



ID: 452438
Sample Name: order_07.21.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:00:15
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report order_07.21.doc 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
System Summary: 4
Data Obfuscation: 4
Jbx Signature Overview 5
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 5
Data Obfuscation: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
Private 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 13
General 13
File Icon 13
Static OLE Info 13
General 13
OLE File "/opt/package/joesandbox/database/analysis/452438/sample/order_07.21.doc" 13
Indicators 13
Streams with VBA 14
Streams 14
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 14
UDP Packets 14
ICMP Packets 14
DNS Queries 14
DNS Answers 14
Code Manipulations 14
Statistics 14
Behavior 15
System Behavior 15
Analysis Process: WINWORD.EXE PID: 2696 Parent PID: 584 15
General 15
File Activities 15
File Created 15
File Deleted 15
File Written 15
Registry Activities 15
Key Created 15
Key Value Created 15
Key Value Modified 15
Analysis Process: cmd.exe PID: 2480 Parent PID: 2696 15

Copyright Joe Security LLC 2021

General 15
File Activities 16
Analysis Process: mshta.exe PID: 2232 Parent PID: 2480 16
General 16
File Activities 16
Registry Activities 16
Analysis Process: regsvr32.exe PID: 2544 Parent PID: 2232 16
General 16
File Activities 16
Disassembly 16
Code Analysis 16

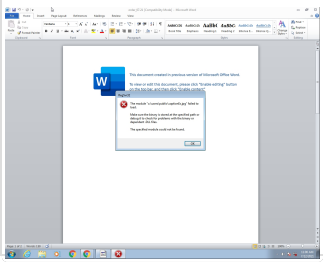
Windows Analysis Report order_07.21.doc

Overview

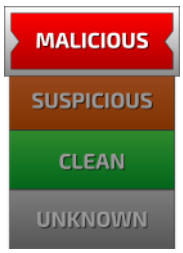
General Information

Sample Name:	order_07.21.doc
Analysis ID:	452438
MD5:	401b19c454075d..
SHA1:	088f76c184a0cba..
SHA256:	6b94e6319e46f52.
Infos:	

Most interesting Screenshot:



Detection

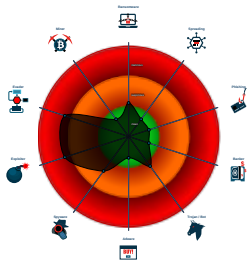


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Register DLL with s…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document exploit detected (process…
- Sigma detected: MSHTA Spawning …
- Sigma detected: Microsoft Office Pr…
- Sigma detected: Regsvr32 Anomaly
- Allocates memory within range whic…
- Creates a process in suspended mo…
- Creates a window with clipboard cap…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2696 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
  - cmd.exe (PID: 2480 cmdline: cmd /c c:\programdata\captionEx.hta MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - mshta.exe (PID: 2232 cmdline: 'C:\Windows\SysWOW64\mshta.exe' 'C:\programdata\captionEx.hta' MD5: ABDFC692D9FE43E2BA8FE6CB5A8CB95A)
      - regsvr32.exe (PID: 2544 cmdline: 'C:\Windows\System32\regsvr32.exe' c:\users\public\captionEx.jpg MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:



Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Anomaly

Data Obfuscation:



Sigma detected: Register DLL with spoofed extension

Copyright Joe Security LLC 2021

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Software Vulnerabilities:



Document exploit detected (process start blacklist hit)

System Summary:



Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

Data Obfuscation:

