ID: 358578
Cookbook: browseurl.jbs
Time: 21:36:25
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

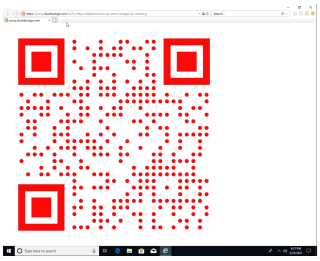
Analysis Report https://proxy.duckduckgo.com/iu/?u=ht…

Overview

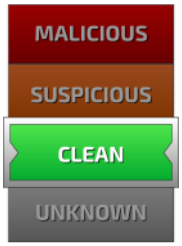
General Information

Sample URL:	http://https://proxy.duckduckgo.com/iu/?u=dataexhaust.io/wp-admin/images/qr-code.png
Analysis ID:	358578
Infos:	

Most interesting Screenshot:



Detection

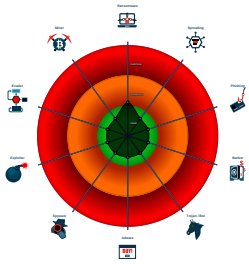


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6748 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6820 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6748 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

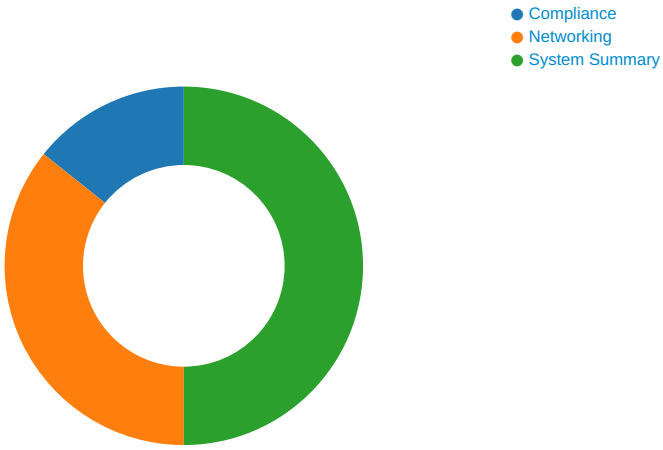
Yara Overview

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.

Compliance:

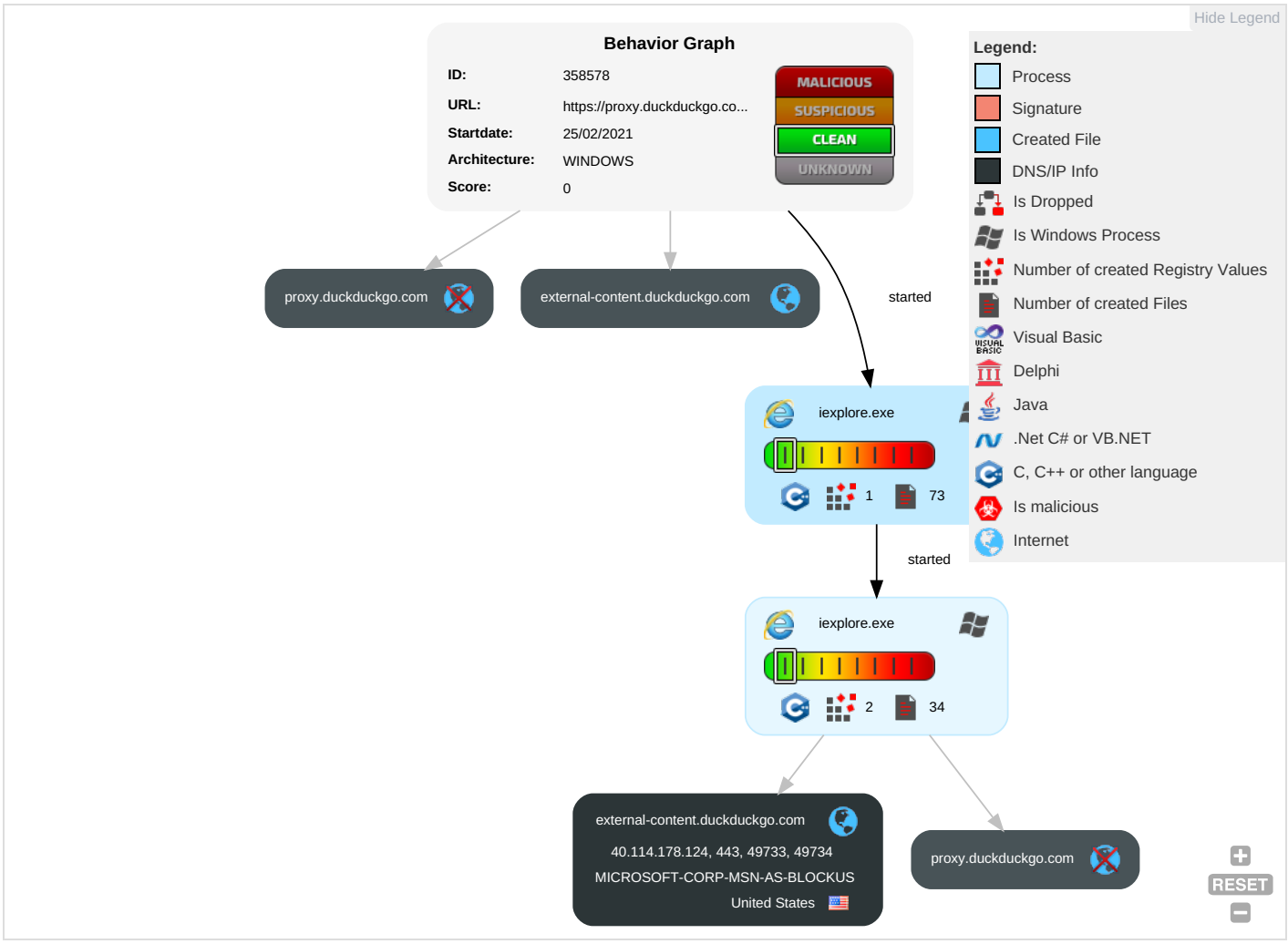
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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

