ID: 433023
Cookbook: browseurl.jbs
Time: 06:49:00
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

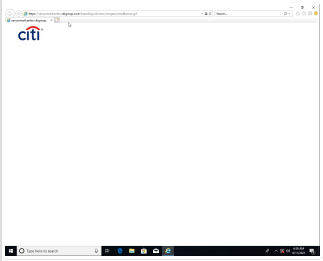
Analysis Report https://securemailcenter.citigroup.com/…

Overview

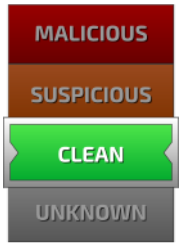
General Information

Sample URL:	http://https://securemailcenter.citigroup.com/branding/citi/emx/images/emailBanner.gif
Analysis ID:	433023
Infos:	

Most interesting Screenshot:



Detection

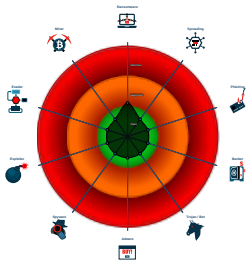


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 6492 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6568 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6492 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

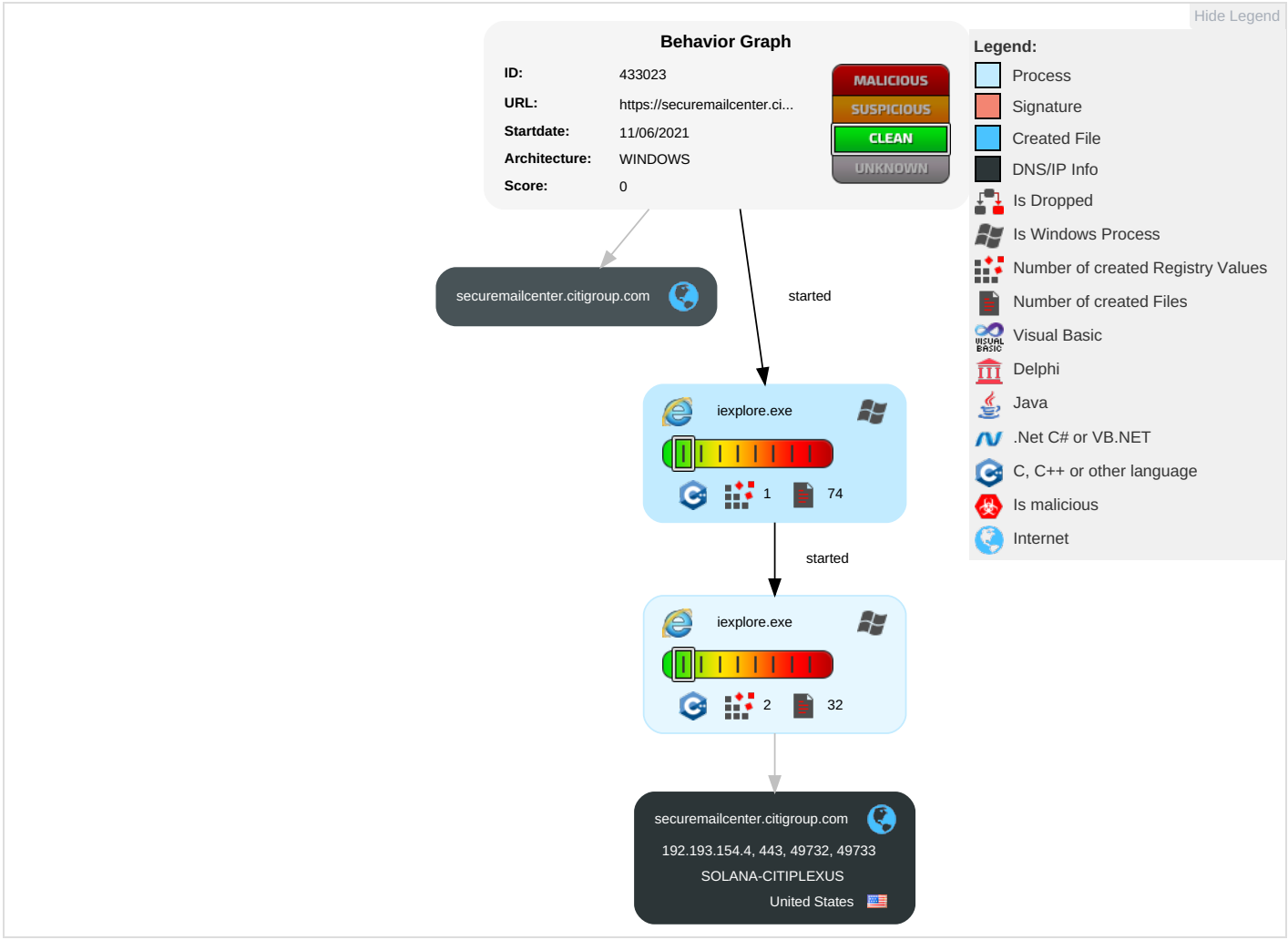
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

