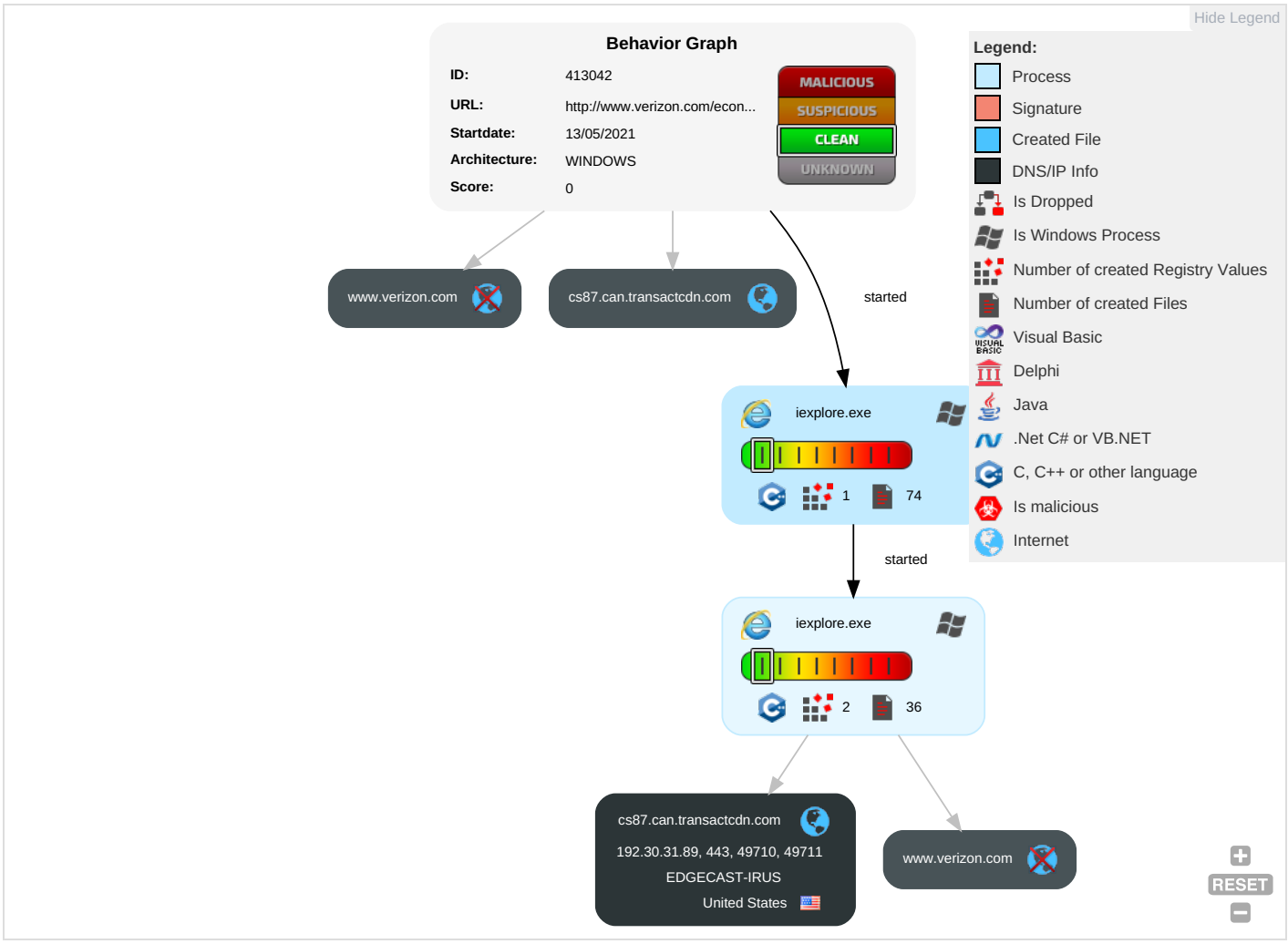
Click to jump to signature section

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	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	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
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 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
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 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 2	SIM Card Swap		Carri Billin Fraud