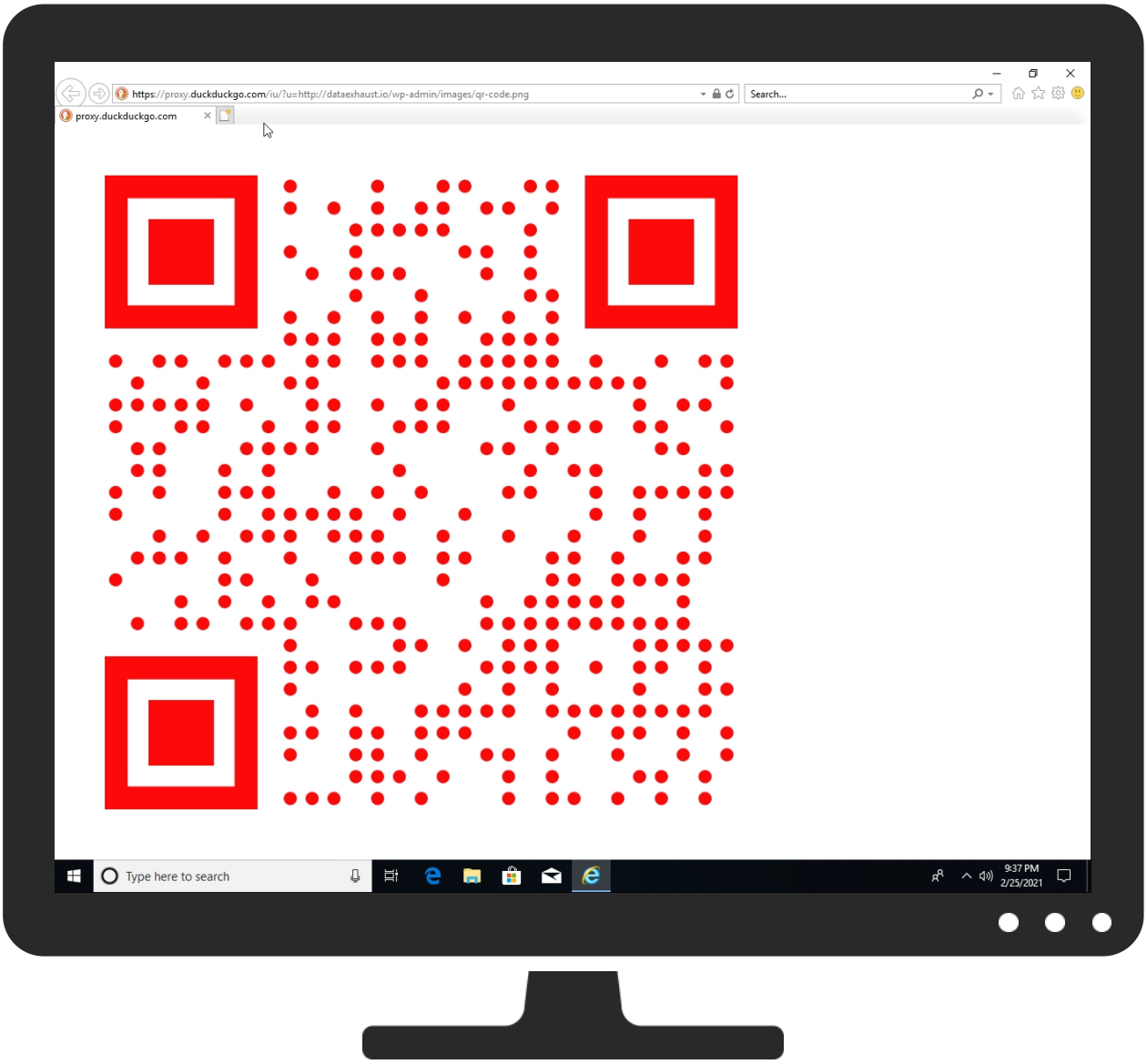
Behavior Graph



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://proxy.duckduckgo.com/iu/?u=dataexhaust.io/wp-admin/images/qr-code.png	0%	Virustotal		Browse
http://https://proxy.duckduckgo.com/iu/?u=dataexhaust.io/wp-admin/images/qr-code.png	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://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
external-content.duckduckgo.com	40.114.178.124	true	false		high
proxy.duckduckgo.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://proxy.duckduckgo.com/iu/?u=dataexhaust.io/wp-admin/images/qr-code.png	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://https://proxy.duckduckgo.com/iu/?u=dataexhaust.io/wp-admin/images/qr-code.png	~DF07954DF9B6288543.TMP.1.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://https://proxy.duckduckgo.com/favicon.ico	imagestore.dat.2.dr	false		high
http://https://proxy.duckduckgo.com/favicon.ico~	imagestore.dat.2.dr	false		high
http://https://proxy.duckduckgo.com/iu/?u=dataexhaust.io/wp-admin/images/qr-code.pngRoot	{3826F327-77A9-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.114.178.124	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358578
Start date:	25.02.2021
Start time:	21:36:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://proxy.duckduckgo.com/iu/?u=dataexhaust.io/wp-admin/images/qr-code.png
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:	10
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@3/18@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 168.61.161.212, 13.64.90.137, 104.42.151.234, 88.221.62.148, 52.147.198.201, 104.43.193.48, 51.104.139.180, 152.199.19.161, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, 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.{3826F325-77A9-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8501084737635667
Encrypted:	false
SSDEEP:	192:r+ZdZm2zWZtVif6nZzMuhBwbDksftnkjX:rKTdKL6HMCzi
MD5:	2FFB609D8E46AB36D3FAAA839ADC01EF
SHA1:	5BA63C39E3B2F283F982036DC428DE6B735367C9
SHA-256:	D0DDE33CA1A50606C660F22A940908D79B27131E0F602044A8566644A10F278C
SHA-512:	4F9D3D7599C740906149D3540A96949CD4324CF0BAE897C06E9681D4EE53D76B58339722BC7E0A932BDE887C5AD24F904FAD3AC3AD5FE2E3C0594614D388343
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\{3826F327-77A9-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24280
Entropy (8bit):	1.651944388630167
Encrypted:	false
SSDEEP:	48:lw1GcprUGwpasG4pQIGrapbShGQpBxObGHHpcx6TGUp8x+GzYpmxb6Gopt7bT4/z:rrZsQs6WBSbjIO2gWgM0jVg