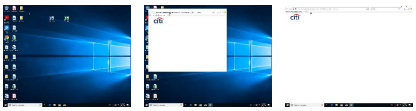
Behavior Graph

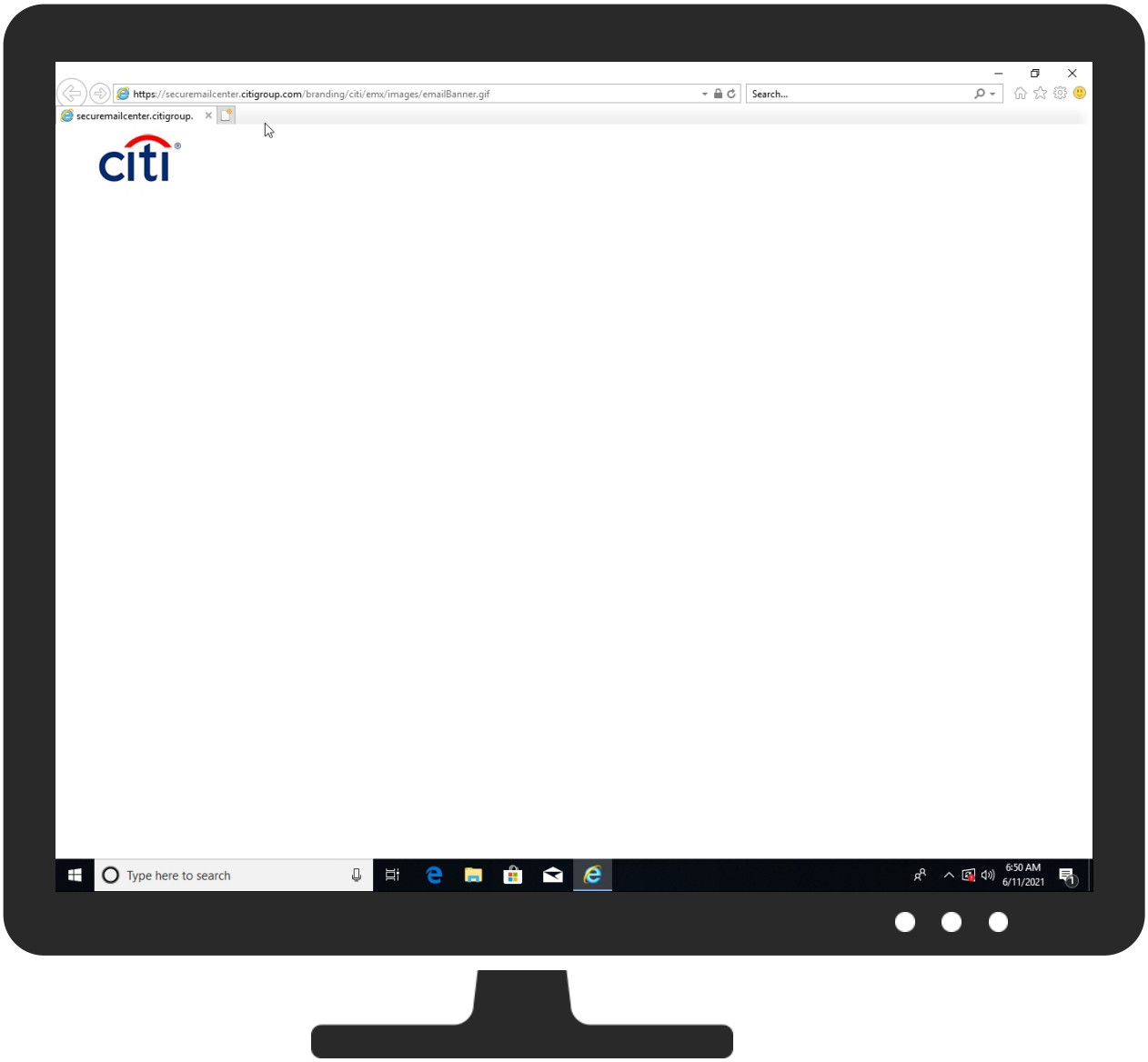


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://securemailcenter.citigroup.com/branding/citi/emx/images/emailBanner.gif	0%	Virustotal		Browse
http://https://securemailcenter.citigroup.com/branding/citi/emx/images/emailBanner.gif	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	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
securemailcenter.citigroup.com	192.193.154.4	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://securemailcenter.citigroup.com/branding/citi/emx/images/emailBanner.gif	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.193.154.4	securemailcenter.citigroup.com	United States		32287	SOLANA-CITIPLEXUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433023
Start date:	11.06.2021
Start time:	06:49:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://securemailcenter.citigroup.com/branding/citi/emx/images/emailBanner.gif
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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/16@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{72BD4AA8-CA70-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8520520737947785
Encrypted:	false
SSDEEP:	192:rxZuZ12RWFthife02zMXOBzoDUsff0HjX:r36sgP+n22DI
MD5:	D4248FB466BC9CBB72FBCB88184FC4B4
SHA1:	9D29D735E71B4D62121B0F99AC4065C59CA49D12
SHA-256:	F94332F9CA7DCAFF84AEBF45B668AEB0BF178D60B44534C52C9FF5F702339273
SHA-512:	E452AEF4E8D13F1279F848B440968A6D7D25FF01F80F2707A3C93FE0CCE983C4B9A8960A203AC20B6627CE5D956935959AE847E484E49B6D90BDACB0103F6B2
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\{72BD4AAA-CA70-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24268

