ID: 358586
Sample Name:
CTR00068CP1XML.XML
Cookbook: default.jbs
Time: 21:51:18
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

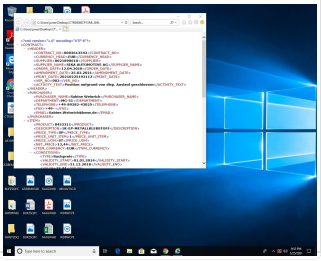
Analysis Report CTR00068CP1XML.XML

Overview

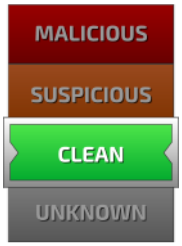
General Information

Sample Name:	CTR00068CP1XML.XML
Analysis ID:	358586
MD5:	63c074333d2e47..
SHA1:	6c8fb2fc7414107..
SHA256:	7c8f59920023503.
Infos:	

Most interesting Screenshot:



Detection

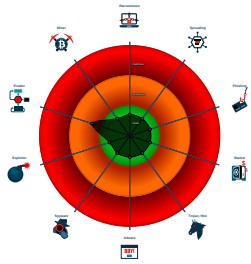


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Contains capabilities to detect virtua…
- Creates a process in suspended mo…
- Monitors certain registry keys / valu…

Classification



Startup

- **System is w10x64**
- MSOXMLED.EXE (PID: 7144 cmdline: 'C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\MSOXMLED.EXE' /verb open 'C:\Users\user\Desktop\CTR00068CP1XML.XML' MD5: 77F586C2DB0175DD4AA085531A82C88A)
  - iexplore.exe (PID: 4584 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' C:\Users\user\Desktop\CTR00068CP1XML.XML MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 2016 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4584 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

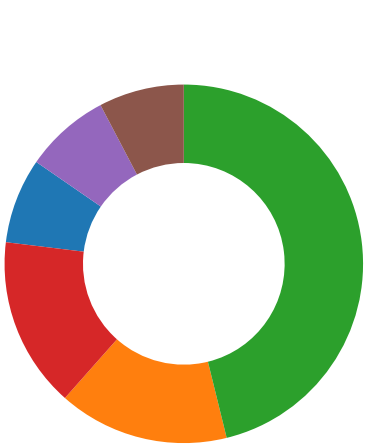
Yara Overview

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

Mitre Att&ck Matrix

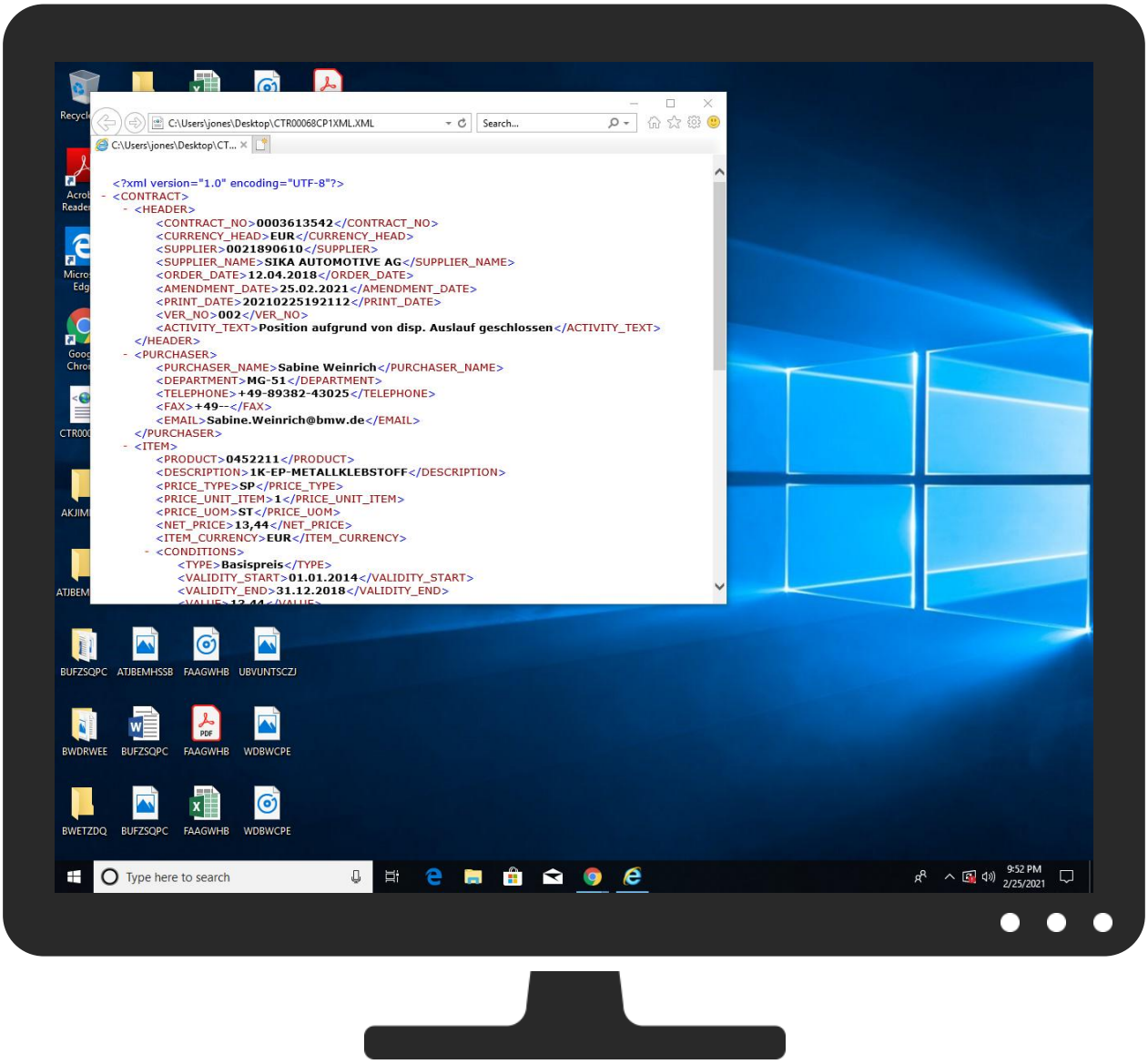
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