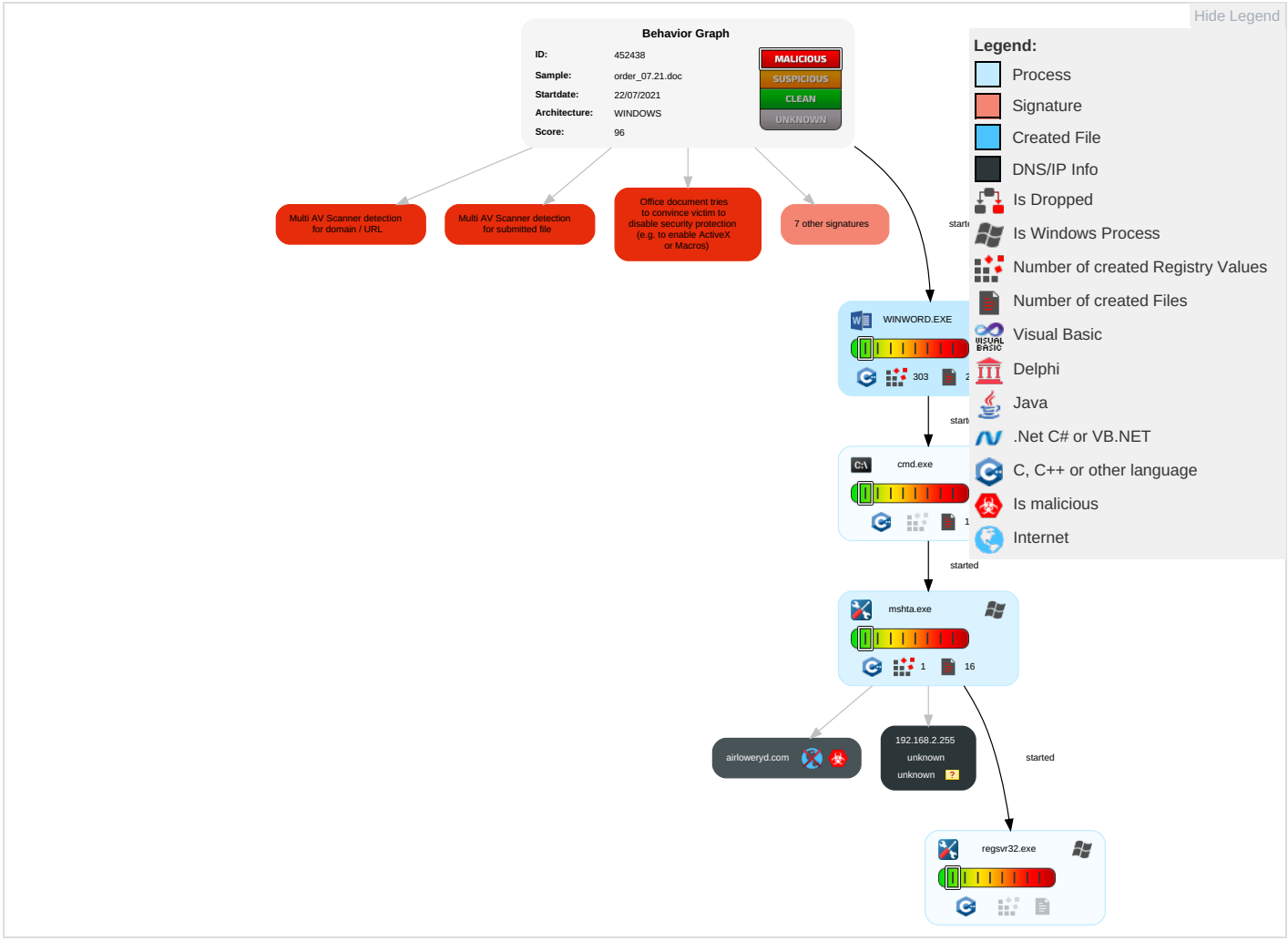


Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 2 2	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop Insecure Network Communic
Default Accounts	Exploitation for Client Execution 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS Redirect Pl Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 2	LSA Secrets	System Information Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service