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{72BD4AAA-CA70-11EB-90EB-ECF4BBEA1588}.dat	
Entropy (8bit):	1.649163218419641
Encrypted:	false
SSDEEP:	48:IwZGcprkGwpa4G4pQwGrapbS+GQpBQJBGHHpcQ32TGUp8QbGzYpmQEQGop71OEGR:r/ZcQo6OBSWjZ2FWGM6V1621g
MD5:	904FCB81A765FC235A9A42D0EBC7D9C3
SHA1:	85DF823E9025036AD5224FFA877A3430FE5A358E
SHA-256:	5BFDEFB3F4FB66D0454130B158A06A3457993175ECF57D147653D69EFC5D6E85
SHA-512:	D45C2D0BC4A1CA3771089AA93CD49FE98590EA85B94F18F480F68394714986564DDBDDA54D6400F65FC670F23B1A10F39F2E416D0D3CC610E0B0F6BEB8E6CF D
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\{72BD4AAB-CA70-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5650150573365063
Encrypted:	false
SSDEEP:	48:Iw4GcprFGwpaAG4pQoGrapbSDGQpKlG7HpRoTGIpG:rMZPQg62BS9AUTsA
MD5:	5CFAEDABD6B89CDE34DC92ECD92C6C67
SHA1:	CC4D19D142A39F8520C55B5278F06E1238EFADB1
SHA-256:	99451BECA267AE947D01E452BBEC1A297580D896A09E4D747FBCFFDC4971797B
SHA-512:	0A68B4968CB633FA42AA9073BA6B3E57B19438EEE11AFD7116C19AABDE81C47B028CD8BEB0A06D489B1091D8DF27533A32CC1882B0F27D88233EC51F43B960I 3
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):	5.094154577651827
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEwibiyGCnWimI002EtM3MHdNMNxOEwibiyGCnWimI00OYGVbkEtMb:2d6NxOk+yNSZHKd6NxOk+yNSZ7YLb
MD5:	DEE976133CC71C41D48BA2BC059958C2
SHA1:	198615407509B7EB6D2691CAE2AF47025EF0EC92
SHA-256:	C9A7695597E51DDDA014FDD8F2B614D96787A2BA7A6E7945FBB0716EB096B46A
SHA-512:	B21B62A99E5E5B62F63D4DE06037CF99D571DF9E02339C3FFA4C2833218EB40DA0356EFEDA38DEFAC201B89E1EA01D2C595A7C29F753CC2FAB9A111BF99E31 46
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x48854b03,0x01d75e7d</date> accdate>0x48854b03,0x01d75e7d</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>0x48854b03,0x01d75e7d</date><accdate>0 x48854b03,0x01d75e7d</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):	5.107612368883238
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kwS5SEGCnWimI002EtM3MHdNMNxe2kwS5SEGCnWimI00OYGkak6Ety:2d6Nxr+NSZHKd6Nxr+NSZ7Yza7b
MD5:	4D17DE08C3BA98CD69E4398C6B2001E3
SHA1:	E788363DE14D4AE5F6357804640AC8965EF38953