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3826F327-77A9-11EB-90EB-ECF4BBEA1588}.dat	
MD5:	F38EC05E748D45E6FE5EBA32EFC5381A
SHA1:	0EBB09D0FF869C93054F68D28734D7CB8E378D6E
SHA-256:	8852F20BB987584A6F8A47463FD93759CFF5B07BF93925284C1332E40F9918B5
SHA-512:	83C8803B357F34B12A291FA45462627AB991C4A709785283745B1A301D37326218B0C1EAF07663273D61A55D9BB35CCFF4883E1909D64D5854980820AE80661E
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\{3826F328-77A9-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5641871226045674
Encrypted:	false
SSDEEP:	48:IwhGcpr4GwpaB7G4pQJGrapbSSGQpKiG7HpRiTGIpG:rXZgQv6pBS6ANT2A
MD5:	669F6C65AE47E21C5CD1DB34A9467BD6
SHA1:	1BE316762D071104E6EF30D2A4D3D74526460856
SHA-256:	22A732111E6289A0C0A503F09CAA197EA0A337E1B7B5279E01F1DE858506F40C
SHA-512:	994B0B2C37ECA36B3F1EFC6598EE8D94DC39DB3092CF3823CA1C980738E579160C9BAD39C4E047ECF4EC69100BFA4F56869777BF48D6D4AAAD216777FEF5B79
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):	656
Entropy (8bit):	5.0581274984028015
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEwd6d1nWimI002EtM3MHdNMNxOEwd6d1nWimI00OYGVbkEtMb:2d6NxOPe1SZHKd6NxOPe1SZ7YLb
MD5:	87F46ED3C0BA837057CBB3783C3A0B71
SHA1:	F745DEF0CA7378243155B94976D057DE189DCABF
SHA-256:	1B198304C2AA8B5C417E9989993804DEDD867DB6ACA37105CC12FCC805A876F1
SHA-512:	769CE34B4678FE075C057BB3DBD12E5AFFF94BE7367E3D76B17A1627F3DB4AAC95CB79E23C4ED0E5F093949F9660B41D393A00986674DA288CDCBE1F603A29I1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x0d860c13,0x01d70bb6</date><accdate>0x0d860c13,0x01d70bb6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x0d860c13,0x01d70bb6</date><accdate>0x0d860c13,0x01d70bb6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.102883897368569
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kw6b66b1nWimI002EtM3MHdNMNxe2kw6b66b1nWimI00OYGkak6Ety:2d6Nxrmv1SZHKd6Nxrmv1SZ7Yza7b
MD5:	1206FDD294D7D2C85F9937542786FD15
SHA1:	535D69446AD8BDC3F1B2FF5BA82BC934D5F3BE1B
SHA-256:	7AA505F3D8D9BF58B899D068933C465D11DD77FA883BC320DE8C57DF678C8908
SHA-512:	13E49D9870D1460E869F0DECFD4AF56A3204662DF294713CBE9371E6C23F14C39ABF78A808E53431B6198D77E1B9CA165493EC5F2C4D897B620FA855772E7024
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x0d7ee526,0x01d70bb6</date><accdate>0x0d7ee526,0x01d70bb6</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>0x0d7ee526,0x01d70bb6</date><accdate>0x0d7ee526,0x01d70bb6</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):	662
Entropy (8bit):	5.0774249736552175
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLwd6d1nWimI002EtM3MHdNMNxvLwd6d1nWimI00OYGmZEtMb:2d6NxvUe1SZHKd6NxvUe1SZ7Yjb
MD5:	C0A5FF2CFA7C0538AF89B01A13FB5C90
SHA1:	C8BDD74AB8CBF4E9997A575E59876B182430D11B
SHA-256:	A2277AC1D6E5C98CD391AE9C545F44B503C96DCE572939C621F9DE0B5C79C45E
SHA-512:	5BADFE0D0532224E0FE1504BF0F6C034B7B58293E793AFDC84C0C12907CDE819785EF63D7DD9BC697FD60B09A214238B2FEADD1AA378C251784B4EFB5A18EEEF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x0d860c13,0x01d70bb6</date><accdate>0x0d860c13,0x01d70bb6</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>0x0d860c13,0x01d70bb6</date><accdate>0x0d860c13,0x01d70bb6</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):	647
Entropy (8bit):	5.08150090988142
Encrypted:	false
SSDEEP:	12:TMHdNMNxiwiw6iw1nWimI002EtM3MHdNMNxiwiw6iw1nWimI00OYGd5EtMb:2d6NxGw9w1SZHKd6NxGw9w1SZ7YEjb
MD5:	CE4AA49330D8EDD4D84D2854648B439F
SHA1:	AF2737F5013E1528C82323933F5BA9F9944586FF
SHA-256:	961FF72A8BC8DDDF0214ADB17AEA0AD19EB1853A34BD797556346844D44B9FB6