Behavior Graph

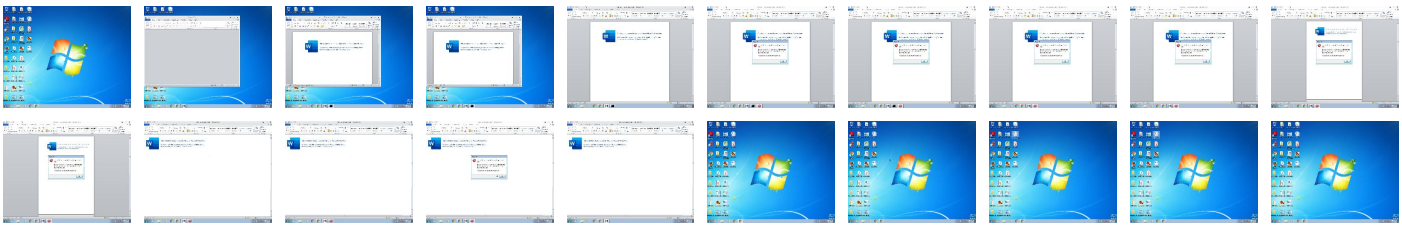
Copyright Joe Security LLC 2021

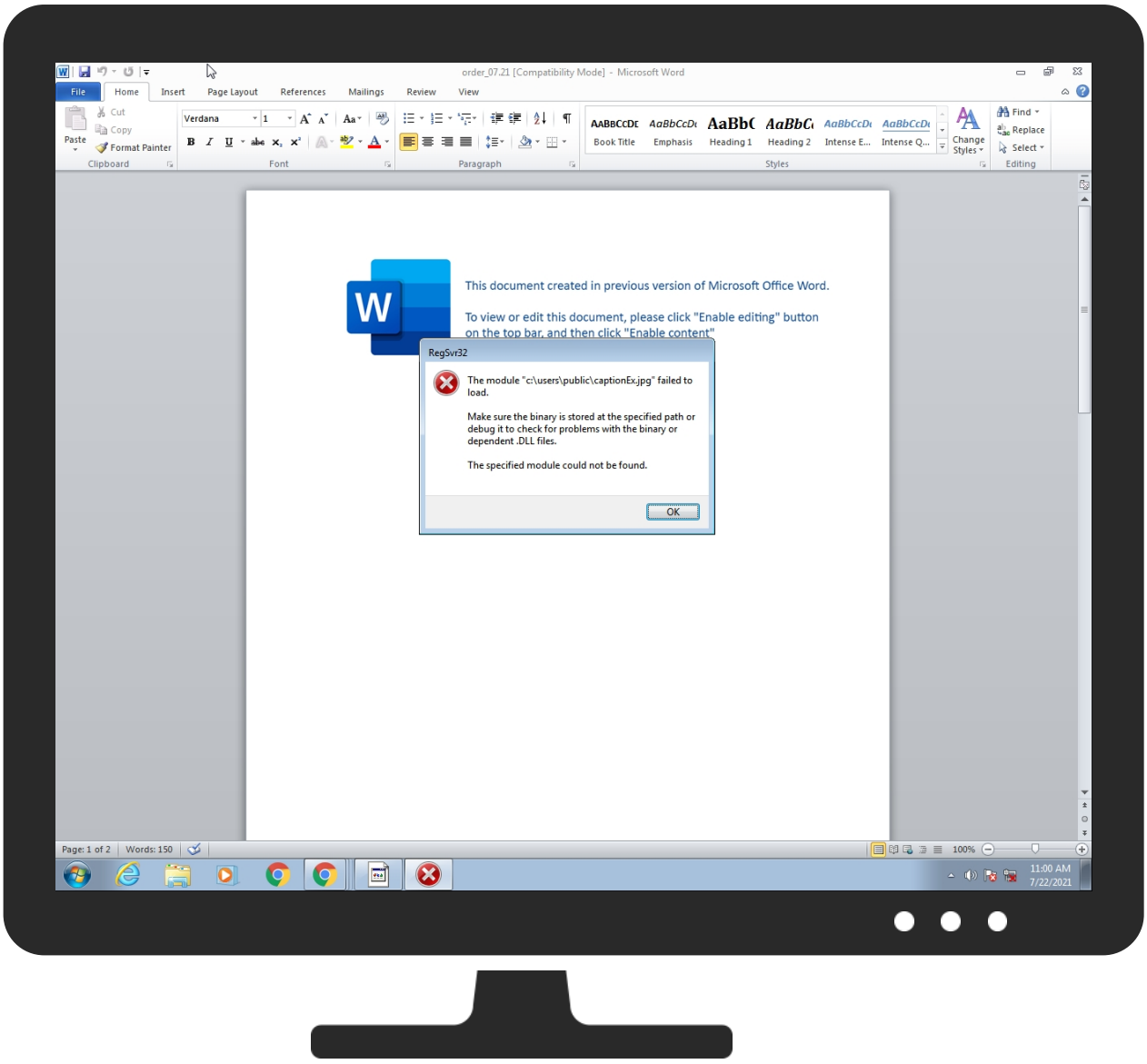


Screenshots

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
order_07.21.doc	48%	Virustotal		Browse
order_07.21.doc	14%	Metadefender		Browse
order_07.21.doc	15%	ReversingLabs	Document-Office.Trojan.Sadoca	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
airloweryd.com	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://airloweryd.com/adda/CzJsZLz8s7e1PAiOuESLghxyuWpr1A46cHBNR/dmIczx3VCKJVxOIM45tzrpZTl8IQ06/ryme	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
airloweryd.com	unknown	unknown	true	• 10%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452438
Start date:	22.07.2021
Start time:	11:00:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	order_07.21.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	7
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

Copyright Joe Security LLC 2021

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.expl.evad.winDOC@8/11@3/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:00:34	API Interceptor	107x Sleep call for process: cmd.exe modified
11:00:35	API Interceptor	86x Sleep call for process: mshta.exe modified
11:00:42	API Interceptor	237x Sleep call for process: regsvr32.exe modified

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:\ProgramData\captionEx.hta	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF, CR line terminators

C:\ProgramData\captionEx.hta	
Category:	dropped
Size (bytes):	3039
Entropy (8bit):	5.8499136819223425
Encrypted:	false
SSDEEP:	48:yAmqAXYLXHqiJXzatwLgXa/1CTaToY/353YaMr8SSjAG75XltCuxa5tD8tlsHsuH:l6YTlhza+gXataeoY/J3YaMrAl7da5t9
MD5:	111964AF02201E77AD219F7562BF19B2
SHA1:	9A48E4281A89383FF5AF45EE2F2BF710704E5152
SHA-256:	FB2A3EB78EF18021BD6DA3398FB8D935FD3884F418DDA72FC123903501B5B503
SHA-512:	141C2DAC7594678BC7DA7DE7E9DFC4E90A6A6B4E5EE5985B03F37E97827B59E0BBB6509D88AB6A3CF129DE2EB1660B90FB953F2ABCE441F5D37154D2F3C347 84
Malicious:	false
Reputation:	low
Preview:	<html>.<body>. fX17KWUoaGN0YWN9O2Vzb2xjLnlyZXVRdHNldXFlcjspMiAsImdwai54RW5vaXRwYWNcXGNpbGJ1cFxcc3Jlc3VcXDpjIhlbGlmb3RldmFzLnlyZXVRdHNldXFlcjspeWRvYmVzbm9wc2VyLmV0ZWxlRHljbmVycnVDeXBvYyhldGlydy55cmV1UXRzZXVxZXI7MSA9IGVweXQueXJldVF0c2V1cWVyO25lcG8ueXJldVF0c2V1cWVyOykibWFlcnRzLmJkb2RhIih0Y2VqYk9YZXZpdGNBIHdlbiA9IHlyZXVRdHNldXFlciByYXZ7eXJ0eykwMDIgPT0gc3V0YXRzLmV0ZWxlRHljbmVycnVDeXBvYyhmaTspKGRuZXMuZXRlbGVEeXNuZXJydUN5cG9jOyllc2xhZiAsInJhS3BVS3Z5PWVtaXQmek5TS2d4WTNVUFpjaUI9ZmVyJmdrN1NJZkg4bGJLZjVHVXZrTGxHWlo9ZGkmbDhyRnBqM1phb0ptYjJKYT1lZ2FwJmtCNGtmeGlaUFJJNnRBcj1kaSZiajVTM3RuMEpjbUY9ZGlzJm9DPXhjRT8xc2VteXIvNjBRSThsVFpwcnp0NTRNSU94VkpLQ1YzeHpjSW1kL1JOQkhjNjRBMXJwV3V5eGhnTFNFdU9pQVAxZTdzOHpMWnNKekMvYWRkYS9tb2MuZHlyZXdvbHJpYS8vOnB0dGgiICwiVEVHIihuZXBvLmV0ZWxlRHljbmVycnVDeXBvYzspInB0dGhsbXguMmxteHNtIih0Y2VqYk9YZXZpdGNBIHdlbiA9IGV0ZWxlRHljbmVycnVDeXBvYyByYXY=aGkhOykiZ3BqLnhFbm9pdHBhY1xcY2lsYnVwXFxzcmVzdVxcOmMgMjNydnNnZXIiKG51ci5ITGxhdjspInRjZWpib21ldHN5c2VsaWYuZ25pdHBpcmNz

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\error[1]	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3247
Entropy (8bit):	5.459946526910292
Encrypted:	false
SSDEEP:	96:vKFlZ/kxjqD9zqp36wxVJddFAdd5Ydddopdyddv+dd865FhlleXckVDuca:C0pv+GkduSDl6LRa
MD5:	16AA7C3BEBF9C1B84C9EE07666E3207F
SHA1:	BF0AFA2F8066EB7EE98216D70A160A6B58EC4AA1
SHA-256:	7990E703AE060C241EBA6257D963AF2ECF9C6F3FBDB57264C1D48DDA8171E754
SHA-512:	245559F757BAB9F3D63FB664AB8F2D51B9369E2B671CF785A6C9FB4723F014F5EC0D60F1F8555D870855CF9EB49F3951D98C62CBDF9E0DC1D28544966D4E70F
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	res://ieframe.dll/error.dlg
Preview:	...<HTML id=dlgError STYLE="font-family: ms sans serif; font-size: 8pt;..width: 41.4em; height: 24em">..<HEAD>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<META HTTP-EQUIV="MSThemeCompatible" CONTENT="Yes">..<TITLE id=dialogTitle>..Script Error..</TITLE>..<SCRIPT>..var L_Dialog_Error Message = "An error has occurred in this dialog.";..var L_ErrorNumber_Text = "Error: ";..var L_ContinueScript_Message = "Do you want to debug the current page?";..var L_AffirmativeKeyCodeLowerCase_Number = 121;..var L_AffirmativeKeyCodeUpperCase_Number = 89;..var L_NegativeKeyCodeLowerCase_Number = 110;..var L_NegativeKeyCodeUpperCase_Number = 78;..</SCRIPT>..<SCRIPT LANGUAGE="JavaScript" src="error.js" defer></SCRIPT>..</HEAD>..<BODY ID=bdy onLo ad="loadBdy()" style="font-family: 'ms sans serif';..font-size: 8pt; background: threedface; color: windowtext;" topmargin=0>..<CENTER id=ctrErrorMessage>..<table id=tbl1 cellPadding=3 cellspacing=3 border=0..style="background: buttonface