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SHA-256:	A275528F0039383DCBF3CA8B7B8A9A0CFE5BD8E19D2E8D97AA629F7954CCE618
SHA-512:	DA70C92B1F99FE90F8EA1C1045602C5AA30AEE5DE7EF5C8FF99DD0ACBAA4C0B5D8473B0D528C68C177A75657EFAAF01BD7ACB09E2D91A0F890518CE40F25E 2C9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x487e23fa,0x01d75e7d</date><a ccdate>0x487e23fa,0x01d75e7d</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>0x487e23fa,0x01d75e7d</date><a ccdate>0x487e23fa,0x01d75e7d</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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):	5.113125523485069
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLwibiyGCnWimI002EtM3MHdNMNxvLwibiyGCnWimI00OYGmZEtMb:2d6Nxvn+yNSZHKd6Nxvn+yNSZ7Yjb
MD5:	438401ECF6A74A69748D9A10BB405772
SHA1:	417B1951E1B6F94BA63B4DF6D4BA78624F0265FC
SHA-256:	75E45D936D66375D9C71E72C9DEE2F31A47E432C8CF0C1305D5E32054A0546EF
SHA-512:	8CDDCDC113414442588E66E099247F9F3CE6051C9126A80E4B6F08577E3BB2709D4E18BB21070A6DD05AAD75B0C762CA3C7F790CB196FD63D215569AEED0F4I 2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x48854b03,0x01d75e7d</date> <accdate>0x48854b03,0x01d75e7d</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>0x48854b03,0x01d75e7d</date><accda te>0x48854b03,0x01d75e7d</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.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):	5.109619731972153
Encrypted:	false
SSDEEP:	12:TMHdNMNxiwibiyGCnWimI002EtM3MHdNMNxiwibiyGCnWimI00OYGd5EtMb:2d6Nxe+yNSZHKd6Nxe+yNSZ7YEjb
MD5:	D1A903C21C31944F2866E7EF9AC3CACA
SHA1:	2A5C6A15412E722DB78FCA7210C2A2625CDC03C7
SHA-256:	979316C7DEFF7127F64A4B80553E97AAD2B95077945CC5C22D33F565D46F40D0
SHA-512:	3237D5CE81A1C1757D989D32C8E4AEE671133A64D7AC756023DF25CB09C4D7FA21D2224FDA1B797E51AAF5BEADCA66BD62FFD1A44CE8699446BF8B50A134E 3A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x48854b03,0x01d75e7d</date><acc date>0x48854b03,0x01d75e7d</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>0x48854b03,0x01d75e7d</date><accdate>0x48854 b03,0x01d75e7d</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):	5.124794044001139
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwwibiyGCnWimI002EtM3MHdNMNxhGwwibiyGCnWimI00OYG8K075Es:2d6NxQw+yNSZHKd6NxQw+yNSZ7YrKajb
MD5:	8F44695FB3C8649062A5C475153E0043
SHA1:	915C85C7D0B6E716C425481391AC61B4ED2E20D9