SHA-512:	A0DCCB2BA4CA50BB969A73740A4369C33087111297F31E8A694FD52DACA5BF2161CCD45A05D5A67AC7FEDB1532953E1E1C957B5EC7B69A244030A87B08CF7C6A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x0d83a9ca,0x01d70bb6</date><accdate>0x0d83a9ca,0x01d70bb6</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>0x0d83a9ca,0x01d70bb6</date><accdate>0x0d83a9ca,0x01d70bb6</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):	656
Entropy (8bit):	5.086434554507504
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwwd6d1nWimI002EtM3MHdNMNxhGwwd6d1nWimI00OYG8K075EtMb:2d6NxQDe1SZHKd6NxQDe1SZ7YrKajb
MD5:	1FC4D8525AF87864734E26EA3E152362
SHA1:	E2B16A79A77D76555C5C7111AB9E7E487A8FA145
SHA-256:	57D17AB1D4977A10F8AC589AD4054EAE6FBEA417FBA87750376D5B0B5E585E25
SHA-512:	3A7F11511532B6D48E5098B8A9E1DCDE15C62154853CD45677CE6F5F34C253EB30697CAA9437EC2D039713DFF15F5114E2B62604B1D28003327549017D777AEC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x0d860c13,0x01d70bb6</date><accdate>0x0d860c13,0x01d70bb6</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>0x0d860c13,0x01d70bb6</date><accdate>0x0d860c13,0x01d70bb6</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):	653
Entropy (8bit):	5.067507039036159
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nwiw6iw1nWimI002EtM3MHdNMNx0nwiw6iw1nWimI00OYGxEtMb:2d6Nx03w9w1SZHKd6Nx03w9w1SZ7Ygb
MD5:	7549C199EBA5A4C85F599B86745CEC02
SHA1:	B848335130A67CE441F8CD654F4FB526FAD7839C
SHA-256:	D50C1A3051EF1FC239515417EC8B7A59E75771D1D30338F919EDD6E7A2557DDA
SHA-512:	F216E4E5681F60EC23A2BA0F7623086B5362E486364F4F95A7E1FD04265C8177A489D3AB87BE596A97B6FB6335B3471AF9F93255A77FF42F9D5E3E71FCBD36FB
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x0d83a9ca,0x01d70bb6</date><accdate>0x0d83a9ca,0x01d70bb6</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>0x0d83a9ca,0x01d70bb6</date><accdate>0x0d83a9ca,0x01d70bb6</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):	656
Entropy (8bit):	5.106056811411475
Encrypted:	false
SSDEEP:	12:TMHdNMNxxwiw6iw1nWimI002EtM3MHdNMNxxwiw6iw1nWimI00OYG6Kq5EtMb:2d6Nx1w9w1SZHKd6Nx1w9w1SZ7Yhb
MD5:	E192B7C40BE5FB6EF5BB209D0C04A9E5
SHA1:	780C580D143B0EF01A751C3D9A0E3A02F2E1BF87
SHA-256:	52F050B092B5A869E44353268CD090627F23C6C85BCE1D1EEB90F84DEB95497A
SHA-512:	F13142298AF8242278A154EE9E62F1B5169C3AA299D7830E3422B58DA58E1E70C8466F258C8AA4918A2E1859D0930C59EAF4A6E7859532A3DFEB7DC863BAF7A7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x0d83a9ca,0x01d70bb6</date><accdate>0x0d83a9ca,0x01d70bb6</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>0x0d83a9ca,0x01d70bb6</date><accdate>0x0d83a9ca,0x01d70bb6</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):	659
Entropy (8bit):	5.10895005790415
Encrypted:	false
SSDEEP:	12:TMHdNMNxcwW2+b6W2+b1nWimI002EtM3MHdNMNxcwW2+b6W2+b1nWimI00OYGVEs:2d6Nxg1911SZHKd6Nxg1911SZ7Ykb
MD5:	D038D3E3373A9C2E5C938F216C5DC2ED
SHA1:	9511603D9F5B515D8797AD23F9E795DB9F25D7BA
SHA-256:	2EF36B3FA8C35F1EF6B5FBEC62050850133CEF241469F05ADA0996592069E37D
SHA-512:	D731CE6D8D30FF58ABB612BBE8F305B3E690DA28D7E2E2C42EE48A409627372965D9726E1981D77DFACEAE5F67D096BD85AE353FBFCCA433C2057A94D0A18E56
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x0d814766,0x01d70bb6</date><accdate>0x0d814766,0x01d70bb6</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>0x0d814766,0x01d70bb6</date><accdate>0x0d814766,0x01d70bb6</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):	653
Entropy (8bit):	5.095734285864599