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
CTR00068CP1XML.XML	0%	Virustotal		Browse

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

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.2.dr	false		high
http://www.nytimes.com/	msapplication.xml3.2.dr	false		high
http://www.live.com/	msapplication.xml2.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.2.dr	false		high
http://www.twitter.com/	msapplication.xml5.2.dr	false		high
http://www.youtube.com/	msapplication.xml7.2.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358586
Start date:	25.02.2021
Start time:	21:51:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CTR00068CP1XML.XML
Cookbook file name:	default.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:	15
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:	clean1.winXML@5/14@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .XML

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 23.54.113.53, 104.43.139.144, 52.255.188.83, 13.64.90.137, 88.221.62.148, 52.147.198.201, 168.61.161.212, 51.104.144.132, 152.199.19.161, 52.155.217.156, 20.54.26.129, 67.27.158.126, 67.27.158.254, 67.26.81.254, 67.27.159.254, 8.248.119.254, 92.122.213.194, 92.122.213.247, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.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.{51D9031F-77AB-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24152
Entropy (8bit):	1.7599278192397318
Encrypted:	false
SSDEEP:	96:rddZXo7ZQB2+OWZfO3tZnufZnt5CtZntQjhVzWZktQC9/:rDZ0Zk2NWZstZufZbCtZYhVzWZI9/
MD5:	0D9D1A71B38FD70DD7299E2597CDB703
SHA1:	8B73B450954E8C35520EBE84641AF3C037BD87B6
SHA-256:	35CF0D16D04767AD288E93B7A214C5F75F45230D0E92815E23F037F0D939CF7F
SHA-512:	18A93766ECC74D26ADE9DDF88E6FEBFDED01C7A7ECBA4E03C76DBBD2FB3BD3B35E5C2236391F5409505742C127A641196057137022ED1A9C87AE14313BDE01B8
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\{51D90321-77AB-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	23640
Entropy (8bit):	1.7277758296265213
Encrypted:	false
SSDEEP:	48:IwOGcprdhGwpafG4p1mwYeTGPHpnewYe/TGMpVwYeYUGKXpbvgwYe1Gpp7vgwYep:rSZd7QxXmz9eInpi5YXZYxDkdrrh
MD5:	F2548FC5D85600DF19490D8B6FF950B3
SHA1:	1E77470430C9C58A30149FB93F58AF9FE3A4BD58
SHA-256:	1BE830F7B70D6B85184707EEB2E3658034158698DAD448510C82942A8AE04665
SHA-512:	47AB6EC7296EDCB53487A69793A7430D36165B9CBA6EE134DDE0FB33A9AE71F8B8E1BA43C62B47BCCF78F0970A26FABDAC9F92D54F5CD52310439AB1E4401AEC
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):	5.062679807225529
Encrypted:	false
SSDEEP:	12:TMHdNMNxOElaNPAnWiml002EtM3MHdNMNxOElaNPAnWiml00OYGVbkEtMb:2d6NxOI2ASZHKd6NxOI2ASZ7YLb
MD5:	6F54F7A1121B4DF4990AA4F33F79146A
SHA1:	62CAC18053860A8150E858741A05BA409DC97717
SHA-256:	7DAD0BFD59EC66A6FC036A256E4CB053443B6BA0062DB3D2931F0F47287C7C76
SHA-512:	9FEE31BDCE8B031A501B6587A38998EE983CA9FAA5954CD7620B5765F6EFEFAB2221FD4F05E091F83AF245993C66EC16CF80A3EDC12C41A2D5A7DF449869F06
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x271b7f7e,0x01d70bb8</date><accdate>0x271b7f7e,0x01d70bb8</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>0x271b7f7e,0x01d70bb8</date><accdate>0x271b7f7e,0x01d70bb8</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):	5.148398441419817
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kGY2aNsY2AnWimI002EtM3MHdNMNxe2kGY2aNjdAnWimI00OYGkakU:2d6Nxr82W2ASZHKd6Nxr826dASZ7Yzan
MD5:	60F77D9D3F633AACF986A41ECF0D8A86
SHA1:	56E38443183D8A8C5E12ED0FFDFEE56AF49285D2
SHA-256:	D1A5AA3EFE0AF0234735521C974AA029BF4ED8B1745F1BEA965BECB8D466592D
SHA-512:	6B285EA03D3C69AD785AF0ACC082A3AC2D1A95A066450E9D6386F3C64F1B3333836CF4D726671C69ECE329AC161FAADFFD5950ABC31AE9DE8861B95EC7E4E61
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x27145854,0x01d70bb8</date><accdate>0x27145854,0x01d70bb8</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>0x27145854,0x01d70bb8</date><accdate>0x2716bab0,0x01d70bb8</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):	5.070930277869505
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLIaNeAnWimI002EtM3MHdNMNxvLIaNeAnWimI00OYGmZEtMb:2d6Nxv0/ASZHKd6Nxv0/ASZ7Yjb
MD5:	82615FFC4CC02B47308A58286FD239AE
SHA1:	D3A58886D3F160040565F5BF158B83FC6D96C0C7
SHA-256:	EC46382322D17E1BBA0BCE3B1800DE93C7774A32C380B1E1E92EACF936997402
SHA-512:	15CAD4528D306D67E6C6704AF6227625888A973BEC54049E49CE6F0F1396405A5F78702EDE2C70A90C284B268AF30B3090E082BC7C241FFD77D5A925F02BCF24
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x271de1b0,0x01d70bb8</date><accdate>0x271de1b0,0x01d70bb8</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>0x271de1b0,0x01d70bb8</date><accdate>0x271de1b0,0x01d70bb8</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):	5.095203237915045
Encrypted:	false
SSDEEP:	12:TMHdNMNxiH0aN90AnWimI002EtM3MHdNMNxiH0aN90AnWimI00OYGd5EtMb:2d6NxG0q0ASZHKd6NxG0q0ASZ7YEjb
MD5:	CC4938748C29FC737CC18EC635969F97
SHA1:	5D326D339BC3496C850C1C5864FEA7DD870A056A
SHA-256:	7163E29CA1B3F4FD667F42D47EC45264314F9BAFD154FE371D1B9B5523AA53B9
SHA-512:	B70FDE9A0D702C9652CB182925E7825FD87F09A4E3778DFAF92610E9B938CECCECE14E41BF17058AE87892D9F59BF2D20F85E6AC8A3C96FE4F57F8AAAE74F65
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x27191d0b,0x01d70bb8</date><accdate>0x27191d0b,0x01d70bb8</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>0x27191d0b,0x01d70bb8</date><accdate>0x27191d0b,0x01d70bb8</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):	5.078162752007357
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwIaNeAnWimI002EtM3MHdNMNxhGwIaNeAnWimI00OYG8K075EtMb:2d6NxQZ/ASZHKd6NxQZ/ASZ7YrKajb
MD5:	4384534A9D8A6E6617FB7B96162AE344
SHA1:	A46EB9F7E2E51669D6E5D1B439FCEA6684FDE2FF
SHA-256:	244F47FB073DC00DC5DCD09520CEB141FB4EF30BF04CB2A00F0C62A70D2DCDDE
SHA-512:	578C0E48F6F3293D3F0337EE77E07014DF81462097ABC8CA743A9BC1324A32A28441ADF809460D200AA7E5039A1E6F45759B3B32F0F5A31EF8259A967ADF1BD6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x271de1b0,0x01d70bb8</date><accdate>0x271de1b0,0x01d70bb8</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>0x271de1b0,0x01d70bb8</date><accdate>0x271de1b0,0x01d70bb8</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):	5.066298468832412
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nlaNPAnWimI002EtM3MHdNMNx0nlaNPAnWimI00OYGxEtMb:2d6Nx0l2ASZHKd6Nx0l2ASZ7Ygb
MD5:	3E7D740C10ABC764BE20900D7ACB6D79
SHA1:	141E8E93AF8F0539BD9F548078011A7EE1C9E878
SHA-256:	8C714A4AAC5025987556991CA1367FB0D0F7A93FAD64AAFFF318C049F90732A7
SHA-512:	BEBB4614FEBEB74631C6865BF6747541583BF0359688E2F6BA66E28ACABEF9C728294DD0D7B3E5A25F6E10834DFD7CC709FD8B55A7827CCEB0DDC244709A076
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x271b7f7e,0x01d70bb8</date><accdate>0x271b7f7e,0x01d70bb8</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>0x271b7f7e,0x01d70bb8</date><accdate>0x271b7f7e,0x01d70bb8</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):	5.102315086553323
Encrypted:	false
SSDEEP:	12:TMHdNMNxxlaNPAnWimI002EtM3MHdNMNxxlaNPAnWimI00OYG6Kq5EtMb:2d6Nxb2ASZHKd6Nxb2ASZ7Yhb
MD5:	B0314B70D4C0A0C20EC88D3C556B4EE6
SHA1:	FDE3E31E2D49FCD28B29222B0EDC9A91ECE99D32
SHA-256:	D99ABDCB95C9B9C999124D9FB7EC2039AE4189AA90DCB62DC01196B0B2F86B42
SHA-512:	A482E606FFE60F8FC1324FECA711D0AE2EF02716FB16CCE62985C05E83F7734013A43270101E18FAFCC58FADBE7138A3A98FB61C7B3469AB72C27159B77BE81
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x271b7f7e,0x01d70bb8</date><accdate>0x271b7f7e,0x01d70bb8</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>0x271b7f7e,0x01d70bb8</date><accdate>0x271b7f7e,0x01d70bb8</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):	5.0935683289258415

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxcH0aN90AnWimI002EtM3MHdNMNxcH0aN90AnWimI00OYGVEtMb:2d6Nx40q0ASZHKd6Nx40q0ASZ7Ykb
MD5:	2351F392A57C1BAE411B162B03329C2A
SHA1:	3DF5D2EC9B872FE0DC5B44B9C9870E15BC239F7D
SHA-256:	44B1749A822CC0D9751E29AC36DA69776241628704C953FAA72921398935AC7F
SHA-512:	F34FE886F0A55159AD2292922BF73A16927A335F600573782C0D837EF97DBF2A56A0108966C2A8475536B9C8B427E485D2143A8A2C2EBD2E955DC1D59D14574A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x27191d0b,0x01d70bb8</date><accdate>0x27191d0b,0x01d70bb8</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>0x27191d0b,0x01d70bb8</date><accdate>0x27191d0b,0x01d70bb8</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):	5.0806768261440824
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnH0aN90AnWimI002EtM3MHdNMNxfnH0aN90AnWimI00OYGe5EtMb:2d6Nxv0q0ASZHKd6Nxv0q0ASZ7YLjb
MD5:	523B0067A4E5067DB51F24EBBDFF4783
SHA1:	EEC34C2436AE1A8AEEF81029A90D64BD88EED22B
SHA-256:	03F52C727EB08239701DD84CF2F68CA385859344594807C10E4357C7DDF63A84
SHA-512:	1A3ED46B4AA0D05AB926E787CB04A608821C9B3EA9C6DA1A1692155473961539339616456548FDD71BA115789D4CD20E43FC0B7AE3D454C74519F4E8F02A0FE3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x27191d0b,0x01d70bb8</date><accdate>0x27191d0b,0x01d70bb8</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>0x27191d0b,0x01d70bb8</date><accdate>0x27191d0b,0x01d70bb8</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\xmltreeview[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	17524
Entropy (8bit):	4.340063035506032
Encrypted:	false
SSDEEP:	192:wiuFhk5un5EpDdblzKaz+OJGbiIBJofNbr5/dn82/jqmo3qAi:rq25unWZd9dvJGiIBJoh387oAi
MD5:	03710426AB25AD1280E197F61249F9DE
SHA1:	F5E7A6FD42503AE4758BC36C8DD78D98EFB35047
SHA-256:	21E63F7C77896ED2B5F115957F2448E0A9E2DD738D7D487E471217421F6A93E1
SHA-512:	213CB55B8573335D1384AE704FF4267F224376056F71548660F9B2FDAA1203D8ABDDB787900AAF5D1E0AC6E5BE261F713BDBEFB67643D08E8D3672512A1AF588
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	res://mshtml.dll/xmltreeview.js
Preview:	(function()..{.. var XHTML = "http://www.w3.org/1999/xhtml";.. .. // Time slicing constants.. var LIMIT = 10; // Maximum number of nodes to process before checking time.. var DURATION = 200; // Maximum amount of time (ms) to process before unblocking UI.. var DELAY = 15; // Amount of time (ms) to unblock UI.... // Tree building state.. var iterator;.. var nextNode;.. var root;.. var rootFirstChild;.. var time;.. .. // Template References.. var attrTemplate, attrName, attrValue;.. var elmStartTemplate, elmStartName;.. var elmEndTemplate, elmEndName;.. var cdataTemplate, cdataValue;.. var commentTemplate, commentValue;.. var style; .. .. // Only invoke this script if it was injected by our parser. Test for a condition that is.. // impossible for a markup to create - two direct children of the document... var secondRootElement = document.documentElement.nextElementSibling;.. if (secondRootElement == null

C:\Users\user\AppData\Local\Temp\~DF57804EB26D01F0F9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34701
Entropy (8bit):	0.44984849215301115
Encrypted:	false
SSDEEP:	48:kBqoxKlmwYe6mwYe0ewYeXewYe1wYeFSwYeY6vgwYeTvgwYeQkwYe5fkwYe5XIps:kBqoxKlmLmjege6vp6YmYJkwkm3
MD5:	C7CB9E57C50883C3386595741132C8D3
SHA1:	F345A194F45BA13C56BEB6D89B8066AF1F948234

C:\Users\user\AppData\Local\Temp\~DF57804EB26D01F0F9.TMP	
SHA-256:	6FBE0670AC7600C6D83DE8794CF55D22E1DB6C8E0402A3620F381D39F7EA0FE6
SHA-512:	2405AF34D191A79968C29CD5E026BCC76A0DA6D7FF0982AE29875D19B4D6D3120FB9959BC7555B832CFCE5B80657D71E9DBD6C4D6C6B08C25243DCBF447EC 3
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFABAAF56B4E43D88B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12965
Entropy (8bit):	0.41687839522456166
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRwF9l8fR49lTqO9Z:c9lLh9lLh9lIn9lIn9loo9lo49lWO9Z
MD5:	8F0CB989BFAF00D5D3CC22F4C0887BC1
SHA1:	231C545A44C4D498D545E7A3E4CDE1FE32592058
SHA-256:	99681DA55BE1170E7397FFA003BA5B49D2B006F13D871C0CB9A0E9D904F35E77
SHA-512:	B4CC75B44ADCBB02849A8E1D42384848AFD9583C8B15BB8F9EB67073254A53B66216DE8725517BB55CF46E7383E03D4228CC098092FAA21EC58166EFD9413DA
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.071805981310584
TrID:	• Generic XML (ASCII) (5005/1) 100.00%
File name:	CTR00068CP1XML.XML
File size:	2058
MD5:	63c074333d2e4746d9da321c93941c4a
SHA1:	6c8fb2fc7414107b7cca214dcef3bd30e3885041
SHA256:	7c8f599200235035ed03dae5e18da4961a71f4f381a02b4b479172cb13a38538
SHA512:	81ab7882fdedf0b8caf0017d5a2cb905e2c4945e2581ad2a5dc47f424c371901ee002fc2bd9ad927c13c90a87fefd04ba5ec9717b6ccbc35a2910de91d2ca04e
SSDEEP:	48:cSan5zBlVL5494BDzmd7NqTuSnavMykHKYxzxRS:9cx3VzIpu7navMyUKYxzxRS
File Content Preview:	<?xml version="1.0" encoding="utf-8"?><CONTRACT><HEADER><CONTRACT_NO>0003613542</CONTRACT_NO><CURRENCY_HEAD>EUR</CURRENCY_HEAD><SUPPLIER>0021890610</SUPPLIER><SUPPLIER_NAME>SIKA AUTOMOTIVE AG</SUPPLIER_NAME><ORDER_DATE>12.04.2018</ORDER_DATE><AMENDMENT_DA

