ID: 446654
Sample Name: SCM Requirements for Sellers during COVID-19 - FINAL JULY 12 21 FINAL.pdf
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 01:27:17
Date: 10/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

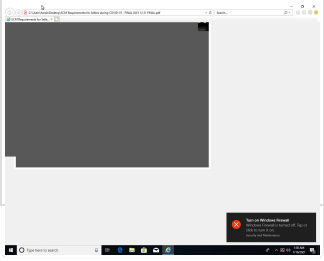
Windows Analysis Report SCM Requirements for Seller…

Overview

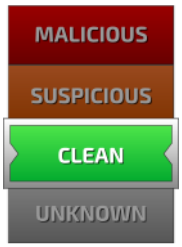
General Information

Sample Name:	SCM Requirements for Sellers during COVID-19 - FINAL JULY 12 21 FINAL.pdf
Analysis ID:	446654
MD5:	65e60bff8b0523a..
SHA1:	2ad84df8272de40.
SHA256:	1dd7144e5a2639..
Infos:	

Most interesting Screenshot:



Detection

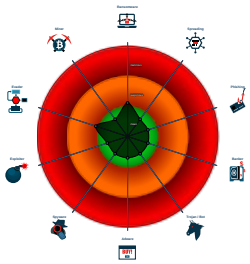


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5816 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5868 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5816 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - AcroRd32.exe (PID: 5952 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' /o /eo /l /b /ac /id 5868 MD5: B969CF0C7B2C443A99034881E8C8740A)
      - AcroRd32.exe (PID: 6040 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 /o /eo /l /b /ac /id 5868 MD5: B969CF0C7B2C443A99034881E8C8740A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

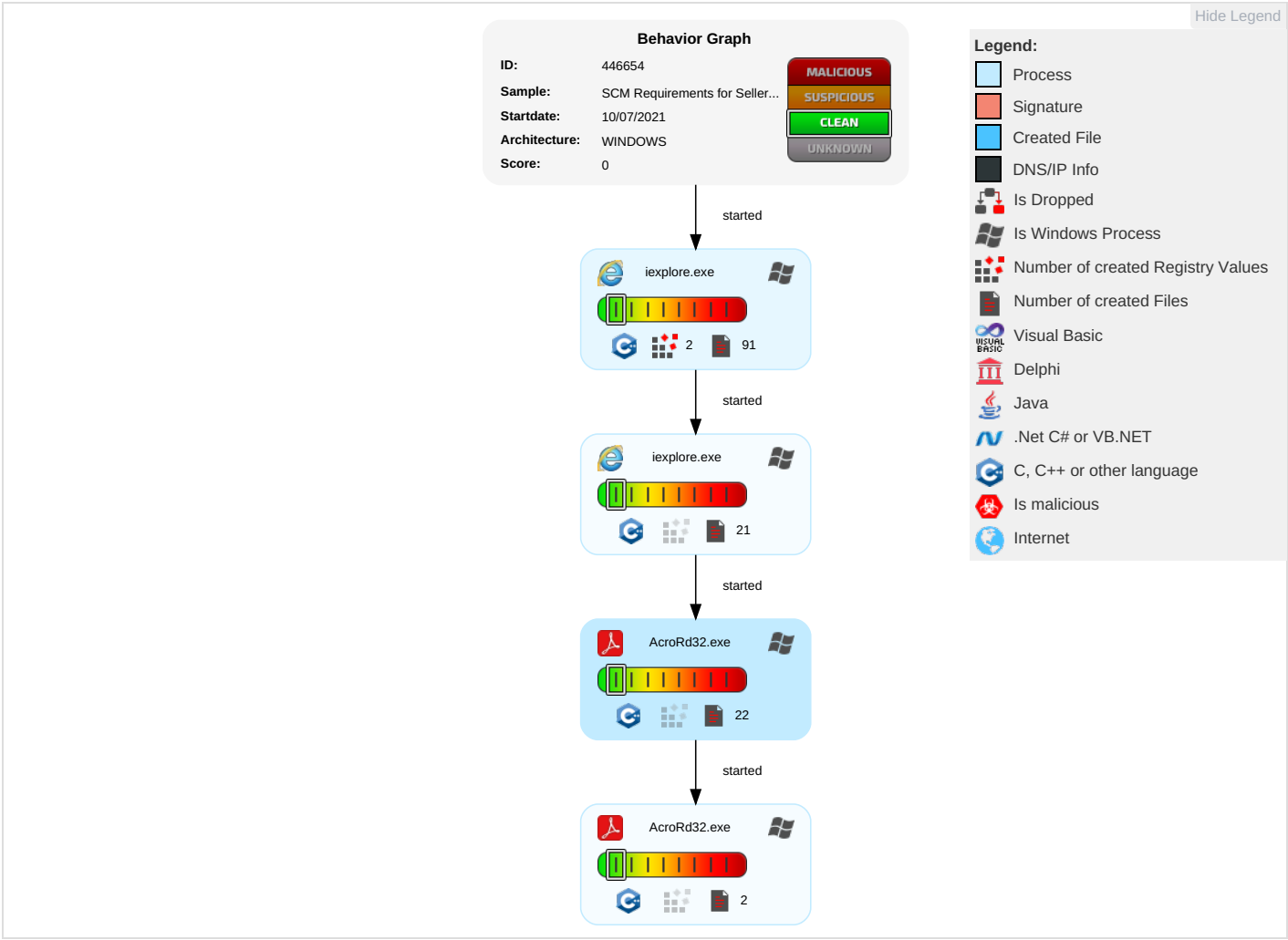
Click to jump to signature section

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	Impact
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	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