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnwW2+b6W2+b1nWimI002EtM3MHdNMNxfnwW2+b6iw1nWimI00OYGe5t:2d6NxH1911SZHKd6NxH19w1SZ7YLjb
MD5:	1E1E4349266E14A521E2DC2682E2F32C
SHA1:	40679DDAF5E7C25AE3CA3C554A2D6974BD6B77C6
SHA-256:	48E604AC6333DBBE02968345F0473BB9811B9C1B46F29771EDF462CE6575B53D
SHA-512:	1FC30938C6B0F0EE6AD7FBD2A093D8BD19D39C18F53BDFA64581229471DC0B6F62A58B492057C4D8F72ACDD1B2A267247382796B0CB75B761B8EA2647871BA2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x0d814766,0x01d70bb6</date><accdate>0x0d814766,0x01d70bb6</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>0x0d814766,0x01d70bb6</date><accdate>0x0d83a9ca,0x01d70bb6</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\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	5672
Entropy (8bit):	4.935186205779581
Encrypted:	false
SSDEEP:	96:DuMYhc3Rsk/dVCjxZhUwwSIICQyhvArRTsmBNTHu:6QRskS0EyKrp5RO
MD5:	0C3EBD64644F6D4070192AC57C1E7BBF
SHA1:	E575BFCF0616B822BF507D73A0220359066D8AAD
SHA-256:	95059F17040F5884FEDB42EFB1A10CDEAFE08F278B4E75E2732C43B67A500140
SHA-512:	9B89A5B657392236E704FC467C9B22235A24C8D89AFE040F9052E62F4D8573A4035CCC42B9E965DA32A3B1D31F7601F00F8E8CF83A318FD5111F9B2ACCDD117
Malicious:	false
Reputation:	low
Preview:	(.h.t.t.p.s.:././.p.r.o.x.y...d.u.c.k.d.u.c.k.g.o...c.o.m./.f.a.v.i.c.o.n...i.c.o.~.............. .h.......(....... ....5Y.+4Y.3Y..:]..:]..3Y..4Y.5Y.+......................U...4Z.Pp........................Pp..4Z.U..............U...3Y...............G.f.M.k.J.|.^..........3Y.U..........4Z........Xv...............>...@...Xv.........4Z.....5Y.+Pp......Xv..3X............g...3X..3Y..3X..Xv......Pp..5Y.+4Y.........3X..Fg.............Bh..'z..!...&|..2\..........4Y.3Y......Nn..3X..p.................'{..+q..%...(x..Nn......3Y..:]......3X..3X................$... ..../c..3X......:]..:]......3X..3X........................O........../c......:]..3Y......Nn..3X..........v_.........v_.c...3X..3X..Nn......3Y..4Y.........3X.........................7[..3X..3X.........4Y.5Y.+Pp......Xv.._|..................r...3X..3X..Xv......Pp..5Y.+....4Z.........Xv..Ll.........Ce..3X..3X..Xv.........4Z.........U...3Y.........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\iu[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1155 x 1155, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	31028
Entropy (8bit):	7.777139810529103
Encrypted:	false
SSDEEP:	768:xo3QRxkxh11iHvqHc2tXme6FWBmmmm0mmmm8wuuuuuuuuuuuBQtmmKmmmmmB7:xo3HlOqHn6U90v7
MD5:	CB0A391DDCA653F6CDA1E3221F5A8B69
SHA1:	5651CC98B0678E974E74669BA41DF3F1D5DD4E92
SHA-256:	AA57A5C0B91CD9095C3507535A78ECFA570D75D1AFD296BFE1B871109038AFCC
SHA-512:	35B7FA318870ED9439835D58BAA2E19C7FA61E40EC884C52DC9F28E5221F4902F3879AF5A62CFB3AD4FA0913F1ECB2050DE127A2D6E58537975EDC8C21A070EB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://proxy.duckduckgo.com/iu/?u=dataexhaust.io/wp-admin/images/qr-code.png
Preview:	.PNG........IHDR.............eih.....bKGD............ .IDATx...1oUg.0..fSM,,aJS.(....S..Q".f$4.d..@...#.&..l.e$4H.HP..].M.Q:K.L.....O..{...}..g..Q....u..5.1......@........c.....f.....vd.....?.#.....Y......Db....L... .M... .M... .M... .M... .M... Z.b...<........fg.YZ*..eu.\.V....h.wt.a.sG...0.J.u.>C..K.$6..I...zu.f..7o{A.|..[......u.ZX..Q5w.6..Hl8OA}...<..gP.......w.na.....!....ZX..Q5w.;<...@..zd..y2.........d..W.m..W..|(........UsG..S....)._61.'3...&++....9z.}...:5.C..wT-.u.;z'OA$6........q.`.&M...ys:..........UsG@&~&..d..oP......k"Ki..._.........UsG..)...L...nc.6...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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):	4.905057992673572
Encrypted:	false
SSDEEP:	96:7uMYhc3Rsk/dVChxZhUwwSIICQyhvArRTsmBNTHB:yQRsks0EyKrp5Rh
MD5:	16C289C3678631CD238D96D5A659178E
SHA1:	AF6F9DFE4E365E659371D5B8EC11271DAAF0C3CA