SHA-256:	F4689A7C34C08DB7A647A22D3ACB6C4B5EFFACF2C6AE4F1BAD045ED0A98E9035
SHA-512:	C29F006F5D6D5E59AB30BA97E8048801B9FC6DB176C594632D2119D2C79AC097EB994FC508E0AA56CDB9345D5884C8B2B05FEF675B0C5CF84119CE60BFF9F5 5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x48854b03,0x01d75e7d</date><accdate>0x48854b03,0x01d75e7d</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>0x48854b03,0x01d75e7d</date><accdate>0x48854b03,0x01d75e7d</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):	5.095367495227131
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nwibiyGCnWimI002EtM3MHdNMNx0nwibiyGCnWimI00OYGxEtMb:2d6Nx0D+yNSZHKd6Nx0D+yNSZ7Ygb
MD5:	635806E31A6BC010CC7D91F2C9907759
SHA1:	D6F8BA5CDC555F4F8D1BBFFE5A09EE67715B0D76
SHA-256:	FC10F556B62F0700496A6C0D50306BF15BC4A8282B9660EFA61BDA89DE04BF58
SHA-512:	A07313CDED638FF1FD922E5919A1B1117630ACF868EA3C428A6A215D415BD8A12CE64AB47BC31038D658A0C6C513C85358B33F92271BCF36ADEFD36C0112EB C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x48854b03,0x01d75e7d</date><accdate>0x48854b03,0x01d75e7d</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>0x48854b03,0x01d75e7d</date><accdate>0x48854b03,0x01d75e7d</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):	5.133789856979621
Encrypted:	false
SSDEEP:	12:TMHdNMNxxwibiyGCnWimI002EtM3MHdNMNxxwibiyGCnWimI00OYG6Kq5EtMb:2d6Nxh+yNSZHKd6Nxh+yNSZ7Yhb
MD5:	1A9C672CC2A31655CE57EFEFBFBF7D18
SHA1:	D8FD12A536074E6805E13D4F511121AF0F4A9CE0
SHA-256:	596AF2CA1E95EA5042C584034D3AF1B3A0CE15066252ED3F32F8C1FACEB6F972
SHA-512:	29275FA96EEFFD7BE48FB54291E35E00437735754DE99A1D6347578AA1AE2780FAD276F0F9DFC0EDC022EF024234B65BCDE61A9F54F0A2CCC68AFBA0BF02312 3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x48854b03,0x01d75e7d</date><accdate>0x48854b03,0x01d75e7d</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>0x48854b03,0x01d75e7d</date><accdate>0x48854b03,0x01d75e7d</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):	5.0991177220794
Encrypted:	false
SSDEEP:	12:TMHdNMNxcwS5SEGCnWimI002EtM3MHdNMNxcwS5SEGCnWimI00OYGVEtMb:2d6NxmNSZHKd6NxmNSZ7Ykb
MD5:	5AD85F9B30C8DC457EC88875A7FB7666
SHA1:	14B0FBEE67852743D110CFE30229C7E4E9550ABB
SHA-256:	0045B2A6DF637818EC1CD0430AF9C6CAAB439ACE4A0DED255B7AF8CC43D200A1
SHA-512:	9C3B3B547B9537603FD9F3170891AD7BDE2E805A83A47D551CC55B61E7019A157A4D0F52A4FA095C9E55756165413091AE738F389C62A95FEB6A1BE852153DDA