File Icon

Icon Hash:	e4ccd4ccccd6d4d8

Network Behavior

UDP Packets

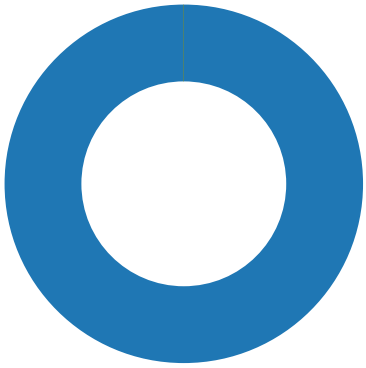
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:51:59.388355970 CET	59123	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:51:59.439922094 CET	53	59123	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:00.336853981 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:00.390525103 CET	53	54531	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:00.521389961 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:00.569787979 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:01.511343002 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:01.561991930 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:03.260380983 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:03.311131001 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:04.712465048 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:04.762527943 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:05.538985968 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:05.590579987 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:07.074266911 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:07.126526117 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:07.330318928 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:07.385862112 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:08.488219976 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:08.538371086 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:09.592072010 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:09.646675110 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:10.379455090 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:10.429874897 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:11.144828081 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:11.199028969 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:12.294450998 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:12.345037937 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:13.416965961 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:13.465939999 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:14.222605944 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:14.271574974 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:15.220835924 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:15.269463062 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:16.230379105 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:16.279181004 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:17.171052933 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:17.224282980 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:17.941698074 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:17.991967916 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:18.888437033 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:18.940488100 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:29.076422930 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:29.129834890 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:37.349268913 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:37.414643049 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:38.257312059 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:38.308598995 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:38.354866982 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:38.406560898 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:39.259438038 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:39.317717075 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:39.368767023 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:39.422754049 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:40.275449991 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:40.325659990 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:41.387204885 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:41.440170050 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:42.117525101 CET	52337	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:52:42.205163956 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:42.322540045 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:42.372592926 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:42.757308006 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:42.848768950 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:43.385538101 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:43.454185963 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:43.517832041 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:43.591595888 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:43.857984066 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:43.919640064 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:44.444902897 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:44.513895988 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:45.143898964 CET	56448	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:45.193085909 CET	53	56448	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:45.400628090 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:45.455884933 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:45.724766016 CET	59172	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:45.787919998 CET	53	59172	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:46.338165998 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:46.388184071 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:46.456851959 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:46.508702040 CET	53	62420	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:47.496530056 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:47.575081110 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:48.065509081 CET	50183	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:48.122950077 CET	53	50183	8.8.8.8	192.168.2.4
Feb 25, 2021 21:52:54.433096886 CET	61531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:52:54.487184048 CET	53	61531	8.8.8.8	192.168.2.4
Feb 25, 2021 21:53:04.270823002 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:53:04.319308043 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 21:53:04.482944965 CET	59794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:53:04.547230959 CET	53	59794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:53:07.267049074 CET	55916	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:53:07.325551987 CET	53	55916	8.8.8.8	192.168.2.4
Feb 25, 2021 21:53:40.448707104 CET	52752	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:53:40.500252008 CET	53	52752	8.8.8.8	192.168.2.4
Feb 25, 2021 21:53:41.923402071 CET	60542	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:53:41.983699083 CET	53	60542	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: MSOXMLED.EXE PID: 7144 Parent PID: 6072

General

Start time:	21:52:06
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\MSOXMLED.EXE' /verb open 'C:\Users\user\Desktop\CTR00068CP1XML.XML'
Imagebase:	0x890000
File size:	220872 bytes
MD5 hash:	77F586C2DB0175DD4AA085531A82C88A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CTR00068CP1XML.XML	unknown	2048	success or wait	1	892C04	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4584 Parent PID: 7144

General

Start time:	21:52:06
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' C:\Users\user\Desktop\CTR00068 CP1XML.XML
Imagebase:	0x7ff6db1a0000
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

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: 2016 Parent PID: 4584

General

Start time:	21:52:07
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:4584 CREDAT:17410 /prefetch:2
Imagebase:	0x10f0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Disassembly