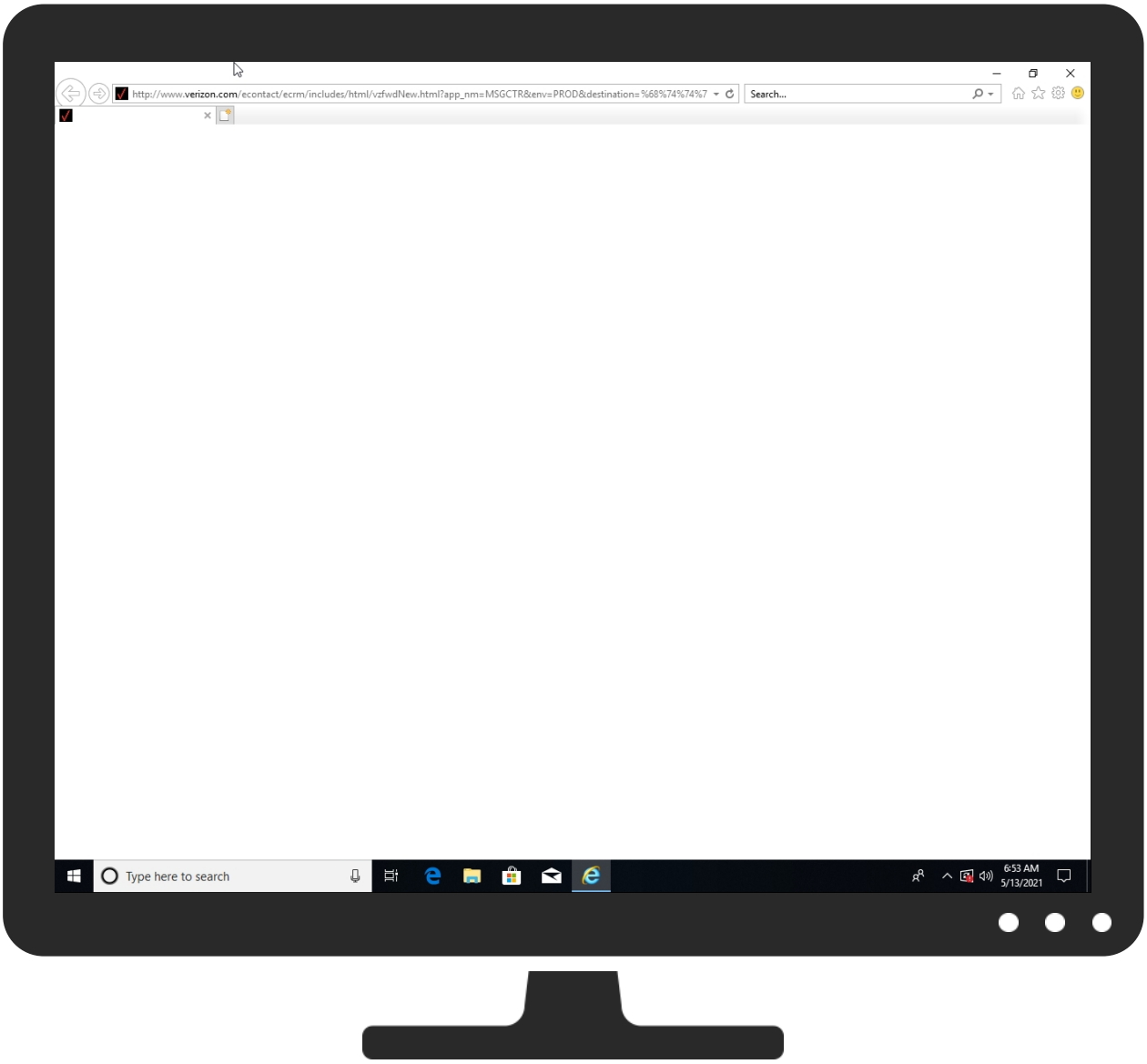
Behavior Graph



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://www.verizon.com/econtact/ecrm/includes/html/vzfwdNew.html?app_nm=MSGCTR&env=PROD&destination=%68%74%74%70%73%3A%2F%2%20Fnandorinha.fr/folder/ac4e-6b7a-4f8c-bd00-1aeb26abea7e%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5<id=0	0%	Virustotal		Browse
http://www.verizon.com/econtact/ecrm/includes/html/vzfwdNew.html?app_nm=MSGCTR&env=PROD&destination=%68%74%74%70%73%3A%2F%2%20Fnandorinha.fr/folder/ac4e-6b7a-4f8c-bd00-1aeb26abea7e%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5<id=0	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs87.can.transactcdn.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs87.can.transactcdn.com	192.30.31.89	true	false	• 0%, Virustotal, Browse	unknown
www.verizon.com	unknown	unknown	false		high

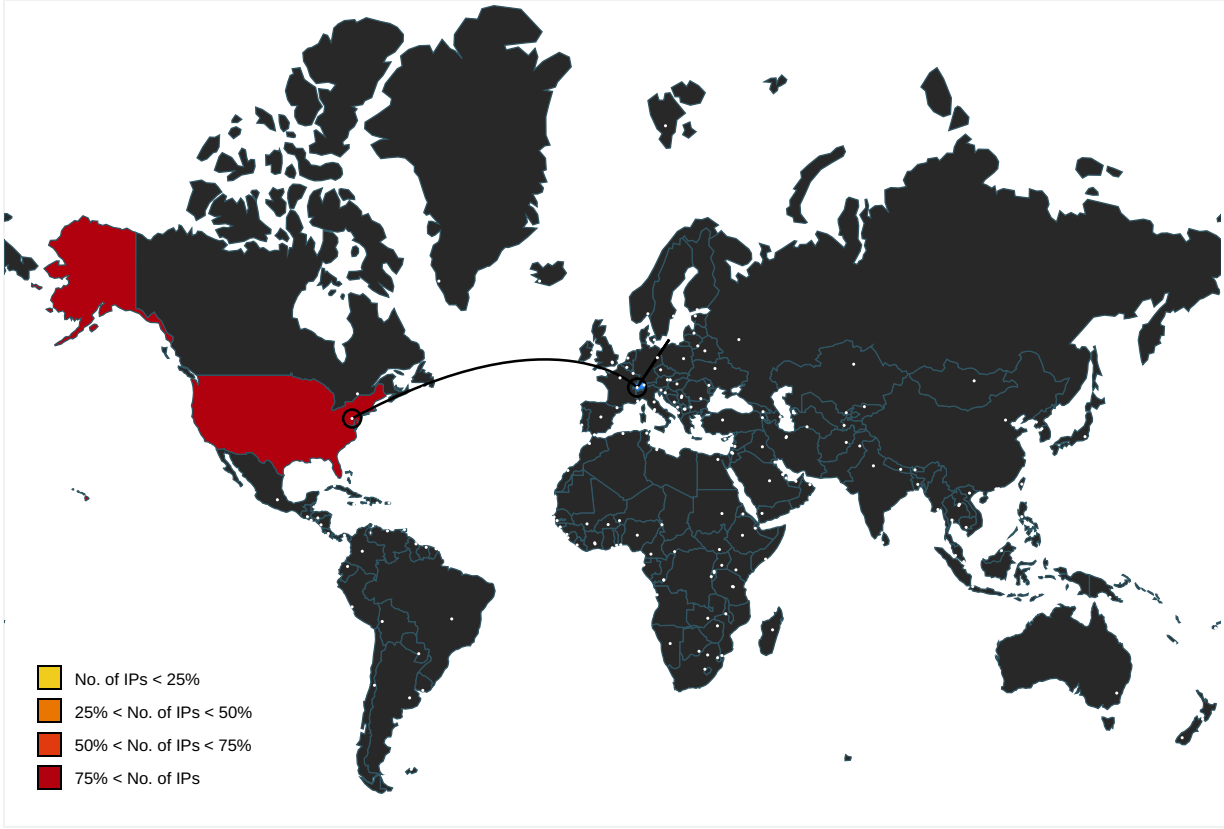
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.verizon.com/econtact/ecrm/includes/html/vzfwdNew.html?app_nm=MSGCTR&env=PROD&destination=%68%74%74%70%73%3A%2F%2%20Fnandorinha.fr/folder/ac4e-6b7a-4f8c-bd00-1aeb26abea7e%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5<id=0	false		high
http://www.verizon.com/econtact/ecrm/includes/html/favicon.ico	false		high
http://www.verizon.com/econtact/ecrm/includes/html/vzfwdNew.html?app_nm=MSGCTR&env=PROD&destination=%68%74%74%70%73%3A%2F%2%20Fnandorinha.fr/folder/ac4e-6b7a-4f8c-bd00-1aeb26abea7e%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5<id=0	false		high
http://www.verizon.com/econtact/ecrm/includes/js/webtoolkit.url.js	false		high
http://www.verizon.com/favicon.ico	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dcrmsitaws.ebiz.verizon.com/ecrm/linktrack/LinkTrackingServlet.serv?	vzfwdNew[1].htm.2.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://https://www.verizon.com/econtact/survey/ecrm/linktrack/LinkTrackingServlet.serv?	vzfwdNew[1].htm.2.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://www.verizon.com/econtact/ecrm/includes/html/vzfwdNew.html?app_nm=MSGCTR&env=PROD&destination=	{816E8D6D-B3F2-11EB-90E5-ECF4BB570DC9}.dat.1.dr, ~DF6D75612F67477265.TMP.1.dr	false		high
http://www.verizon.com	vzfwdNew[1].htm.2.dr	false		high
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://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.verizon.com/favicon.ico6	imagestore.dat.2.dr	false		high
http://www.webtoolkit.info/	webtoolkit.url[1].js.2.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://www.verizon.com/econtact/ecrm/linktrack/LinkTrackingServlet.serv?	vzfwdNew[1].htm.2.dr	false		high
http://www98.verizon.com/econtact/ecrm/linktrack/LinkTrackingServlet.serv?	vzfwdNew[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.30.31.89	cs87.can.transactcdn.com	United States		14153	EDGECAST-IRUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413042
Start date:	13.05.2021
Start time:	06:51:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.verizon.com/econtact/ecrm/includes/html/vzfwdNew.html?app_nm=MSGCTR&env=PROD&destination=https%3A%2F%2 Fnandorinha.fr/folder/ac4e-6b7a-4f8c-bd00-1aeb26abea7e%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5<id=0
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:	16
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:	CLEAN
Classification:	clean0.win@3/19@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.{816E8D6B-B3F2-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.844373475280905
Encrypted:	false
SSDEEP:	96:r1EZ3FZG423W+txbfs3gKMIlqcuQlxfA316X:r1EZ3FZG423W+tlfsVMJODfA8X
MD5:	08A73E8ACA75294E96BE84554B32264E
SHA1:	079ECC075B69AC5431C8184E1B3662922F87B21E
SHA-256:	39DA10B655172D54B0ACFF6D99330D4DEFDD778EF88D44CE6CDD37CCD158C430
SHA-512:	5375EC83BBEAF120A5302B01AF280CA60EFCA9B61004464B80FC14C78DC92F02EAFEB2875E9C1736FCE45E1055E442D4BF2A4CDA8BEA87B52803590ECEA1FF 79
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\{816E8D6D-B3F2-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{816E8D6D-B3F2-11EB-90E5-ECF4BB570DC9}.dat	
Category:	dropped
Size (bytes):	24612
Entropy (8bit):	1.7136430477539015
Encrypted:	false
SSDEEP:	48:IwVGcprvGwpa3G4pQbGrapbSVGQpBTGHHpc1kTGUp81/GzYpm1/TGopUb/jsjDd1:rLZZQ56PBSfjW21cW1NM1dGbYjDdPtMg
MD5:	7607AAE67BA2635D3C25B8FA23FB36A8
SHA1:	79711331EF1EA7C1D6A854E3D23100A8EE7E26DD
SHA-256:	9C6691C99E3595DC08165CA583F0ED3F0A9D15F0BB16D3B7BEF29DA6AADC1C4A
SHA-512:	A0EB2D7640DCD1B1BFD2F87817D6FA235BA8CF0A39FEFB0FCB3E03F0533EF2F39A6D7F458DC1BEBE030D574935DC2D75D6390E3E38C691DE72B1E79427E42(84
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\{816E8D6E-B3F2-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5611310082278154
Encrypted:	false
SSDEEP:	48:IwRGcprAGwpaQG4pQsGrapbS1GQpK/G7HpRBTGIpG:rnZIQQ6qBS/AOTXA
MD5:	0592A205B593D971BD468B5A9BFB6D39
SHA1:	1F9570B0868965F361074CD67164FEAF4C95CDF6
SHA-256:	5BD0193720EF01663668859BC37CA033D60336B9D308ADED91D7CA4F98298C21
SHA-512:	7589CBFDE68A73D25AED29758171AAD796977868CB8C5F39FE8AFAB7543A4EA50CCB0EEC8CBDFF5901AD6E2C8EA22065236CC5F1B3872732CB1B01448EAE1 A5
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):	5.114429369991024
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEpryOreCnWimI002EtM3MHdNMNxOEpryOreCnWimI00ONVbkEtMb:2d6NxOXCSZHKd6NxOXCSZ7Qb
MD5:	C2A06803E53224C619D44CF6CA8CD99F
SHA1:	66D033DE6A875E5FD50E9BBCFA13927047F35D29
SHA-256:	736EEAAE608DC211A41F695174C27F8236E8AB7E5E1AAD67083EDCE66D07233C
SHA-512:	BAE748336963E98A44BC36F2EAD1BF6AACD56B3CD9FF52701394523BFB53D78AE58970492507DD362F15700D68299637A2A01474798D0551EDED8464EF58382B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x57236f9c,0x01d747ff</date><accdate>0x 57236f9c,0x01d747ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml ver sion="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x57236f9c,0x01d747ff</date><accdate>0x57236f9c, 0x01d747ff</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msappli cation></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):	5.123800201837835
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2khyseCnWimI002EtM3MHdNMNxe2khyseCnWimI00ONkak6EtMb:2d6NxrHCSZHKd6NxrHCSZ72a7b
MD5:	D1F092B4BE74BB240B2C01A90A1F9D3A