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>0x487e23fa,0x01d75e7d</date><accdate>0x487e23fa,0x01d75e7d</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>0x487e23fa,0x01d75e7d</date><accdate>0x487e23fa,0x01d75e7d</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):	5.080703969340126
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnwS5SEGCnWimI002EtM3MHdNMNxfnwS5SEGCnWimI00OYGe5EtMb:2d6NxnNSZHKd6NxnNSZ7YLjb
MD5:	232134E10010C1B53FA6CB68636D6653
SHA1:	03D0A0D97344F56367699B70973AC90AD62372AA
SHA-256:	83C5D4AA9D7B7ABF21A8188066E4B54DD24E04D6E369D8E53CE01FA3684C5A63
SHA-512:	B97957529792C25EEB7D4FAC17371E2BFDB1328BFA72BE0349752D5BD6E2817210831A8CF543695F10663C4CB8B771BE7ACF49A5F7314045D569065C58F622E6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x487e23fa,0x01d75e7d</date><accdate>0x487e23fa,0x01d75e7d</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>0x487e23fa,0x01d75e7d</date><accdate>0x487e23fa,0x01d75e7d</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\emailBanner[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 150 x 68
Category:	downloaded
Size (bytes):	5493
Entropy (8bit):	7.7035084703150165
Encrypted:	false
SSDEEP:	96:G75u2qwUw5Q5HrX/9ekNqhtN60D5LVbmMiLGl6QV2anQ0bUUXaYhsaTMWREUKKDt:GwwUkQ9jFIPN6kPiMSGlHQwNRDPt
MD5:	D3DE6F4BC837FC5CB9539266FD89D654
SHA1:	F9559568F6EA916F795355A0F9AD1BCF834E3503
SHA-256:	B72A8F8B7ED769364F1B0930373CD92BC39E94A9347221CB68CD449A09B4B031
SHA-512:	E35D996BE807093446CBD12BC7E7DEA9CBD4B33CCF65AE0F3AE80AD0AD934A618E4AEA4A06A717AFB391461C3EEE2519D7DDAFDBDEB6EC42A6D1BF7C1B285198
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://securemailcenter.citigroup.com/branding/citi/emx/images/emailBanner.gif
Preview:	GIF89a..D....,:m|...LKhx.....9Gs.ig.....;F.....WW.....W.....-z.....r.....CT~.....uq.0tO\.....-p....-u.&{....$Y.....c.....0k..... ."iXc.....`[.....-n.....j.....e.....00.)^.....#r...ir....aj.....-n.....M..... a...uz.....&2_.....(v.(p.&r..i.....$|.....el.....J.....r. .....+o.....V.....?.... j.-q.....*g./f.....ir..\].-j.....$`.@C....(r.....k.(l.-w....&i.+t..m.....a.+u.....{}.....g f.$m.....r.....^.\].....a.....\...!.....,.....D.....e..H.....*\....#J.H....3j.... .*.&...9...2m...(..a..fM~.P. ..$.;...J..."l..a..F(..Y....)."...g.0(Q".....&..+.d.x.+.. x..}...5..5S...a..-..M .3l.bx.D.|:.....n..C..>B.....e.