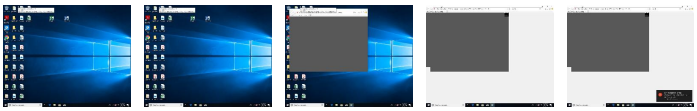
Behavior Graph

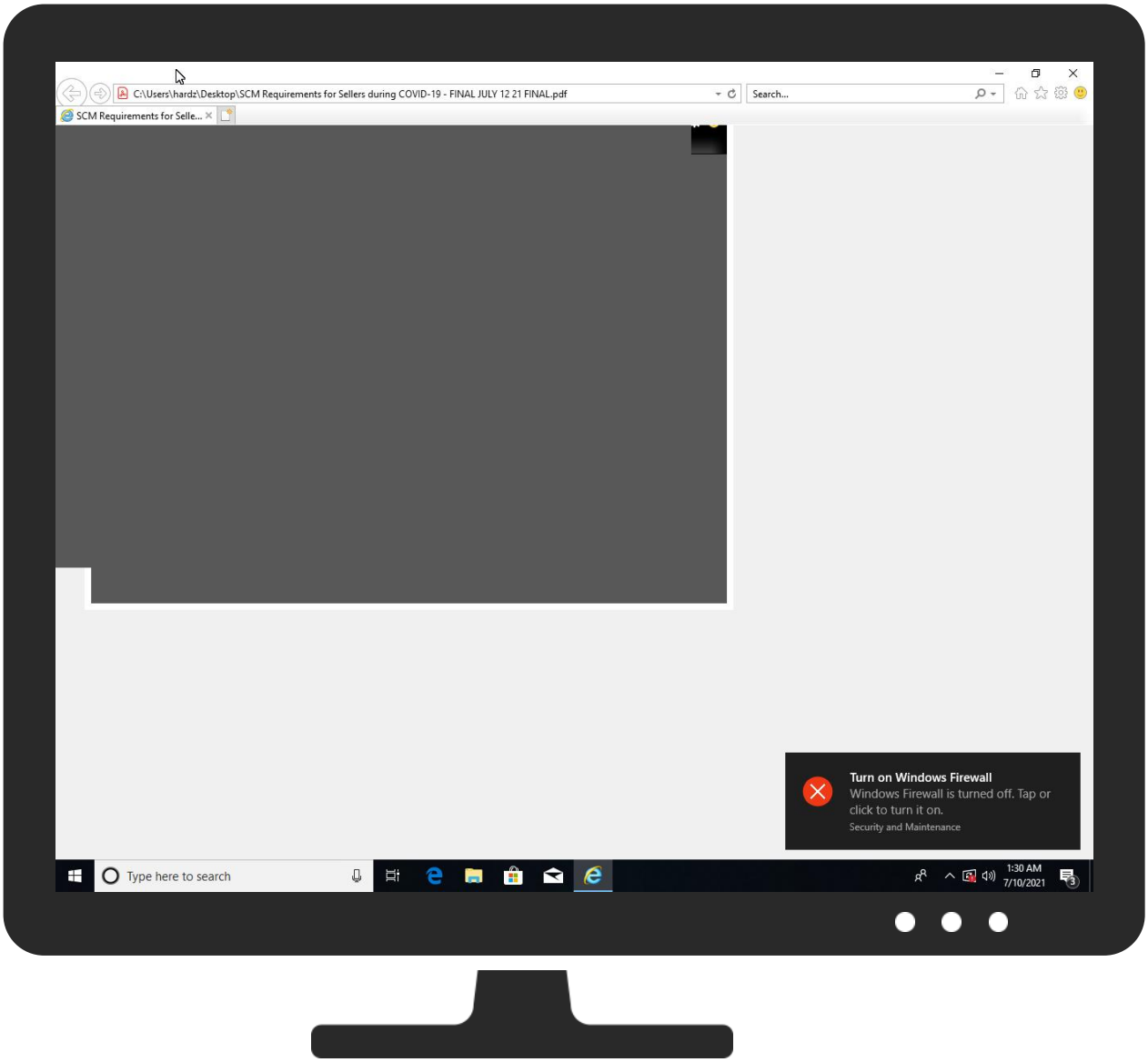


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	446654
Start date:	10.07.2021
Start time:	01:27:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SCM Requirements for Sellers during COVID-19 - FINAL JULY 12 21 FINAL.pdf
Cookbook file name:	defaultwindowshtmlcookbook.jbs
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:	24
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.winPDF@7/15@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .pdf
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.{BEF748A0-E158-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8723867146155309
Encrypted:	false
SSDEEP:	96:rSZJZbX2bKWb7htb7hfb7RRMb7pYb7Nb7wb7ytb70i3:rSZJZT2mWxtxfBRMZY9Aitki3
MD5:	456268A88A54E2E92F4F30FE4B29927D
SHA1:	A0AA1B7D41AA1224CFD56462F06265415C455E57
SHA-256:	5425AF1998A7431A59D02E51E14AD27FEA633FC9CB662022DEDB1836BED712B1
SHA-512:	7FACF1977B82999F7B6D0A54BB892F221075681A36925D28A7CA9ED81F093AA3498BFEB6997B71F1859A6025975D6EDCBFC640D0B0FC439BFC32883A23AA705E
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\{BEF748A2-E158-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27116
Entropy (8bit):	1.750182820432524
Encrypted:	false
SSDEEP:	96:rtZKQ+66BSTjNfL2NdVWNKMNl11j8JW1oKA:rtZKQ+66kTjNfL2NdVWNKMNlPj0U3A
MD5:	BC5395152A2EA417006ED1CA24B52774
SHA1:	7C8AF14CE5DABFED12355B81FCF6A62EF43DECEB
SHA-256:	36C38AC1E185EF5B16D0D1F183DA764DC96C049860C451EF72348958A8556B8E
SHA-512:	7B9B8A1C4040573DBB9810737195FB83AEFB930D6A64AA48CD16B75F8786D9CD40AA9A8FE1031EE5DA1C1FA21ED884250037F6B493905C18EDEBE2F9B17C23 E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BEF748A2-E158-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BEF748A3-E158-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5639854119598748
Encrypted:	false
SSDEEP:	48:IwkGcprtGwpa8G4pQIGrapbS8q9GQpKVG7HpRiTGIpG:r4Z3Qc6WBS82AET2A
MD5:	4FAB506E3495FF145F3542445449993E
SHA1:	2F6B9E73CA0441610CF6A427B97EB907CB2493C1
SHA-256:	2408598FB902D55DD23DDAC670EB18A7130290A7C1417145D129D4393CB153BF
SHA-512:	C1D27E5BFE7C25E48DA9F782DD7A055D0DA208B46DB113313E6BF0C6CA1A40EB5BBC5B1D09757A30DBCAC13FDC34484EDB48E69270005DD14664D45174997A5
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):	5.123521259946243
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEImtmgnWimI002EtM3MHdNMNxOEImtmgnWimI00ObVbkEtMb:2d6NxOrmtmgSZHKd6NxOrmtmgSZ76b
MD5:	684634A6581A6F29B5171504EA355A02
SHA1:	8D0A15A17FA31EEC549B20E4D41B1A5D77D23208
SHA-256:	2F3EBB1A8DBEEC6F234318180659ABBB9146ACC11341FD75D7B6A7F69F849915
SHA-512:	2414B0FE1A88B4B232437D87BC78287EDA668C50491F1508DCB1253B3FF81630BB6DEE7287563F906BBD1B4F2F510E68316E36F1185D3EEB51AAA72E6F7E2312
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x9480470d,0x01d77565</date><accdate>0x9480470d,0x01d77565</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>0x9480470d,0x01d77565</date><accdate>0x9480470d,0x01d77565</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):	5.1757579353923155
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kbKWnWimI002EtM3MHdNMNxe2kbKWnWimI00Obkak6EtMb:2d6Nxr4SZHKd6Nxr4SZ7Aa7b
MD5:	D3C5B3BC01E5C7C298E876DC5C54C121
SHA1:	C2C555E86BFF3140295F24BC56C9580A4DD1ECD3
SHA-256:	5C3A76A239A3F5CE495956D8FDB25C964D01040BD77C7FD9063BD0BB38057DAE
SHA-512:	B810512BD35FA668527A20E4245D51E9492DB5AB4A1D48CB4FAD55F7A0E970A3DEE8796441F70603414931DA703AFD0FAB58069658A95BCD8BCA84269F5EEC9F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x94792029,0x01d77565</date><accdate>0x94792029,0x01d77565</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>0x94792029,0x01d77565</date><accdate>0x94792029,0x01d77565</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):	5.14197931262454
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLImtmgnWimI002EtM3MHdNMNxvLImtmgnWimI00ObmZEtMb:2d6NxvsmtmgSZHKd6NxvsmtmgSZ7mb
MD5:	1EA75A91BEC291EB4D469AA9DC74A004
SHA1:	E6F4DA6D27AB049F3C2983CF826CAC18FA8D527A
SHA-256:	883AE49FEC27791B8CC6907BB06BA772136D96F3C9A64856990EDAA905AD8823
SHA-512:	50A8FE2B5546A9351328EB49953882128AAE7F1E5B887581B04AAEC12726513235BA16C9E6385C7401104CECBDA0840DABEACC10B2DA371F0B521DE3C8824E9A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x9480470d,0x01d77565</date><accdate>0x9480470d,0x01d77565</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>0x9480470d,0x01d77565</date><accdate>0x9480470d,0x01d77565</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):	5.169036851737172
Encrypted:	false
SSDEEP:	12:TMHdNMNxibKWnWimI002EtM3MHdNMNxibrmgnWimI00Obd5EtMb:2d6Nx2SZHKd6NxkmgSZ7Jjb
MD5:	987C9D741E455CBC8E92152F79610E2A
SHA1:	0B5C87469E08AC87B673799E036CE4173C728AF1
SHA-256:	30355BBF97FA70BF6E7829EC41FF71C23820EDBD4FB59331948F13DFBB971BC9
SHA-512:	EAD742206E092D142C938026868F188B2B0E3BB36E2349212E8ED3F6484FCDD3BB3232C658C808E2099339F88CEDF9C7787157D2517AE2B14B1DBDDBEF76535
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x94792029,0x01d77565</date><accdate>0x94792029,0x01d77565</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>0x94792029,0x01d77565</date><accdate>0x9480470d,0x01d77565</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):	5.193446235028963
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwJnWimI002EtM3MHdNMNxhGwJnWimI00Ob8K075EtMb:2d6NxQYSZHKd6NxQYSZ7YKajb
MD5:	FA25ED624DF2FDA47AFF5770E1FA989C
SHA1:	574596991379021086DA674C5AECAF7A20A1D179
SHA-256:	4BDAC41D6BD985DA6024E52D6556372542AC9B16A633D4B1AB1848A854DF2A9E
SHA-512:	1F3876AC5B3CDD44025C7B38646FC38C43730EA1D97C3A6775E32D1AF6AC430EFB6EF54FD3C488DEB6B8D307A46A2B77FC985D5D3F4AC1C568266DA38F924BC9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x94876e29,0x01d77565</date><accdate>0x94876e29,0x01d77565</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>0x94876e29,0x01d77565</date><accdate>0x94876e29,0x01d77565</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Entropy (8bit):	5.124393907750963
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nImtmgnWimI002EtM3MHdNMNx0nImtmgnWimI00ObxEtMb:2d6Nx0ImtmgSZHKd6Nx0ImtmgSZ7nb
MD5:	7698523B60C066EC412B4B569BA01D25
SHA1:	3CF5842A437389BFD16BC93552EFF05C22CD7911
SHA-256:	586ABA0CDB02F288E872297F883AB458A7EE342A88FBF756CC085A84AE46BF60
SHA-512:	1737630A49CE40C00D6736A2CDB173085A1960A110BD8F476D7632433908C1DEA2503CCE6997B124CFD06599557D78512B33415FDFC58E2EE983456B1E557667
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x9480470d,0x01d77565</date><accdate>0x9480470d,0x01d77565</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>0x9480470d,0x01d77565</date><accdate>0x9480470d,0x01d77565</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):	5.163944961216941
Encrypted:	false
SSDEEP:	12:TMHdNMNxxImtmgnWimI002EtM3MHdNMNxxImtmgnWimI00Ob6Kq5EtMb:2d6NximtmgSZHKd6NximtmgSZ7ob
MD5:	3517A4EB0DA85C40D1F77410C2FFCD66
SHA1:	34A140817F8DACE1A65A48D357C4D38FBA087596
SHA-256:	A7E7097979A1FB5A1CBCCC3245113FD33C41FD833F593FC8ACEFCBB4A294A127
SHA-512:	C3529810C78AA9FC2678BD58E2F19C83846DAD66C73E1B1D1CB33B8A98E965B297AC63A1012C16A9A37DCD21F55341052B1FB5809F9DF866A9A92FB4CFF4F65
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x9480470d,0x01d77565</date><accdate>0x9480470d,0x01d77565</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>0x9480470d,0x01d77565</date><accdate>0x9480470d,0x01d77565</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):	5.1738619691987635
Encrypted:	false
SSDEEP:	12:TMHdNMNxcbKWnWimI002EtM3MHdNMNxcbKWnWimI00ObVEtMb:2d6NxgSZHKd6NxgSZ7Db
MD5:	F8ACC5E62973C6D921639DD1C6A239B4
SHA1:	AF25E807D7A3E079FA00F193C45FE3070467C867
SHA-256:	5FD8A26F05379610E34CF89D457E4448225606F336D7FFB35F0B7DEFD50EEB13
SHA-512:	EC349B2B1CF38DD82F112C4D6C06EA6EBC9CD16A0D6BA43A2FE8D5001A72172B0451E0B10FFEF7B9D088863C08D68501615309C290549F65FA89508771BFEE3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x94792029,0x01d77565</date><accdate>0x94792029,0x01d77565</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>0x94792029,0x01d77565</date><accdate>0x94792029,0x01d77565</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):	5.154197668045525
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnbKWnWimI002EtM3MHdNMNxfnbKWnWimI00Obe5EtMb:2d6NxlSZHKd6NxlSZ7ijb
MD5:	4D26BCF5DF1F350C63A5999C8A820D02
SHA1:	68880048F9B856A8D7D8F48C61713A54D493494D
SHA-256:	838FD1A759B7F2BCDFDE9769E03B799A45CB775F7BDB7482AF32A0DD0F853240

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA-512:	6B95452FE3BB8B0E834085BD8D437F07164D7DE2822CFF6AF64A69F571F0969313117D43A3890E7C0CA40C347E18359AF19AF1936BCDE3B89059D137547B3F47
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x94792029,0x01d77565</date><accdate>0x94792029,0x01d77565</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>0x94792029,0x01d77565</date><accdate>0x94792029,0x01d77565</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Temp\~DF7A6BB424845185F6.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
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC22B9CC0E3CA76DE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5119802161770426
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lobqF9lobm9lWbb9ChhCNShCB:kBqoIbxb3bb9CjCNQCB
MD5:	CC1B1ADDCE28AB62F06F38858A4B3882
SHA1:	DEBA19A5E0D04E23B363B4995EAD4EE7257A7A28
SHA-256:	B90796D0CC0465900628907FB0838CD07DA5E2288A92CBDF7054BCE9D2C4DC6D
SHA-512:	9D6A893E1883A0B1B141B52D56F2FD1A4B92F4FCE97F5C64FA81F8ED529E2D0C35780F170FDCE241A6E9F96B0DA9224E6A55A2BCA69A8BD5610952647B1C8161
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFEDD5BCE5AB102DBA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38653
Entropy (8bit):	0.406427771420416
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+NMNqNwNRNdINdZCmjdcVSCmwcV:kBqoxKAuvScS+NMNqNwNRNaN31jZ1
MD5:	EFBD1F1639296066C876A857336A20D2
SHA1:	FB406207012FDBCB2DF11D986B6CBE3A6596545A
SHA-256:	852F545C52CA93947A28AAEF010F0516C3D83C8AB31464013863EC8AA6694816
SHA-512:	102AA02FD17F027FF66753BBF39924F22489D472DBA6E733F9E56F9A649E9B2E3A6B8256434888228454137AECE8C79B1D81C55F1A99EF8BABF92FB1E6F58682
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	HTML document, ASCII text
Entropy (8bit):	4.982031180418199
TrID:	• HyperText Markup Language (15015/1) 100.00%
File name:	SCM Requirements for Sellers during COVID-19 - FINAL JULY 12 21 FINAL.pdf
File size:	317
MD5:	65e60bff8b0523a162ae96668ee24a1c
SHA1:	2ad84df8272de40de999d8c77b8a9beea1fb0b14
SHA256:	1dd7144e5a2639935ad32cfd8d9b464985165298c737a027e737811398e1f7aa
SHA512:	47813f6ef747d0edf3637e716c392458cb94f85d8c24fd223fcab0525b0161438c4162f6a2f229f3b8988ecaf5fb4d35742b6d6fb2393a6309bfb22d008eda4a
SSDEEP:	6:hxuJL/ps6OqB10L98lV9zYwUQJqbc0MYkFbmNYQCI6xRMGOF8uJYUuahX4QL:hYoVH3G9j2bmx9Giu7ahoQL
File Content Preview:	<!DOCTYPE html>.<html>. <body style="font-family: Arial, sans-serif;">. Updated 7/12/2021 - GM SCM COVID-19 Requirements . Good morning, There is an update to the GM SCM COVID-19 requirements. Please check the attched fil

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/10/21-01:31:05.954900	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	192.168.2.1

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5816 Parent PID: 792

General

Start time:	01:28:04
Start date:	10/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7b4760000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 5868 Parent PID: 5816

General

Start time:	01:28:05
Start date:	10/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5816 CREDAT:17410 /prefetch:2
Imagebase:	0xed0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: AcroRd32.exe PID: 5952 Parent PID: 5868

General

Start time:	01:28:07
Start date:	10/07/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' /o /eo /l /b /ac /id 5868
Imagebase:	0x1300000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Registry Activities — Show Windows behavior

Key Created

Analysis Process: AcroRd32.exe PID: 6040 Parent PID: 5952

General

Start time:	01:28:09
Start date:	10/07/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 /o /eo /l /b /ac /id 5868
Imagebase:	0x1300000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Disassembly