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SHA1:	676B2ADB28ABA953CEE857C01C6E647B8DF71C8C
SHA-256:	2684863408B3BD7E5C0D7559C9DC4581BCDF120235D9C7FF3FA0CD519753897F
SHA-512:	D0C1A8BEA1C937FF47F83C7E2C91ADB6F12010B279EF0021A4917E5742AD5A7CD0321E8C9FFC213FAC5DF36CA6B282B4E157AAAEF6105B355B5125AA9CB35F3D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x571c4889,0x01d747ff</date><accdate>0x571c4889,0x01d747ff</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>0x571c4889,0x01d747ff</date><accdate>0x571c4889,0x01d747ff</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):	5.089397043273909
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLmyreCnWimI002EtM3MHdNMNxvLmyreCnWimI00ONmZEtMb:2d6NxvKCSZHKd6NxvKCSZ7Ub
MD5:	19AAA86CF982DE04B8B0F9D82E8E3533
SHA1:	72E3B55A52AE2B736D4D690C2BDC2A43854534B0
SHA-256:	417CC1D80EE4D4C20ECC88E6A17D01474D9AAFFCE774116E90873FF4FEE4E5AF
SHA-512:	FFACC3F9C3B5D013598AD9D8C183B989CBF238B8AC18772EB98C480D3E9A178580821C30BAD919910861FDCAEBDFEF347692180C7132E27574E812D4FF4AF12
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x5725d1e1,0x01d747ff</date><accdate>0x5725d1e1,0x01d747ff</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>0x5725d1e1,0x01d747ff</date><accdate>0x5725d1e1,0x01d747ff</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):	5.085978715544124
Encrypted:	false
SSDEEP:	12:TMHdNMNxi7y2eCnWimI002EtM3MHdNMNxi7y2eCnWimI00ONd5EtMb:2d6NxVCSZHKd6NxVCSZ7njb
MD5:	4C350BCA564B65F0947473504A453B95
SHA1:	7B9A75E64219AE5D5F79880E4CF77D047A4EBDDC
SHA-256:	6422EFEDEC6539279A55DFD6408AA709053BEA4B43A9A6F45323B57A8F398E63
SHA-512:	DD25D39A4B51C60B2B6FBDAA80DF4071F6E12B7318BB7A7CD5DE9AAA302DAFD7895205C76B7D5E47E3457F5400917AEFF59F566950C9D06109E86419BABBE47
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x57210d40,0x01d747ff</date><accdate>0x57210d40,0x01d747ff</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>0x57210d40,0x01d747ff</date><accdate>0x57210d40,0x01d747ff</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):	5.104703063981266
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwmyreCnWimI002EtM3MHdNMNxhGwmyreCnWimI00ON8K075EtMb:2d6NxQdCSZHKd6NxQdCSZ7uKajb
MD5:	4865BA3A00023F4AD6C8D918F791CFF3
SHA1:	655B2B43320D88BE3E84E975F58BE0FB5DAE07EF
SHA-256:	423681C1D4777A99D11547DBE0A93AF0F1327CF593D4E47C5E8FE0C07DAE166D
SHA-512:	CC206655D13FF54CF5E00B21378685502453E34D4930E314F12CACCCBF5850B4DCF67CD72B675C40D47209FB1F0A15ED2983FE8352400FF6A626D18EF9BB613

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x5725d1e1,0x01d747ff</date><accdate>0x5725d1e1,0x01d747ff</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>0x5725d1e1,0x01d747ff</date><accdate>0x5725d1e1,0x01d747ff</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):	5.118269778158012
Encrypted:	false
SSDEEP:	12:TMHdNMNx0npryOreCnWimI002EtM3MHdNMNx0npryOreCnWimI00ONxEtMb:2d6Nx0YCSZHKd6Nx0YCSZ7Vb
MD5:	18106F12E9C1F1280DA7E1C22A0706DB
SHA1:	0FAD5F9C0B865825B85594AB8318E292078E0B84
SHA-256:	DFEDAB4BE48BF7C8D4DABCB59375547332FEA67C9C96BEEFD3464064FFAB280D
SHA-512:	100A049126C6830ACCA1EBFC6529B0953C9A2116F5B5A419022AF3334F815880A59E6E1AC80F0CB5856C0F0ED8E5BB86B403D8A95C54EC2B05F040477E81DB2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x57236f9c,0x01d747ff</date><accdate>0x57236f9c,0x01d747ff</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>0x57236f9c,0x01d747ff</date><accdate>0x57236f9c,0x01d747ff</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):	5.129663080411459
Encrypted:	false
SSDEEP:	12:TMHdNMNxx7y2eCnWimI002EtM3MHdNMNxx7yOreCnWimI00ON6Kq5EtMb:2d6NxSCSZHKd6NxYCSZ7ub
MD5:	296F23BBA7B130C7316F9E857C306D59
SHA1:	401EF833990DFBFB0D9DBE8B94A3DCD1151E0676
SHA-256:	2D0D5EEFE93162841E4D60F61AD03CBDAB0605071F53CE10C00AD4F84B31C13C
SHA-512:	7EB520FBFBD8371199B7B66B08AD98C4173E2D20CBD43C3F112E462681FC81BC28B869082E499EC3892F96DB5D61F1754042E71421327DD86B8CBF0D6732593
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x57210d40,0x01d747ff</date><accdate>0x57210d40,0x01d747ff</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>0x57210d40,0x01d747ff</date><accdate>0x57236f9c,0x01d747ff</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):	5.071741807226985
Encrypted:	false
SSDEEP:	12:TMHdNMNxcK8qy98qeCnWimI002EtM3MHdNMNxcK8qy98qeCnWimI00ONVEtMb:2d6Nx9CSZHKd6Nx9CSZ71b
MD5:	31CA6C958CA810224AC46BEE98AAAB78
SHA1:	9CC94ED42AC296ADDA3FD36BC82C3EA573C10938
SHA-256:	16EA0D20AB4878202782EC98F407934565A16BA12EBC136ACFAF678531B2D412
SHA-512:	B84DB6DD7B4F5193B6576A9648ACB3DE978AF95F56EDB441974046501BBD751C0EC36057510B598AA9CA6631B8EE013C99F6844F12821529143DA6FCE9ADC8C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x571eaad6,0x01d747ff</date><accdate>0x571eaad6,0x01d747ff</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>0x571eaad6,0x01d747ff</date><accdate>0x571eaad6,0x01d747ff</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):	5.071469147433025
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn7y2eCnWimI002EtM3MHdNMNxfn7y2eCnWimI00ONe5EtMb:2d6NxECSZHKd6NxECSZ7Ejb
MD5:	7B94EA0CD4A68F4D4B295F877AD1043E
SHA1:	F5775B21FF432DD2E74CE067C9D5B2D5217F88DF
SHA-256:	607A2F4A67463150D23D0A961D0D51651BC996721DBDA74FA062F4B470BC0B11
SHA-512:	9DF1D49A45A5833B461F42ACD60DDF0F602586C770F9AA13F6AEB434971562B5F6C22291746D386A8AB4251FB24DA1C0A7A09E2C1E15DB50B8BCDC1DCBCED 77
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x57210d40,0x01d747ff</date><accdate>0x57210d40,0x01d747ff</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>0x57210d40,0x01d747ff</date><accdate>0x57210d40,0x01d747ff</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:	modified
Size (bytes):	928
Entropy (8bit):	1.302717355074014
Encrypted:	false
SSDEEP:	6:+rWGlKlcAMlGdAlfWN2q/lcTd9dMNbNbNbj7mt:8plNfdq0
MD5:	6AE77088B4B1108AD5ED499E502F93D7
SHA1:	3EA6FAC966E862DA8CFF3D01C35F492D40DC8B16
SHA-256:	412C7EFE0E84E617C0BAC7507B87F626DCE1DC452CD53995097324A518D1B4E6
SHA-512:	7E5544C183EAC3570DE5474CB3FEBDC70444D84D26FCD85A4F5B0694F384749BABC2B06A73D89175EE77BEC8DECB1628D67249C0B5D5EB2D3574A5BF65D90 6E
Malicious:	false
Reputation:	low
Preview:	".h.t.t.p.:././.w.w.w...v.e.r.i.z.o.n...c.o.m./.f.a.v.i.c.o.n...i.c.o.6...BM6.......6...(...+..+...+..+...+..+..+..+......................................+..+.....+...................................+..+........+..+................................+..+........+..+................................+..............+..+...+..+...+..+..+..+...+..+..+..+...+..+...5/.`....5/.`....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\vzfwdNew[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12288
Entropy (8bit):	5.327218756201661
Encrypted:	false
SSDEEP:	192:7+Qc213305QQLN47DcfNbVlHnxdhPFpd6crmpwLd6crWuaBP/:7+Qc2133MQQh47DclbVlHnxdhPFpdZrg
MD5:	B02E821E0528B295E7F675193213E5D9
SHA1:	1C9CEBBEBFBF9EC14FA9B2DBF3209FDF9D6D2B8E
SHA-256:	277FBCB419FAC1127F81FA6EA9A373C2DC8151F467209829F3DEC5657CFE1F01
SHA-512:	ABE1F9F88EEE99F27D545942BB1B2957CF68582AA7D00EDDB04F49301B92A4D8B8FD630C64A3BF2004C7E26CBC0BABDBC7FA5A2FEF55DFB228F88590579A4E 81
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.verizon.com/econtact/ecrm/includes/html/vzfwdNew.html?app_nm=MSGCTR&env=PROD&destination=%68%74%74%70%73%3A%2F%2%20Fnandorinha.fr/folder/ac4e-6b7a-4f8c-bd00-1aeb26abea7e%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5<id=0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\vzfwdNew[1].htm	
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">..<html>..<head>..<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">..<title> </title>..<script type="text/javascript" src="../js/webtoolkit.url.js"></script>..<script type="text/javascript">.....var MAX_WAIT_TIME_MS = 3000;...../* Asynchronously calls PNP app server Link Tracking Servlet */...../* vzfwd.html */.....function callAppServer(query) {.....var xmlhttp;....if (window.XMLHttpRequest)....{ // code for IE7+, Firefox, Chrome, Opera, Safari.... xmlhttp=new XMLHttpRequest();....} else { // code for IE6, IE5.... xmlhttp=new ActiveXObject("Microsoft.XMLHTTP");....}.....var outcome = 'OK';....xmlhttp.open("POST", "https://www.verizon.com/econtact/ecrm/linktrack/LinkTrackingServlet.serv?" + query, true);....xmlhttp.onreadystatechange = function() {.. if (xmlhttp.readyState == 4 && xmlhttp.status == 200) {.. . outcome = xmlhttp.respon

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PC bitmap, Windows 3.x format, 16 x 16 x 24
Category:	downloaded
Size (bytes):	822
Entropy (8bit):	0.8765502306033963
Encrypted:	false
SSDEEP:	3:bRl9lslFlWNWxKx/lcTd9dMNbNbNb:bAlfWN2q/lcTd9dMNbNbNb
MD5:	17A3708551FA2B7540A7F5744295E50D
SHA1:	77609EDCE3E415EFC9CA2F02472D62ECAD05BBC6
SHA-256:	F0F64EDF261A2CC8FD6A78D11337DC61590A059578D2075BDCAC8500A1A72750
SHA-512:	31E8DC0F524A3293C83512B4B6C46E7F21ABB8C62CF856E8B881A5DEE665DFD796F47E141E11D9B90873032CE1C8C47F1965F60D1F7D2D7E36D4FC889554168
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.verizon.com/personal/favicon.ico
Preview:	BM6.....6...(.....+..+.....+..+.....+..+..+..+..... .....+..+.....+.....+..+.....+..+.....+..+.....+..+.....+..+.....+..+.....+..+..... .....+..+.....+..+.....+..+.....+..+.....+..+.....+..+..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\webtoolkit.url[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1660
Entropy (8bit):	5.095951651357762
Encrypted:	false
SSDEEP:	24:3ggCJ2Yir8yF8SMOUrK68rCTvOXAqF0dCBoHTagaIvXEuRNqCMwlh:3tYir8RrxTGA+oH+WIv1rDh
MD5:	3698851F84853A282507BF55C81C90A1
SHA1:	1F237972D27FA54A1137E2A084B481D0DE91AAD4
SHA-256:	F92EBF721CEDD80F2370F31111E654B437E06E6AF44C004B523BD199E56F3522
SHA-512:	B5A2F4397DBFCAE2B8B272B636AEB1B7CE225C2F8EC8E7AC2079FD968A7C2B623176F3344379CB9AAD4C2FA213EC5E2CFA5284FC2BECAFB856D0EFD16E542E47
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.verizon.com/econtact/ecrm/includes/js/webtoolkit.url.js
Preview:	/**..*..* URL encode / decode..* http://www.webtoolkit.info/..*..**/.. ..var Url = {.. .../// public method for url encoding...encode : function (string) {....return escape(this._utf8_encode(string));...},.. .../// public method for url decoding...decode : function (string) {....return this._utf8_decode(unescape(string));...},.. .../// private method for UTF-8 encoding..._utf8_encode : function (string) {....string = string.replace(/\r\n/g,"\n");....var utftext = "";.. ....for (var n = 0; n < string.length; n++) {.. .....var c = string.charCodeAt(n);.. .....if (c < 128) {.....utftext += String.fromCharCode(c);.....}.....else if((c > 127) && (c < 2048)) {.....utftext += String.fromCharCode((c >> 6)	192);.....utftext += String.fromCharCode((c & 63)	128);.....}.....else {.....utftext += String.fromCharCode((c >> 12)	224);.....utftext += String.fromCharCode(((c >> 6) & 63)	128);.....utftext += String.fromCharCode((c & 63)	128);.....}.. ....}.. ....return utftext;...},.. .../

C:\Users\user\AppData\Local\Temp\~DF208DEF91A3497C58.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4779545740292569
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo+T9lo+T9lW+uCRxeVexIXICC7Ve7E:kBqoI+U+K+uCxeExIXICC7E7E
MD5:	2B67019F4FAECC5E95112310D20C395B
SHA1:	5097FF8F7D4B9FF0A83C36CC5AA2C5043F33E0CF
SHA-256:	3925CC1E0492BF7C87E158B16AEF82C09CCC75B4B48431642AFAF783137040C0
SHA-512:	105929A737DE2B0AF3509A60024584D4E28C13751C092233D89F318CE9C77A3B2D436DFB3E40B6A62B74B9E94C1D04EEE24457CC1CA0DD62E90AF2D7B37F302
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF208DEF91A3497C58.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF6D75612F67477265.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34805
Entropy (8bit):	0.426485350684051
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+Ei1q1D1/I1/qb/jsjDdPtoh:kBqoxKAuvScS+Ei1q1D1w1SbYjDdPt0
MD5:	064BCA7078ED7363F3418C60217D2386
SHA1:	5973C41F784F1E6F1F31578CAE85FB412293CE0A
SHA-256:	3525E188E5B0403F6ABE3C93AE474C3DA05A3AD69B96639AD348A73050AFE451
SHA-512:	E58C45E4DBCFC9953045CAE84BC112CEE5C8FA4D44AA2398B6472840574F5FAAD5B3041A493001A8B86498A6EFB2084DF6479245825802CE6A4E2D0222DB2F1
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF73F5B5B6EE82AEDF.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

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:52:53.001055956 CEST	49710	80	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.001096964 CEST	49711	80	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.041866064 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.041896105 CEST	80	49710	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.041996956 CEST	49711	80	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.042054892 CEST	49710	80	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.042593956 CEST	49711	80	192.168.2.5	192.30.31.89

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:52:53.083285093 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.292612076 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.292644024 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.292663097 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.292717934 CEST	49711	80	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.292740107 CEST	49711	80	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.345866919 CEST	49711	80	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.387378931 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.792135000 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.792155981 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.792165995 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.792268991 CEST	49711	80	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.898958921 CEST	49711	80	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.910224915 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.939702034 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.940802097 CEST	80	49711	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.940922976 CEST	49711	80	192.168.2.5	192.30.31.89
May 13, 2021 06:52:53.951137066 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:53.951324940 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.040229082 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.044488907 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.081563950 CEST	443	49714	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.081690073 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.082329035 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.085315943 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.085485935 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.085531950 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.085568905 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.085572004 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.085594893 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.085598946 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.085645914 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.085736036 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.087148905 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.087184906 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.087224007 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.087244987 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.119563103 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.123315096 CEST	443	49714	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.123369932 CEST	443	49714	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.123447895 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.123495102 CEST	443	49714	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.123553038 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.123573065 CEST	443	49714	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.123631001 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.123636961 CEST	443	49714	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.123716116 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.124739885 CEST	443	49714	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.124805927 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.124819040 CEST	443	49714	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.124867916 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.128467083 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.130878925 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.133464098 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.161783934 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.162107944 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.171013117 CEST	443	49714	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.171125889 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.178142071 CEST	443	49714	192.30.31.89	192.168.2.5
May 13, 2021 06:52:54.178311110 CEST	49714	443	192.168.2.5	192.30.31.89
May 13, 2021 06:52:54.219346046 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:55.030807972 CEST	443	49713	192.30.31.89	192.168.2.5
May 13, 2021 06:52:55.031018019 CEST	49713	443	192.168.2.5	192.30.31.89
May 13, 2021 06:53:10.196899891 CEST	49719	80	192.168.2.5	192.30.31.89

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:53:10.237679005 CEST	80	49719	192.30.31.89	192.168.2.5
May 13, 2021 06:53:10.237812996 CEST	49719	80	192.168.2.5	192.30.31.89
May 13, 2021 06:53:10.237972975 CEST	49719	80	192.168.2.5	192.30.31.89
May 13, 2021 06:53:10.278645039 CEST	80	49719	192.30.31.89	192.168.2.5
May 13, 2021 06:53:10.679235935 CEST	80	49719	192.30.31.89	192.168.2.5
May 13, 2021 06:53:10.679322958 CEST	49719	80	192.168.2.5	192.30.31.89

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:52:43.115426064 CEST	53	65307	8.8.8.8	192.168.2.5
May 13, 2021 06:52:43.267436028 CEST	64344	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:43.327318907 CEST	53	64344	8.8.8.8	192.168.2.5
May 13, 2021 06:52:43.549571037 CEST	62060	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:43.598252058 CEST	53	62060	8.8.8.8	192.168.2.5
May 13, 2021 06:52:43.756352901 CEST	61805	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:43.814901114 CEST	53	61805	8.8.8.8	192.168.2.5
May 13, 2021 06:52:44.689474106 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:44.738120079 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 06:52:45.856559992 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:45.905173063 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 06:52:46.755719900 CEST	61733	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:46.804429054 CEST	53	61733	8.8.8.8	192.168.2.5
May 13, 2021 06:52:47.943487883 CEST	65447	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:47.996988058 CEST	53	65447	8.8.8.8	192.168.2.5
May 13, 2021 06:52:49.464818001 CEST	52441	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:49.517682076 CEST	53	52441	8.8.8.8	192.168.2.5
May 13, 2021 06:52:50.645354986 CEST	62176	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:50.694264889 CEST	53	62176	8.8.8.8	192.168.2.5
May 13, 2021 06:52:51.675924063 CEST	59596	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:51.736776114 CEST	53	59596	8.8.8.8	192.168.2.5
May 13, 2021 06:52:52.921271086 CEST	65296	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:52.991512060 CEST	53	65296	8.8.8.8	192.168.2.5
May 13, 2021 06:52:53.214195013 CEST	63183	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:53.267889977 CEST	53	63183	8.8.8.8	192.168.2.5
May 13, 2021 06:52:54.634458065 CEST	60151	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:54.685925007 CEST	53	60151	8.8.8.8	192.168.2.5
May 13, 2021 06:52:55.829817057 CEST	56969	53	192.168.2.5	8.8.8.8
May 13, 2021 06:52:55.878746033 CEST	53	56969	8.8.8.8	192.168.2.5
May 13, 2021 06:53:10.113632917 CEST	55161	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:10.161549091 CEST	54757	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:10.183742046 CEST	53	55161	8.8.8.8	192.168.2.5
May 13, 2021 06:53:10.222615957 CEST	53	54757	8.8.8.8	192.168.2.5
May 13, 2021 06:53:14.180011988 CEST	49992	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:14.243144035 CEST	53	49992	8.8.8.8	192.168.2.5
May 13, 2021 06:53:21.691133976 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:21.751271963 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 06:53:22.452790976 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:22.511131048 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 06:53:22.693180084 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:22.744829893 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 06:53:23.461847067 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:23.510818958 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 06:53:23.710779905 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:23.762413025 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 06:53:24.521812916 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:24.577253103 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 06:53:25.985274076 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:26.038570881 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 06:53:26.537219048 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:26.586036921 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 06:53:29.990562916 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:30.051325083 CEST	53	60075	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:53:30.537467957 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:30.586246014 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 06:53:33.797079086 CEST	64345	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:33.856121063 CEST	53	64345	8.8.8.8	192.168.2.5
May 13, 2021 06:53:38.490628958 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 06:53:38.549829960 CEST	53	57128	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 06:52:52.921271086 CEST	192.168.2.5	8.8.8.8	0x1500	Standard query (0)	www.verizon.com	A (IP address)	IN (0x0001)
May 13, 2021 06:53:10.113632917 CEST	192.168.2.5	8.8.8.8	0xb9e5	Standard query (0)	www.verizon.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 06:52:52.991512060 CEST	8.8.8.8	192.168.2.5	0x1500	No error (0)	www.verizon.com	cs87.can.transactcdn.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 06:52:52.991512060 CEST	8.8.8.8	192.168.2.5	0x1500	No error (0)	cs87.can.transactcdn.com		192.30.31.89	A (IP address)	IN (0x0001)
May 13, 2021 06:53:10.183742046 CEST	8.8.8.8	192.168.2.5	0xb9e5	No error (0)	www.verizon.com	cs87.can.transactcdn.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2021 06:53:10.183742046 CEST	8.8.8.8	192.168.2.5	0xb9e5	No error (0)	cs87.can.transactcdn.com		192.30.31.89	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.verizon.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49711	192.30.31.89	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 06:52:53.042593956 CEST	1213	OUT	GET /econtact/ecrm/includes/html/vzfwdNew.html?app_nm=MSGCTR&env=PROD&destination=%68%74%74%70%73%3A%2F%2%20Fnandorinha.fr/folder/ac4e-6b7a-4f8c-bd00-1aeb26abea7e%2FVerizon&txid=B20200331_1488798683&lid=18207&tid=121811&vno=5&ltid=0 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/20100101 Firefox/12.0 Accept-Encoding: gzip, deflate Host: www.verizon.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 06:52:53.292612076 CEST	1214	IN	HTTP/1.1 200 OK Content-Encoding: gzip Accept-Ranges: bytes Cache-Control: private cdn-requestid: 552897254471553357123804889084094403 49 Content-Type: text/html; charset=UTF-8 Date: Thu, 13 May 2021 04:52:53 GMT Last-Modified: Wed, 09 Dec 2020 17:16:50 GMT ntCoent-Length: 12288 Server: Apache Set-Cookie: AkaSTrackingID=f29f62b627245ddda5eced1de6ea4cb3; path=/; domain=verizon.com; Secure; HttpOnly Set-Cookie: NSC_xxx22_fdpoubdu_mcw=ffffffff8f64858c45525d5f4f58455e445a4a4229a2;path=/;httponly x-ec-fail: no-zip-code x-ec-geoHdr: country_code=CH,region_code=ZH,city=Zurich,dma=-1,msa=-1,lat=47.4300,long=8.5718,zip=8152,continent=EU,timezone= Content-Length: 2328 Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 5a 7d 6f da 48 1a ff 9b 95 f6 3b 4c 5d 29 40 21 36 b4 bd db bd 12 5a e5 48 7a 8d 2e 94 a8 b8 db 9e 56 55 64 ec 21 b8 35 b6 77 3c 40 e8 6e bf fb 3d cf cc f8 0d db 24 a4 6d 5a 75 83 10 36 33 cf fb cb 6f 66 0c 07 f7 8e 46 03 f3 7f 67 c7 64 c6 e7 1e 39 7b fd ef d3 93 01 d1 f6 0d e3 cd a3 81 61 1c 99 47 e4 85 39 3c 25 8f f5 4e 97 98 cc f2 23 97 bb 81 6f 79 86 71 fc 52 23 da 8c f3 f0 89 61 ac 56 2b 7d f5 48 0f d8 85 61 be 32 50 d4 63 c3 0b 82 88 ea 0e 77 b4 a7 3f ff 74 80 63 e2 4a 2d 07 af 73 ca 2d d0 c9 c3 7d fa c7 c2 5d f6 b5 41 e0 73 ea f3 7d 73 1d 52 8d d8 f2 5b 5f e3 f4 92 0b 81 3d 62 cf 2c 16 51 de 7f 6d 3e df ff 55 08 e5 2e f7 e8 d3 3d 7f 12 85 bd 03 43 7e 83 e1 c8 66 6e c8 09 07 49 4a c0 7b 6b 69 c9 51 8d 44 cc ee 6b ba 6e bc 8f 8c 15 9d f0 20 f0 3e b8 5c 5f 30 4f 7f 1f 69 4f 0f 0c 49 77 a5 1c 20 f8 f9 a7 da d2 62 64 78 f8 f6 fc cd e1 89 79 6e 9e 0c 8f cf 87 63 d2 27 8f 3a 9d 4e 4f 10 18 0f c8 61 b4 f6 ed 19 0b fc 60 11 79 6b 62 5b 9e 17 91 b3 97 67 c4 0a 43 12 51 b6 a4 8c 9c ba fe 07 8c af fd c1 f5 2f c8 18 06 3d ca c9 03 03 24 48 21 cb 8f d3 95 a3 8b 24 c5 a3 d3 85 6f 63 32 84 c4 c3 30 44 2e ca 1a 7f 2c 28 5b 37 c9 9f a8 1e a8 84 89 97 73 0f 63 0d 26 d5 6a ee 94 34 56 ae ef 04 2b fd ed f0 f4 05 0c bf 82 14 d0 88 37 71 f6 4f 62 18 10 7d 87 92 69 c0 c8 c9 f1 2f ad 36 79 ee 32 3a 0d 2e db 64 00 5e cc 69 9b 8c 42 ca ac 36 19 5b 53 8b b9 c8 45 62 0d 7d 9f ae 48 5e 6c a3 29 d4 7e 22 d4 8b 28 d9 94 ff cf 36 7c fc a3 28 e3 10 5c 5b d2 b7 a3 c9 7b 6a f3 86 36 74 6d 16 44 c1 94 0b 9b 4d f3 4c 53 52 b3 5e 06 0b 6e 83 7d 10 ff fa e8 bf 75 31 af 44 ea 41 48 fd 86 76 36 1a 9b 5a 5b 56 6d a4 ca 16 42 e6 7e 0c 7c 1d 38 0d 8a 65 67 d9 1c 6e d8 dc f0 20 27 1c 53 62 60 76 e2 e4 a8 dc e8 98 b8 67 1a 69 11 11 ef 36 e1 6c 41 a5 4d 89 4e 9f 41 b1 af 23 6e 71 0a b5 eb 5f a0 65 71 d2 1a 22 43 24 79 61 56 e2 00 e8 82 6f 8c 7c a4 df 27 8f c9 de 5e 32 85 d2 16 11 0e 3f ec 74 48 93 64 a5 40 08 d3 10 a4 b2 a2 30 f0 23 6a 42 Data Ascii: Z}oH;L])@!6ZHz.VUd!5w<@n=$mZu63ofFgd9{aG9<%N#oyqR#aV+}Ha2Pcw?tcJ-s-}]As}sR[_=b,Qm>U.=C~fnIJ{kiQDkn >_0OiOIw bdxync':NOa`ykb[gCQ/=$H!$oc20D.,([7sc&j4V+7qOb}i/6y2:.d^iB6[SEb}H^l)~"(6|(\[{j6tmDMLSR^n}u1DAHv6Z[VmB~\|8egn 'Sb`vgi6lAMNA#nq_eq"C$yaVo|'^2?tHd@0#jB
May 13, 2021 06:52:53.345866919 CEST	1217	OUT	GET /econtact/ecrm/includes/js/webtoolkit.url.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko/20100101 Firefox/12.0 Accept-Encoding: gzip, deflate Host: www.verizon.com Connection: Keep-Alive Cookie: NSC_xxx22_fdpoubdu_mcw=ffffffff8f64858c45525d5f4f58455e445a4a4229a2
May 13, 2021 06:52:53.792135000 CEST	1223	IN	HTTP/1.1 200 OK Accept-Ranges: bytes cdn-requestid: 121035941846674083401501769618305932178 9 Content-Type: application/javascript Date: Thu, 13 May 2021 04:52:53 GMT Last-Modified: Wed, 19 Aug 2020 09:35:01 GMT Server: Apache Set-Cookie: AkaSTrackingID=f29f62b627245ddda5eced1de6ea4cb3; path=/; domain=verizon.com; Secure; HttpOnly x-ec-fail: no-zip-code x-ec-geoHdr: country_code=CH,region_code=ZH,city=Zurich,dma=-1,msa=-1,lat=47.4300,long=8.5718,zip=8152,continent=EU,timezone= Content-Length: 1660 Data Raw: 2f 2a 2a 0d 0a 2a 0d 0a 2a 20 20 55 52 4c 20 65 6e 63 6f 64 65 20 2f 20 64 65 63 6f 64 65 0d 0a 2a 20 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 65 62 74 6f 6f 6c 6b 69 74 2e 69 6e 66 6f 2f 0d 0a 2a 0d 0a 2a 2a 2f 0d 0a 20 0d 0a 76 61 72 20 55 72 6c 20 3d 20 7b 0d 0a 20 0d 0a 09 2f 2f 20 70 75 62 6c 69 63 20 6d 65 74 68 6f 64 20 66 6f 72 20 75 72 6c 20 65 6e 63 6f 64 69 6e 67 0d 0a 09 65 6e 63 6f 64 65 20 3a 20 66 75 6e 63 74 69 6f 6e 20 28 73 74 72 69 6e 67 29 20 7b 0d 0a 09 09 72 65 74 75 72 6e 20 65 73 63 61 70 65 28 74 68 69 73 2e 5f 75 74 66 38 5f 65 6e 63 6f 64 65 28 73 74 72 69 6e 67 29 29 3b 0d 0a 09 7d 2c 0d 0a 20 0d 0a 09 2f 2f 20 70 75 62 6c 69 63 20 6d 65 74 68 6f 64 20 66 6f 72 20 75 72 6c 20 64 65 63 6f 64 69 6e 67 0d 0a 09 64 65 63 6f 64 65 20 3a 20 66 75 6e 63 74 69 6f 6e 20 28 73 74 72 69 6e 67 29 20 7b 0d 0a 09 09 72 65 74 75 72 6e 20 74 68 69 73 2e 5f 75 74 66 38 5f 64 65 63 6f 64 65 28 75 6e 65 73 63 61 70 65 28 73 74 72 69 6e 67 29 29 3b 0d 0a 09 7d 2c 0d 0a 20 0d 0a 09 2f 2f 20 70 72 69 76 61 74 65 20 6d 65 74 68 6f 64 20 66 6f 72 20 55 54 46 2d 38 20 65 6e 63 6f 64 69 6e 67 0d 0a 09 5f 75 74 66 38 5f 65 6e 63 6f 64 65 20 3a 20 66 75 6e 63 74 69 6f 6e 20 28 73 74 72 69 6e 67 29 20 7b 0d 0a 09 09 73 74 72 69 6e 67 20 3d 20 73 74 72 69 6e 67 2e 72 65 70 6c 61 63 65 28 2f 5c 72 5c 6e 2f 67 2c 22 5c 6e 22 29 3b 0d 0a 09 09 76 61 72 20 75 74 66 74 65 78 74 20 3d 20 22 22 3b 0d 0a 20 0d 0a 09 09 66 6f 72 20 28 76 61 72 20 6e 20 3d 20 30 3b 20 6e 20 3c 20 73 74 72 69 6e 67 2e 6c 65 6e 67 74 68 3b 20 6e 2b 2b 29 20 7b 0d 0a 20 0d 0a 09 09 09 76 61 72 20 63 20 3d 20 73 74 72 69 6e 67 2e 63 68 61 72 43 6f 64 65 41 74 28 6e 29 3b 0d 0a 20 0d 0a 09 09 09 69 66 20 28 63 20 3c 20 31 32 38 29 20 7b 0d 0a 09 09 09 09 75 74 66 74 65 78 74 20 2b 3d 20 53 74 72 69 6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 28 63 29 3b 0d 0a 09 09 09 7d 0d 0a 09 09 09 65 6c 73 65 20 69 66 28 63 20 3e 20 31 32 37 29 20 26 26 20 28 63 20 3c 20 32 30 34 38 29 29 20 7b 0d 0a 09 09 09 09 75 74 66 74 65 78 74 20 2b 3d 20 53 74 72 69 6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 28 28 63 20 3e 3e 20 36 29 20 7c 20 31 39 32 29 3b 0d 0a 09 09 09 09 75 74 66 74 65 78 74 20 2b 3d 20 53 74 72 69 6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 28 28 63 20 26 20 36 33 29 20 7c 20 31 32 38 29 3b 0d 0a 09 09 09 7d 0d 0a 09 09 09 65 6c 73 65 20 7b 0d 0a 09 09 09 09 75 74 66 74 65 78 74 20 2b 3d 20 53 74 72 69 6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 28 28 Data Ascii: /**** URL encode / decode* http://www.webtoolkit.info/***/ var Url = { // public method for url encodingencode : function (string) {return escape(this._utf8_encode(string));}, // public method for url decodingdecode : function (string) {return this._utf8_decode(unescape(string));}, // private method for UTF-8 encoding_utf8_encode : function (string) {string = string.replace(/\r\n/g,"\n");var utftext = ""; for (var n = 0; n < string.length; n++) { var c = string.charCodeAt(n); if (c < 128) {utftext += String.fromCharCode(c);}else if((c > 127) && (c < 2048)) {utftext += String.fromCharCode((c >> 6) | 192);utftext += String.fromCharCode((c & 63) | 128);}else {utftext += String.fromCharCode((

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 06:52:53.898958921 CEST	1227	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/20100101 Firefox/12.0 Host: www.verizon.com Connection: Keep-Alive Cookie: NSC_xxx22_fdpoubdu_mcw=ffffffff8f64858c45525d5f4f58455e445a4a4229a2
May 13, 2021 06:52:53.940802097 CEST	1228	IN	HTTP/1.1 301 Moved Permanently cdn-requestid: 308580323872949650254027823752608343 72 Date: Thu, 13 May 2021 04:52:53 GMT Location: https://www.verizon.com/personal/favicon.ico Server: ECD (fcz/0E9C) Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49719	192.30.31.89	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 13, 2021 06:53:10.237972975 CEST	1277	OUT	GET /econtact/ecrm/includes/html/favicon.ico HTTP/1.1 User-Agent: AutoIt Host: www.verizon.com
May 13, 2021 06:53:10.679235935 CEST	1285	IN	HTTP/1.1 200 OK cdn-requestid: 8625937419218820951265045164476 4984857 Content-Type: image/vnd.microsoft.icon Date: Thu, 13 May 2021 04:53:10 GMT Server: Apache Set-Cookie: AkaSTrackingID=771866d4674850b9929612b433ca55e7; path=/; domain=verizon.com; Secure; HttpOnly Set-Cookie: NSC_xxx22_fdpoubdu_mcw=ffffffff8f64858c45525d5f4f58455e445a4a4229a2;path=/;httponly x-ec-fail: no-zip-code x-ec-geoHdr: country_code=CH,region_code=ZH,city=Zurich,dma=-1,msa=-1,lat=47.4300,long=8.5718,zip=8152,continent=EU,timezone= Content-Length: 0

HTTPS Packets

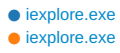
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 13, 2021 06:52:54.087184906 CEST	192.30.31.89	443	192.168.2.5	49713	CN=www.verizon.com, O="Verizon Digital Media Services, Inc.", L=Los Angeles, ST=California, C=US, SERIALNUMBER=C2891519, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 03 02:00:00 CEST 2021	Sun Nov 07 00:59:59 CET 2021	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=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

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 06:52:54.124819040 CEST	192.30.31.89	443	192.168.2.5	49714	CN=www.verizon.com, O="Verizon Digital Media Services, Inc.", L=Los Angeles, ST=California, C=US, SERIALNUMBER=C2891519, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 03 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Sun Nov 07 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028 Mon Nov 10 01:00:00 CET 2031	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=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 2924 Parent PID: 792

General

Start time:	06:52:50

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:	0x7ff62c240000
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: 5524 Parent PID: 2924

General

Start time:	06:52:51
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:2924 CREDAT:17410 /prefetch:2
Imagebase:	0x100000
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