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\warning[1]	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	GIF image data, version 89a, 36 x 38
Category:	downloaded
Size (bytes):	1062
Entropy (8bit):	4.517838839626174
Encrypted:	false
SSDEEP:	12:z4ENetWsdvCMtkEFk+t2cd3iklbOViGZVsMLfE4DMWUcC/GFvyVEZd6vcmadxVtS:nA/ag/QSi6/LKZzqKVQgJOexQkYfG6E
MD5:	124A9E7B6976F7570134B7034EE28D2B
SHA1:	E889BFC2A2E57491016B05DB966FC6297A174F55
SHA-256:	5F95EFF2BCAAEA82D0AE34A007DE3595C0D830AC4810EA4854E6526E261108E9
SHA-512:	EA1B3CC56BD41FC534AAC00F186180345CB2C06705B57C88C8A6953E6CE8B9A2E3809DDB01DAAC66FA9C424D517D2D14FA45FBEF9D74FEF8A809B71550C7C 45
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	res://ieframe.dll/warning.gif
Preview:	GIF89a$.&.....h.....h.hh..h..h..h..h....h.....h.....h.....h.....hh.h..h..h..h..h.hhhhh.hh.hh.hh.hh..hh.h..h..h.h..h..hh.h..h..h..h..h..hh.h..h..h..h..h. .hh.h..h..h..h..h....h.....h.hh..h..h..h..h..h....h.....h.....h.....h.....h.hh..h..h..h..h....h.....h.....h.....h.....h... .....h.hh.h..h..h..h....h.....h.....h.....h.....h.....h.hh..h..h..h..h....h.....h.....h.....h..... .....!.....,....$.&.@.....H.....<0.....VXQH..C..1>.(..@..C.t.q"B..S.\.r.D...Z.. .M.41.".....<.r.;.r4..P..]....+.T-...N...x....1.:...TdD...^ .j..W.r...y....V...Lx0..):8p q.4.;...f`.r-K...(..P....t.].~..l..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\error[1]	
Process:	C:\Windows\SysWOW64\mshta.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\error[1]

File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1706
Entropy (8bit):	5.274543201400288
Encrypted:	false
SSDEEP:	48:NIAbzyYh8rRLkRVNaktqavP61GJZoF+SMy:xWqxztqaHO
MD5:	B9BEC45642FF7A2588DC6CB4131EA833
SHA1:	4D150A53276C9B72457AE35320187A3C45F2F021
SHA-256:	B0ABE318200DCDE42E2125DF1F0239AE1EFA648C742DBF9A5B0D3397B903C21D
SHA-512:	C119F5625F1FC2BCDB20EE87E51FC73B31F130094947AC728636451C46DCED7B30954A059B24FEF99E1DB434581FD9E830ABCEB30D013404AAC4A7BB1186AD A
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	res://ieframe.dll/error.js
Preview:	...window.onerror = HandleError..function HandleError(message, url, line)..{..var str = L_Dialog_ErrorMessage + "\n\n"..+ L_ErrorNumber_Text + line + "\n"..+ message;..al ert (str);..window.close();..return true;..}..function loadBdy()..{..var objOptions = window.dialogArguments;..btnNo.onclick = new Function("btnOKClick()");..btnNo.onkeyd own = new Function("SwitchFocus()");..btnYes.onclick = new Function("btnYesClick()");..btnYes.onkeydown = new Function("SwitchFocus()");..document.onkeypress = new Function("docKeypress()");..spnLine.innerText = objOptions.getAttribute("errorLine");..spnCharacter.innerText = objOptions.getAttribute("errorCharacter");..spnError.i nnerText = objOptions.getAttribute("errorMessage");..spnCode.innerText = objOptions.getAttribute("errorCode");..txaURL.innerText = objOptions.getAttribute("errorUrl");..if (objOptions.errorDebug)..{..divDebug.innerText = L_ContinueScript_Message;..}..btnYes.focus();..}..function SwitchFocus()..{..var HTML_KEY_ARROWLEFT = 37;..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6002BB0F.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 1022 x 235, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	25449
Entropy (8bit):	7.717073073385733
Encrypted:	false
SSDEEP:	768:5Q0NLh5g3xayQTvC4JwSJHfVEhWlB6zLn:5Qig3xayQ7JwoHfVEhWlB6H
MD5:	8F21C647D253A3CE991C371D19437151
SHA1:	6FCD455E7A040B387AA6F5A6737FFE06C5B9E39A
SHA-256:	7E7864C1563D7D1EDFE3FBDD2F9524F30EFC716716E84F25A1691DF7F628206F
SHA-512:	260AD36890A8947D351AA2FE73B76CCD7361950D3F564191E04FD540C62A89C55E65FB8C31024C18D21BD7B018CE44FB12CFD0B0268CF41DA56588B70FA1F7C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR....._../...&iCCPAdobe RGB (1998)..(.c``2ptqre.``..+).rwR...R`?.....> v^~^*...v...D_....@..J.(*.....(%.8...../)..3...E..... vQH.3.}...K.....I..... ..H} :....6....KR+@.28..T.e.g.(.ZZZ*8..'.*.W.....+x.%.....%.....B.....j..d.2....9....bg.b..\ZT.e22...#.#.....B...a.....T...!...>..9...O..:6\....pHYs.....+.....iTXtXML:com.adobe.xmp..... <?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.164648, 2021/01/12-15:52:29 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:tiff="http://ns.adobe.com/tiff/1.0/"

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{47D4F006-6281-436E-ADD1-2266A057AE87}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{76C67B44-1352-433D-B760-8C34027C46CD}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{76C67B44-1352-433D-B760-8C34027C46CD}.tmp	
Size (bytes):	9588
Entropy (8bit):	3.36228779012647
Encrypted:	false
SSDEEP:	192:KJtOd6IW2Ju7gkWlqCqvcDFoIIHMSWjWHSHf:Ati6MJu7gkWovQKMS2
MD5:	B18AD56AEC351E4A3116AAE4BCFB1EEA
SHA1:	867CCD578E80F0A9BE76ED84D9102C43D3017B76
SHA-256:	D9FACCCA44F5328AE0D1BD28C0C0223C174D3272D832710DF7D257A753E030AA
SHA-512:	FEBD24CF0E2F8E3510191D27D6D3A449F00E45710C964FFB47160B6C21DA11FFC216FAB5122E8C9FADD9D0733C806D8973263C0ACFC8B50B53311F0547BEE7(B
Malicious:	false
Preview:	....<.h.t.m.l.>...<.b.o.d.y.>...<.d.i.v. .i.d.=.'.i.n.t.e.g.e.r.S.w.a.p.'.>..... ....b.....*.....d...h.....H...L...z...~...l.....4...z.....4...:..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	71
Entropy (8bit):	4.153101000769482
Encrypted:	false
SSDEEP:	3:M1MtaUd2SmuaUd2mX1MtaUd2v:MyZd2qdWZdI
MD5:	50718DAD15698A25C72EC2E62022DC0E
SHA1:	75B30EC623E66D04149B44D9C1D7931709741E26
SHA-256:	C8FCB6D1F3A340DBD6830E135E41231564BBF702D6BF94C715343744BD412514
SHA-512:	1345294D60234FA9229AE7E3A24D3358A19740EC9D199000E8A8092796473D22A851787AED65F23BDE4F430EA4145F1E38F30B728D9AF5CBBF1BE112640D0562
Malicious:	false
Preview:	[doc]..order_07.21.LNK=0..order_07.21.LNK=0..[doc]..order_07.21.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\order_07.21.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:12 2020, mtime=Wed Aug 26 14:08:12 2020, atime=Thu Jul 22 17:00:31 2021, length=89257, window=hide
Category:	dropped
Size (bytes):	2038
Entropy (8bit):	4.519446214646222
Encrypted:	false
SSDEEP:	24:83Xk/XTwz6Ikn+NeHXxZDv3q+dM7dD23Xk/XTwz6Ikn+NeHXxZDv3q+dM7dV:8nk/XT3Ik+Nsu+Qh2nk/XT3Ik+Nsu+Q/
MD5:	037ED454C333186B84D3F7A64DC56ABA
SHA1:	17B4E2E34D22F3388540F461DB8D6D07BF61F07D
SHA-256:	ABDEB150FAC2362C15E723E834020A747C1CA0B67816ADC163EA72FF32E367CC
SHA-512:	62648EFD5A9ABB79B8458CE5DDC178B92812B6A991E0BC07E5D1593CBE51AF497334B30E1D156CC02836DA291360D3E2204FA039E44E2E291BBE1067A3BE7D B
Malicious:	false
Preview:	L.....F.... ...f....{..f....{..5UGv#....\.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....h.2..\...R.. .ORDER_~1.DOC..L.....Q.y.Q.y*...8.....o.r.d.e.r._.0.7...2.1...d.o.c.....y.....-...8...[.....?J.....C:\Users\..#.....\\3771 42\Users.user\Desktop\order_07.21.doc.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.o.r.d.e.r._.0.7...2.1...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.- .2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....377142.....D_....3N...W...9F.C.....[D_....3N...W...9F

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\Desktop\~$der_07.21.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.976846319095004
TrID:	• Microsoft Office XML Flat File Format Word Document (ASCII) (139530/1) 62.14% • Microsoft Office XML Flat File Format (ASCII) (66519/1) 29.62% • Visual Basic Script (13500/0) 6.01% • Generic XML (ASCII) (5005/1) 2.23%
File name:	order_07.21.doc
File size:	89257
MD5:	401b19c454075d52bd832725f3c22cfe
SHA1:	088f76c184a0cba673abc41bd5582e4e21672fdd
SHA256:	6b94e6319e46f52058d5f0c1bc07d7e367152e3bb769f2fd1af097914fe64ce3
SHA512:	b83ddf0a5dc6174591e0c07a1b87f5ffb5a1efa731913707829195415bed70a5dff43d9669e948e509fd3e77d15986391e1e01b9344c2694dd1b0fba5b87f894
SSDEEP:	1536:EVzJCsRRHr11AQYyqGJHQYCDEtU6dLTR97YVuL6:NKPxQYNtU6ZvYVuu
File Content Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<?mso-application progid="Word.Document"?>..<w:wordDocument xmlns:aml="http://schemas.microsoft.com/aml/2001/core" xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmln

File Icon



Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	Word2003_XML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/452438/sample/order_07.21.doc"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False

Indicators

Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Streams with VBA

Streams

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-11:01:07.680252	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
07/22/21-11:01:08.693819	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8

Network Port Distribution

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 11:01:04.599126101 CEST	192.168.2.22	8.8.8.8	0xa163	Standard query (0)	airloweryd.com	A (IP address)	IN (0x0001)
Jul 22, 2021 11:01:05.609379053 CEST	192.168.2.22	8.8.8.8	0xa163	Standard query (0)	airloweryd.com	A (IP address)	IN (0x0001)
Jul 22, 2021 11:01:06.623332024 CEST	192.168.2.22	8.8.8.8	0xa163	Standard query (0)	airloweryd.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 11:01:06.670084000 CEST	8.8.8.8	192.168.2.22	0xa163	Server failure (2)	airloweryd.com	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 11:01:07.680150032 CEST	8.8.8.8	192.168.2.22	0xa163	Server failure (2)	airloweryd.com	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 11:01:08.693541050 CEST	8.8.8.8	192.168.2.22	0xa163	Server failure (2)	airloweryd.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2696 Parent PID: 584

General

Start time:	11:00:32
Start date:	22/07/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fff0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: cmd.exe PID: 2480 Parent PID: 2696

General

Start time:	11:00:33
Start date:	22/07/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c c:\programdata\captionEx.hta
Imagebase:	0x4a150000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

File Activities — Show Windows behavior

Analysis Process: mshta.exe PID: 2232 Parent PID: 2480

General

Start time:	11:00:34
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\mshta.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\mshta.exe' 'C:\programdata\captionEx.hta'
Imagebase:	0x12a0000
File size:	13312 bytes
MD5 hash:	ABDFC692D9FE43E2BA8FE6CB5A8CB95A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: regsvr32.exe PID: 2544 Parent PID: 2232

General

Start time:	11:00:41
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' c:\users\public\captionEx.jpg
Imagebase:	0xb20000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities — Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021