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon[1].ico</th></tr>
<tr><td>SHA-256:</td><td>3EC69A44BD0DF1B1E6DA6A2A7EC8A5AA53CFC6A3149841C52AEEFEB61F5BA923</td></tr>
<tr><td>SHA-512:</td><td>30E8157B1739AAD5696A1A8FCC7B983C7648639186D310BDE3072EB62703F1C0A3818C2E665D9436CDC57B38D01156F4A955EB2F0C27C99A354A8F2897CFF774</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://proxy.duckduckgo.com/favicon.ico</td></tr>
<tr><td>Preview:</td><td>............ .h...&... ....(....... ....5Y.+4Y.3Y..:]..:]..3Y..4Y.5Y.+........................U...4Z.Pp..........................Pp..4Z.U..............U...3Y................G.
f.M.k.J.|.^...........3Y.U...........4Z.........Xv................>...@...Xv..........4Z.....5Y.+Pp......Xv..3X.............g...3X..3Y..3X..Xv......Pp..5Y.+4Y.........3X..Fg.............Bh..'z..!...&|..2\....
......4Y.3Y......Nn..3X..p..................'{..+q..%...(x..Nn......3Y..:]......3X..3X.................$... ..../c..3X......:]..:]......3X..3X.........................O........../c......:]..3Y......Nn..3X.....
......v_..........v_.c...3X..3X..Nn......3Y..4Y.........3X.........................7[..3X..3X..........4Y.5Y.+Pp......Xv.._|.................r...3X..3X..Xv......Pp..5Y.+....4Z.........Xv..Ll.........Ce..3X..
3X..Xv..........4Z.........U...3Y.............Nn..3X..3X..Nn.............3Y.U..............U...4Z.Pp........</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\~DF07954DF9B6288543.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34473
Entropy (8bit):	0.36904920335922986
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+x7WxO7xex3xbIxb/7bT4/1:kBqoxKAuvScS+oI7k1eFs
MD5:	5621F51BC5EDD488D454FCEB2AE085BB
SHA1:	4DB2F874AAA66D11F0F26E622863DE21C0E5B68B
SHA-256:	1E2FA28B906C6C698A2F1B4C207AD6FC9CDF0F3723B2B4E1F1B474F6DCEA3173
SHA-512:	1F6810268AEED55BDF40BB30DF788566589368F6DB746AB2E2BD3BF01163BBD236DD7D9A29C8F0A345280D6587AF8322F25A263908FA6D1C988F782CF86167D8
Malicious:	false
Reputation:	low
Preview:	.............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF292E862C5B5A2C12.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4716040007670098
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loo9lo49lWD4z8aA:kBqoID1HaA
MD5:	23E7BDC0484E997281F7E4D56AFC8114
SHA1:	2E4AB90D90717BEAF8302B7C574567830EFCCCC6
SHA-256:	264C72BD5959DB7D75FC244AD17040FA7695D9A024762FA8B4A95E16F05DB2DE
SHA-512:	0CFC70E61FEAEA5B03ED84C0D0195CEE200C161D9066F0833F6CDCD71C488F3139C36DB9F57C35070E3D46A4DE95C9824D14FCFE6023F02A6AC8E25B5D9C3 8
Malicious:	false
Reputation:	low
Preview:	.............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9B9B171105311C92.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.2956398003355815
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA2XfX1:kBqoxxJhHWSVSEab2XP1
MD5:	54B4610F48CBBB0FD88C03786775A485
SHA1:	F04199CC2E136FBAA68004AC25060CC37C1915C5
SHA-256:	B9020167DF3571AE51ACCCECECEFE949AF54AFE14FFC920282708E6CB4569FA0
SHA-512:	3B022E72EB12F8425D14E622BD21E97F1162AE5BB56E3BBE4984022E77D46453A023E263BCC540B1F4E3A141D3AEA4507109E0BC5501A9AD8A43A15F04CBA1A 6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF9B9B171105311C92.TMP	
Preview:	................................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 90

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:37:07.492121935 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.493489981 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.540076017 CET	443	49733	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.541229963 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.541328907 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.541480064 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.550374985 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.550509930 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.598094940 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.598268032 CET	443	49733	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.598742962 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.598783970 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.598819017 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.598875046 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.598911047 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.598923922 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.599591970 CET	443	49733	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.599636078 CET	443	49733	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.599668980 CET	443	49733	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.599694967 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.599730015 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.599735975 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.632311106 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.632563114 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.637816906 CET	49733	443	192.168.2.4	40.114.178.124

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:37:07.637995005 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.638022900 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.680398941 CET	443	49733	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.680455923 CET	443	49733	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.680488110 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.680517912 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.680531979 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.680561066 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.680574894 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.680609941 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.681724072 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.682262897 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.685431957 CET	443	49733	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.685516119 CET	49733	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.685583115 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.685841084 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.685894966 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.685934067 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.685940027 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.685947895 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.685981035 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.685997963 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.686022043 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.686055899 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.686063051 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.686064959 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.686100960 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.686117887 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.686142921 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.686175108 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.686182022 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.728348970 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.728403091 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.728441000 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.728451967 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.728478909 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.728480101 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.728498936 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.728538990 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.733946085 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.733990908 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734028101 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734033108 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734051943 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734076977 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734083891 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734122038 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734153986 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734160900 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734164953 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734200954 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734216928 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734241009 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734272003 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734278917 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734317064 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734335899 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734348059 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734355927 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734388113 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734395981 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.734405041 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734441042 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.734461069 CET	49734	443	192.168.2.4	40.114.178.124

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:37:07.734517097 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.775589943 CET	443	49733	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.944917917 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.994606972 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.994663000 CET	443	49734	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:07.994694948 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:07.994723082 CET	49734	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:24.364932060 CET	49747	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:24.412720919 CET	443	49747	40.114.178.124	192.168.2.4
Feb 25, 2021 21:37:24.412805080 CET	49747	443	192.168.2.4	40.114.178.124
Feb 25, 2021 21:37:24.415115118 CET	49747	443	192.168.2.4	40.114.178.124

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:37:00.470205069 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:00.520275116 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:01.418504953 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:01.468132019 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:02.409610033 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:02.459348917 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:03.556929111 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:03.605729103 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:05.046515942 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:05.098303080 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:06.180340052 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:06.233460903 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:06.421772003 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:06.475343943 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:07.431369066 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:07.480659008 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:07.584456921 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:07.644830942 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:08.713653088 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:08.771136999 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:10.026587009 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:10.080698013 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:10.977418900 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:11.025978088 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:12.272568941 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:12.331250906 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:13.236026049 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:13.285968065 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:14.418044090 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:14.466774940 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:15.718683004 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:15.767530918 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:16.736660004 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:16.788564920 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:17.582732916 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:17.631462097 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:18.552776098 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:18.606745005 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:19.500803947 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:19.561144114 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:24.287046909 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:24.362622023 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:24.606416941 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:24.654902935 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:25.689815998 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:25.738804102 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:30.775564909 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:30.824507952 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:36.541053057 CET	49612	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:37:36.589975119 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:37.047591925 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:37.097771883 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:37.533193111 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:37.584428072 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:38.100989103 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:38.152363062 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:38.547175884 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:38.596060038 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:39.109792948 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:39.158973932 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:40.566097021 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:40.615756989 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:41.135902882 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:41.184808969 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:44.604016066 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:44.653052092 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:45.141561985 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:45.192073107 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 21:37:48.639009953 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:37:48.730321884 CET	53	50601	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:37:07.431369066 CET	192.168.2.4	8.8.8.8	0x4387	Standard query (0)	proxy.duck duckgo.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:37:24.287046909 CET	192.168.2.4	8.8.8.8	0xd394	Standard query (0)	proxy.duck duckgo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:37:07.480659008 CET	8.8.8.8	192.168.2.4	0x4387	No error (0)	proxy.duck duckgo.com	external-content.duckduckgo.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:37:07.480659008 CET	8.8.8.8	192.168.2.4	0x4387	No error (0)	external-content.duckduckgo.com		40.114.178.124	A (IP address)	IN (0x0001)
Feb 25, 2021 21:37:24.362622023 CET	8.8.8.8	192.168.2.4	0xd394	No error (0)	proxy.duck duckgo.com	external-content.duckduckgo.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:37:24.362622023 CET	8.8.8.8	192.168.2.4	0xd394	No error (0)	external-content.duckduckgo.com		40.114.178.124	A (IP address)	IN (0x0001)

HTTPS Packets

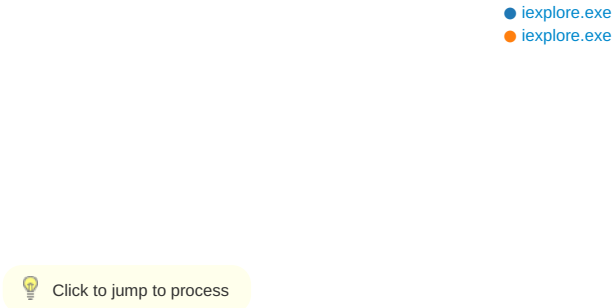
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:37:07.598819017 CET	40.114.178.124	443	192.168.2.4	49734	CN=*.duckduckgo.com, O="Duck Duck Go, Inc.", L=Paoli, ST=Pennsylvania, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 01:00:00 CET 2021 Wed Mar 08 13:00:00 CET 2023	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 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 21:37:07.599668980 CET	40.114.178.124	443	192.168.2.4	49733	CN=*.duckduckgo.com, O="Duck Duck Go, Inc.", L=Paoli, ST=Pennsylvania, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 01:00:00 CET 2021 Wed Mar 08 13:00:00 CET 2023	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 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 25, 2021 21:37:24.465496063 CET	40.114.178.124	443	192.168.2.4	49747	CN=*.duckduckgo.com, O="Duck Duck Go, Inc.", L=Paoli, ST=Pennsylvania, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 01:00:00 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6748 Parent PID: 800

General

Start time:	21:37:04
Start date:	25/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff63d1a0000
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: 6820 Parent PID: 6748

General

Start time:	21:37:05
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6748 CREDAT:17410 /prefetch:2
Imagebase:	0x1240000
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