C:\Users\user\AppData\Local\Temp\~DF280D04EE554E50CF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.312668745001186
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAMXw4ibeU:kBqoxxJhHWSVSEabN
MD5:	2802B4EB84325EB84BCB72BE2A1620D0
SHA1:	C28AECF4F53ABDF52BC12326E9A2C6910CD3455B
SHA-256:	C5F4BD61659EE28336EB1043A0120C21FEE8D2F27FE85678668F32080235ADEF
SHA-512:	71F4B6EFFFF12420CE806301C65899B50EF9C5CAB6095E98CCCABF0403C11F2C7C0DEA7FAFE7FA418E5D213F16BA8831FB16A6F0EE683BD0E691C747E897969
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF280D04EE554E50CF.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF2B830054C2999F0C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34461
Entropy (8bit):	0.36745426814800136
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+QVQ7Q5QoQEIQE51OEGa0n:kBqoxKAuvScS+MqwRaX16n
MD5:	E20D8BBC51CF7E6C39C30EEE6DC6D68E
SHA1:	78E72CB54D21DF5D502CB3D5B7254EDBC755B831
SHA-256:	F803EBC148F2E8003052526A1E270AB2DD8A734BAE3F20B96DED325066E04A11
SHA-512:	4BBF143E6224A301BB729DBC3FEA277A0752828905E5778384B308EC0B7CC48F796A9003277A47319489299FE194DC9CD76298AC95EB6C7BD5B0BF5003136D58
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF4E2977DE7B6AC2F0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47643165726207365
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRDm+F9l8fRDmC9lTqDmCMmkMmKjmgmkMmUo:c9lLh9lLh9lIn9lIn9lop9loJ9lWqsYQ
MD5:	4DAFC1F81FC36DEFC4A590B992075299
SHA1:	F5A3082A7A1517617A4BFCBE2E72E5FB7EAD98A7
SHA-256:	6C1153D74C72DDCA5F72209573A8DD971DC929EBDEFA20493BF66EAD88818B37
SHA-512:	754E21DC7ACF39ADEE07BAC0BD5F73A63C184ADC03DC52C92BF0C87CACAF2EA0F92FBDF6D99B05247ABE563BB97C508FF5FB07E0BCE20B7221EAAB40F6DE E740
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 06:49:50.325176954 CEST	192.168.2.4	8.8.8.8	0xfed8	Standard query (0)	securemail center.cit igroup.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:50:06.606499910 CEST	192.168.2.4	8.8.8.8	0x5f18	Standard query (0)	securemail center.cit igroup.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 06:49:50.466156960 CEST	8.8.8.8	192.168.2.4	0xfed8	No error (0)	securemail center.cit igroup.com		192.193.154.4	A (IP address)	IN (0x0001)
Jun 11, 2021 06:50:06.751233101 CEST	8.8.8.8	192.168.2.4	0x5f18	No error (0)	securemail center.cit igroup.com		192.193.154.4	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
Jun 11, 2021 06:49:50.807967901 CEST	192.193.154.4	443	192.168.2.4	49733	CN=securemailcenter.citigroup.com, O=Citigroup Inc., L=New York, ST=New York, C=US, SERIALNUMBER=2154254, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, 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 SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Mar 12 01:00:00 CET 2020	Sat May 21 14:00:00 CEST 2022	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		
Jun 11, 2021 06:49:50.808104038 CEST	192.193.154.4	443	192.168.2.4	49732	CN=securemailcenter.citigroup.com, O=Citigroup Inc., L=New York, ST=New York, C=US, SERIALNUMBER=2154254, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, 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 SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Mar 12 01:00:00 CET 2020	Sat May 21 14:00:00 CEST 2022	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		
Jun 11, 2021 06:50:07.079905033 CEST	192.193.154.4	443	192.168.2.4	49746	CN=securemailcenter.citigroup.com, O=Citigroup Inc., L=New York, ST=New York, C=US, SERIALNUMBER=2154254, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, 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 SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Mar 12 01:00:00 CET 2020	Sat May 21 14:00:00 CEST 2022	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 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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6492 Parent PID: 800

General

Start time:	06:49:48
Start date:	11/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7deac0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 6568 Parent PID: 6492

General

Start time:	06:49:48
Start date:	11/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6492 CREDAT:17410 /prefetch:2
Imagebase:	0x8a0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly