

JoeSandbox Cloud BASIC



**ID:** 682633

**Sample Name:**

berniesbooksdocument08.11.doc

**Cookbook:**

defaultwindowsofficecookbook.jbs

**Time:** 19:47:42

**Date:** 11/08/2022

**Version:** 35.0.0 Citrine

# Table of Contents

Table of Contents	2
Windows Analysis Report berniesbooksdocument08.11.doc	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Sigma Signatures	4
Snort Signatures	4
Joe Sandbox Signatures	5
AV Detection	5
System Summary	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
World Map of Contacted IPs	8
Public IPs	8
General Information	8
Warnings	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASNs	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B1045D8E.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD5D5437.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{B098A39C-D2D9-4D2C-A419-D30C217371D1}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6C55D25D-240D-4843-97E8-D3E7E4EF3D22}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E93ACC5D-7686-4896-9F93-FE726BDE714B}.tmp	11
C:\Users\user\AppData\Local\Temp\~DF425318190330F69E.TMP	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\berniesbooksdocument08.11.LNK	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	12
C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	12
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	12
C:\Users\user\Desktop\~\$rniesbooksdocument08.11.doc	13
Static File Info	13
General	13
File Icon	13
Static OLE Info	13
General	13
OLE File "opt\package\joesandbox/database/analysis/682633/sample/berniesbooksdocument08.11.doc"	13
Indicators	13
Streams with VBA	14
VBA File Name: ThisDocument.cls, Stream Size: 2850	14
General	14
VBA Code	14
Streams	14
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365	14
General	14
Stream Path: PROJECTwm, File Type: data, Stream Size: 41	14
General	14
Stream Path: VBA\ VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7	14
General	14
Stream Path: VBA\__SRP_2, File Type: data, Stream Size: 5108	14
General	14
Stream Path: VBA\__SRP_3, File Type: data, Stream Size: 2724	15
General	15
Stream Path: VBA\dir, File Type: data, Stream Size: 486	15
General	15
Network Behavior	15
TCP Packets	15




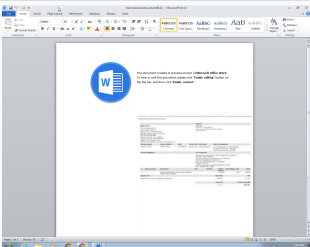
Statistics	15
System Behavior	15
Analysis Process: WINWORD.EXEPID: 2688, Parent PID: 576	16
General	16
File Activities	16
File Created	16
File Deleted	16
File Read	16
Registry Activities	16
Key Created	16
Key Value Created	17
Key Value Modified	18
Disassembly	22

# Windows Analysis Report

berniesbooksdocument08.11.doc

## Overview

### General Information

Sample Name:	berniesbooksdocument08.11.doc
Analysis ID:	682633
MD5:	2b10f2617b3285..
SHA1:	448e513536aa0c..
SHA256:	3b86f8aff12d2b3..
Tags:	<div>doc</div> <div>lcedID</div>
Infos:	<div></div> <div></div>

### Detection

MALICIOUS

SUSPICIOUS

CLEAN

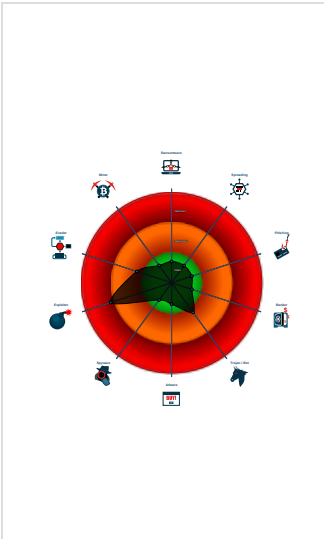
UNKNOWN

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


### Signatures

Office document tries to convince v...
Multi AV Scanner detection for subm...
Document contains an embedded V...
Machine Learning detection for sam...
Potential document exploit detected...
Tries to connect to HTTP servers, b...
Document contains an embedded V...
Document contains embedded VBA...
IP address seen in connection with ...
Document misses a certain OLE str...

### Classification



## Process Tree

System is w7x64
 WINWORD.EXE (PID: 2688 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
cleanup

## Malware Configuration

No configs have been found
----------------------------

## Yara Signatures

No yara matches
-----------------

## Sigma Signatures

No Sigma rule has matched
---------------------------

## Snort Signatures

No Snort rule has matched
---------------------------

# Joe Sandbox Signatures

## AV Detection



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

## System Summary



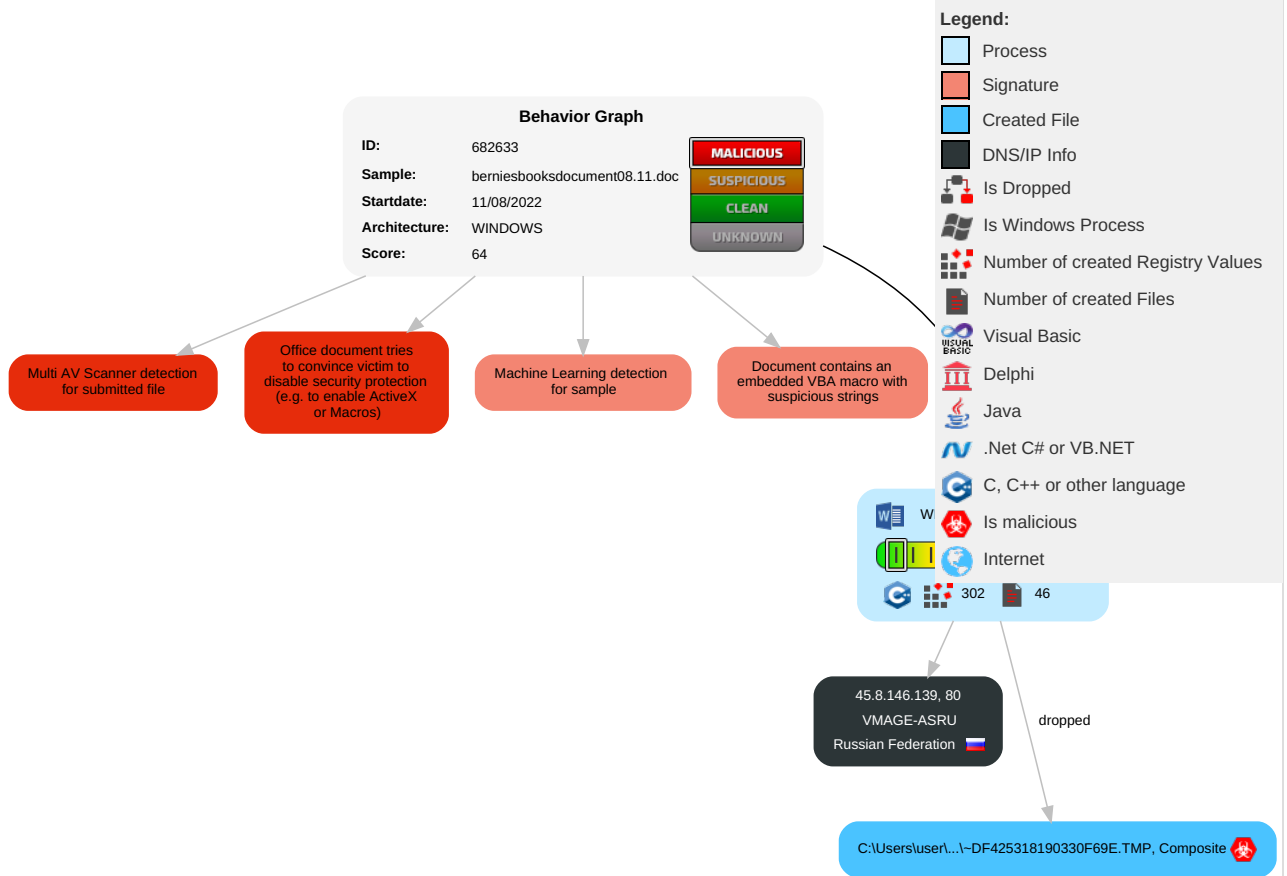
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro with suspicious strings

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	<div>12</div> Scripting	Path Interception	Path Interception	<div>1</div> Masquerading	OS Credential Dumping	<div>1</div> File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	<div>1</div> Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	<div>1</div> Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	<div>1</div> Disable or Modify Tools	LSASS Memory	<div>1</div> System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	<div>12</div> Scripting	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

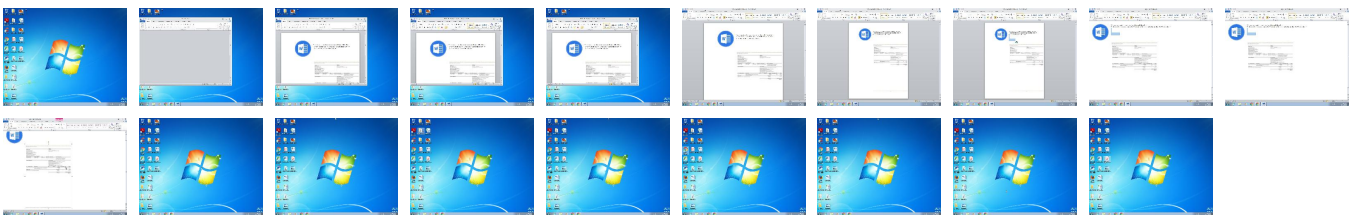
## Behavior Graph

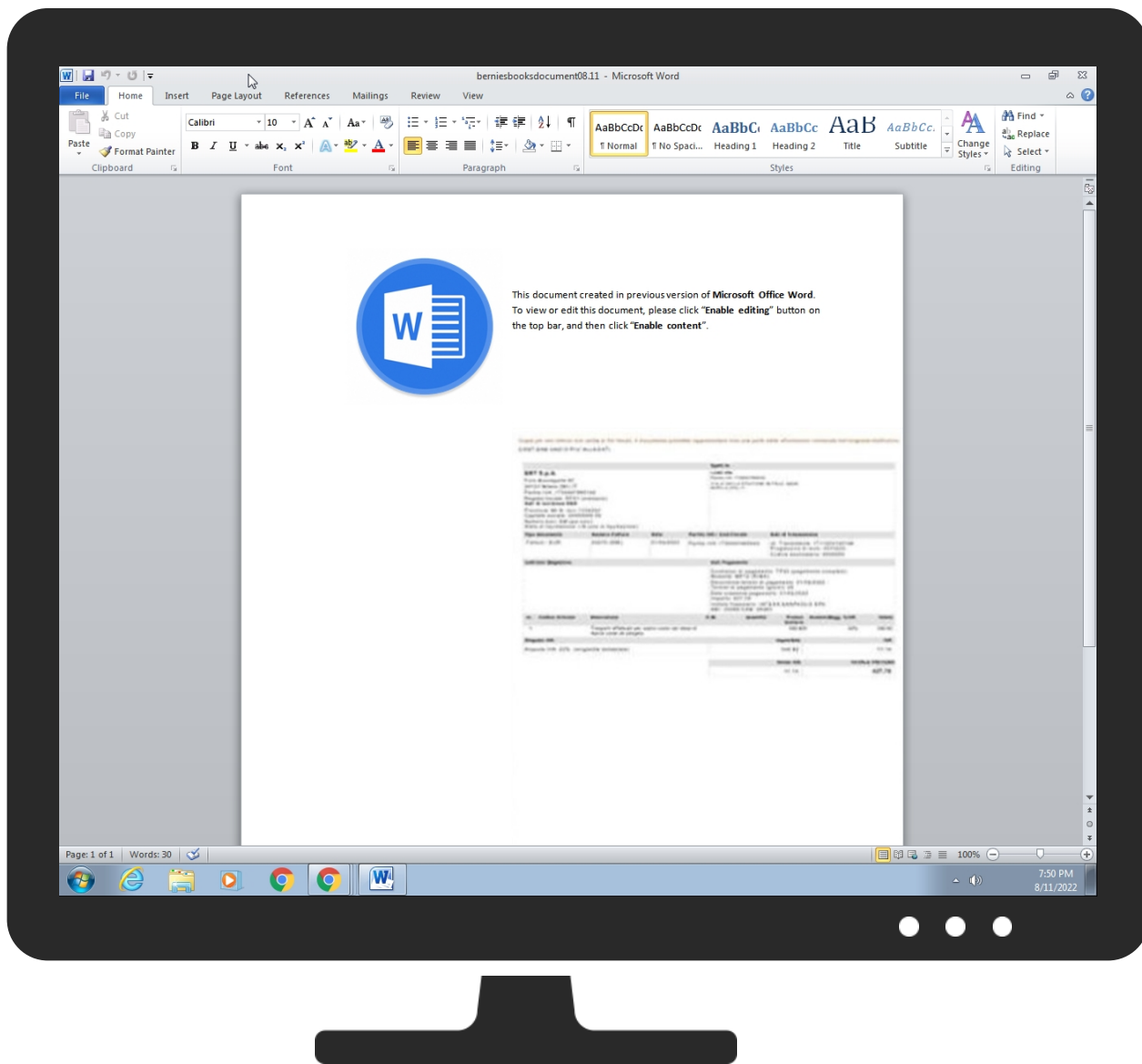


## Screenshots

### Thumbnails

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





## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

Source	Detection	Scanner	Label	Link
berniesbooksdocument08.11.doc	25%	Virustotal		<a href="#">Browse</a>
berniesbooksdocument08.11.doc	15%	ReversingLabs	Script-Macro.Trojan.Amp hitryon	
berniesbooksdocument08.11.doc	100%	Joe Sandbox ML		

### Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\--DF425318190330F69E.TMP	100%	Joe Sandbox ML		

### Unpacked PE Files

🚫 No Antivirus matches

### Domains

🚫 No Antivirus matches

### URLs

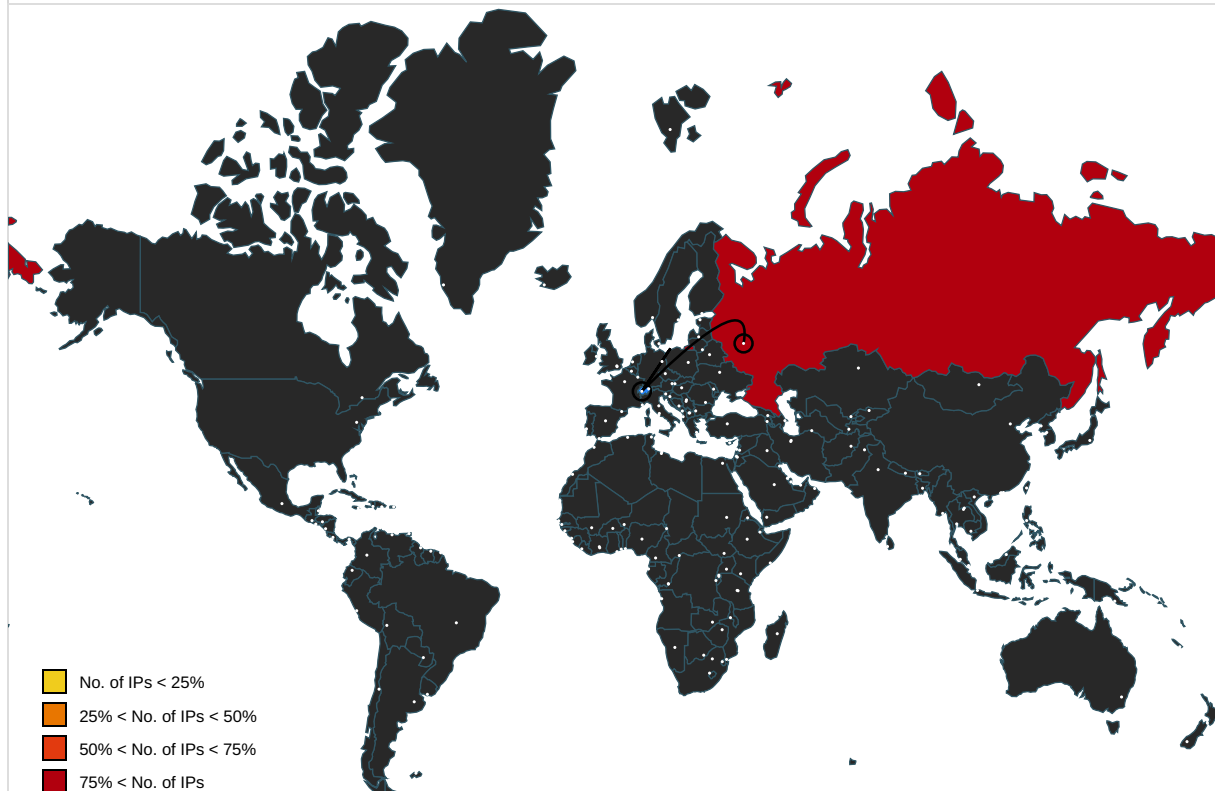
⛔ No Antivirus matches

## Domains and IPs

### Contacted Domains

⛔ No contacted domains info

### World Map of Contacted IPs



### Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.146.139	unknown	Russian Federation		44676	VMAGE-ASRU	false

## General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682633
Start date and time:	2022-08-11 19:47:42 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	berniesbooksdocument08.11.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Run name:	Without Instrumentation
Number of analysed new started processes analysed:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0




Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.expl.winDOC@1/11@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>
Cookbook Comments:	<ul style="list-style-type: none"><li>• Found application associated with file extension: .doc</li><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found Word or Excel or PowerPoint or XPS Viewer</li><li>• Attach to Office via COM</li><li>• Scroll down</li><li>• Close Viewer</li></ul>

Warnings

- 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

 No context

Domains

 No context


ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files



 No context

Created / dropped Files



File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.123533094102747
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lakwkvq4HW49W4PII4WHkUZJ/W4c:4LG1ND9Pxn824ksiWeWYiWHyz
MD5:	08F60D513FD293740B13D3F6BFA25487
SHA1:	BE7E51B82521595903D808CC7DCC7B3A83772F6D
SHA-256:	F7E0814E3D99D3FA7140E6A51F93D158A9121D0E0979ACF6AF88E33948B273D2
SHA-512:	40CA70AF8D3BD6B0F67C2FA58224C8845034D212A2CE772CEB2AF95AE64D6DBD14F83B79A1B5C4CB95BCA122D88094452DAF07067781A9D799CDDD141556643
Malicious:	false
Reputation:	low
Preview:	.....T.h.i.s .d.o.c.u.m.e.n.t .c.r.e.a.t.e.d .i.n .p.r.e.v.i.o.u.s .v.e.r.s.i.o.n .o.f .M.i.c.r.o.s.o.f.t .O.f.f.i.c.e .W.o.r.d.....T.o .v.i.e.w .o.r .e.d.i.t .t.h.i.s .d.o.c.u.m.e.n.t., .p.l .e.a.s.e .c.l.i.c.k ..E.n.a.b.l.e .e.d.i.t.i.n.g. .b.u.t.t.o.n .o.n .t.h.e .t.o.p .b.a.r., .a.n.d .t.h.e.n .c.l.i.c.k ..E.n.a.b.l.e .c.o.n.t.e.n.t. ....Z.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E93ACC5D-7686-4896-9F93-FE726BDE714B}.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:	95F83AE84CAFCCEDE5AE504546725C34D5F9710E5CA2D11761486970F2FBECB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF425318190330F69E.TMP  									
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE								
File Type:	Composite Document File V2 Document, Cannot read section info								
Category:	dropped								
Size (bytes):	60928								
Entropy (8bit):	4.154380696227403								
Encrypted:	false								
SSDEEP:	768:HgP1WOsa9Q1Lod1jK04+OziZ7hP0Wd/sr5ZWaGvcP HOGBau:oDQ1k1e04+OziZsr/bGjGBau								
MD5:	3D9FDC90F073DE06FA3494E40C8DD3E0								
SHA1:	FEA48EF264B99F460F0C6842593936E3F67759BA								
SHA-256:	7CCD6AAC1E7529DD61946227FFBF6337C3B574A7308C23891A2A5BD26C78F934								
SHA-512:	29B8551E60D97A214E933C5F733F9165E711F3478D0F2CC8BFF90869D9CDB65054C1828E755DCA466B5998F65B8666FA4C06D0B3BF3B1888BA2247B8F352376								
Malicious:	true								
Antivirus:	<ul style="list-style-type: none"><li>Antivirus: Joe Sandbox ML, Detection: 100%</li></ul>								
Preview:	.....>.....T.....(.....!...".#...\$...%...&...'.....)*...+...-.../...0...1...2...3...4...5...6...7...8...9...:<...=...>...?......<div> <div data-bbox="102 1971 1517 2161" data-label="Table"><table><tr><td colspan="2">C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\berniesbooksdocument08.11.LNK</td></tr><tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\WINWORD.EXE</td></tr><tr><td>File Type:</td><td>MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:45:53 2022, mtime=Tue Mar 8 15:45:53 2022, atime=Fri Aug 12 01:49:12 2022, length=2298836, window=hide</td></tr><tr><td>Category:</td><td>dropped</td></tr></table></div> <div data-bbox="76 2166 1517 2188" data-label="Page-Footer"><div>Copyright Joe Security LLC 2022</div><div>Page 11 of 22</div></div>	C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\berniesbooksdocument08.11.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=Tue Mar 8 15:45:53 2022, mtime=Tue Mar 8 15:45:53 2022, atime=Fri Aug 12 01:49:12 2022, length=2298836, window=hide	Category:	dropped
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\berniesbooksdocument08.11.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=Tue Mar 8 15:45:53 2022, mtime=Tue Mar 8 15:45:53 2022, atime=Fri Aug 12 01:49:12 2022, length=2298836, window=hide								
Category:	dropped								

Size (bytes):	1089
Entropy (8bit):	4.563669334661553
Encrypted:	false
SSDEEP:	12:83YZvgXg/XAICPCHaXRBktB/xQpX+WVrW/xgitBiO4icvbFk4wBi+DtZ3YiIMMEy:86/XThOljrW/xfTTrepkR1Dv3qJu7D
MD5:	E11F18A7556CDFA5D3EFE4B8903FD756
SHA1:	896F273A9D2083A39D96A7B30213495C493199E0
SHA-256:	8FE28D1FB2B4D3A719D6A044B7752C449021E2A183D930FEF312116EA8A89740
SHA-512:	B0A426907A287C1A7AE6AA102B23514E852E754431BF218BAB82CAD00771EFC969AA8F64CCAF157975E566DEC9E5CB8E807442E50DF5A67E604B1E62ABD0D8E9
Malicious:	false
Preview:	L.....F....3.....3.....#.....P.O. .i.....+00.../C:\.....t.1....QK.X..Users.`.....QK.X*.....6....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3....L.1....hT....user.8.....QK.XhT.*...&=...U.....A.l.b.u.s.....z.1....hT....Desktop.d.....QK.XhT.*..._...=.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-2.1 .7.6.9.....2...#.U'. .BERNIE~1.DOC..h.....hT..hT.*...r.....'. .....b.e.r.n.i.e.s.b.o.o.k.s.d.o.c.u.m.e.n.t.0.8...1.1...d.o.c.....8..[.....?J.....C:\Users\..#..... \124406\Users.user\Desktop\berniesbooksdocument08.11.doc.4.....\.....\.....\.....\D.e.s.k.t.o.p\l.b.e.r.n.i.e.s.b.o.o.k.s.d.o.c.u.m.e.n.t.0.8...1.1...d.o.c.....,LB. ).Ag.....1SPS.XF.L8C....&m.m.....-...S.-1.-5.-2.1.-9.6.6.7.7.1.3.1.5.-3.0.1.9.4.0.5.6.3.7.-3.6.7.3.3.6.4.7.7.-1.0.0.6.....`.....X..

<b>C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	101
Entropy (8bit):	4.692698988371966
Encrypted:	false
SSDEEP:	3:bDuMJlfyNS58JRQU9CmX14BS58JRQU9Cv:bCUyZJGM6dJGMs
MD5:	57D1B08878CF3A9EE8C43DEE40795E0D
SHA1:	25240A63B87F096D1F9F743D25E654BCB248576D
SHA-256:	2DB51BE5DD72BBE9D0783A8F1075B216F99D07D805EA1BE2C2D3DF48D717E73F
SHA-512:	BAC49CF018A74006D3A35B8C3E544A5ACDA8B20261B7530FCAA237E42D43CF9258A7B66C2BC39F9F2CDB221C2CF796A5E767D77B0289976E88976C8A2D1A9E9D
Malicious:	false
Preview:	[folders]..Templates.LNK=0..berniesbooksdocument08.11.LNK=0..[doc]..berniesbooksdocument08.11.LNK=0..

<b>C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJyIp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDF5A533BC9E428B0637562AFA
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....X...

<b>C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDf1C54CA0D4

Malicious:	false
Preview:	..

<b>C:\Users\user\Desktop\~\$rniesbooksdocument08.11.doc</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJyIp2bG/WWNJbiFGUld/ln:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDA533BC9E428B0637562AFA
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

<b>Static File Info</b>	
<b>General</b>	
File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993790073605077
TrID:	<ul style="list-style-type: none"><li>Word Microsoft Office Open XML Format document (49504/1) 49.01%</li><li>Word Microsoft Office Open XML Format document (43504/1) 43.07%</li><li>ZIP compressed archive (8000/1) 7.92%</li></ul>
File name:	berniesbooksdocument08.11.doc
File size:	2298836
MD5:	2b10f2617b32857999df1cf5f19f0d8d
SHA1:	448e513536aa0c576b123d5b243e1bdc6d261d6f
SHA256:	3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f9e47
SHA512:	f99a1ffdb12b9fe4bc512f33ef98fa989312951fdbfc6aa8cc09d0725cbb90e2c11727dced788991e00087859054b273f09917d2fa3b52cd5be54ecd257dd85c
SSDEEP:	49152:tljQhPf8F7u26T076/JsKhCa8CCGEET1yEU:WjufCre/1UMEEzyh
TLSH:	73B533F8C2706D07F858D195355BEAF27960C6A2863B5EE9F275131BE139B1F4070B28
File Content Preview:	PK.....!.U~.....rels/.rels...J.@.....4.E..D.....\$...T..w-.j..... zs..z.z.*X.%(v.....6O.{PI.....`S__x.C..CR.....t.R.....hl.3..H.Q..*.;.=..y... n.....yo.....[vrf..A..6..3[>_...-K....\NH!....<..r...E.B..P...<_.

<b>File Icon</b>	
	
Icon Hash:	e4eea2aaa4b4b4a4

<b>Static OLE Info</b>	
<b>General</b>	
Document Type:	OpenXML
Number of OLE Files:	1

<b>OLE File "/opt/package/joesandbox/database/analysis/682633/sample/berniesbooksdocument08.11.doc"</b>	
<b>Indicators</b>	
Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False

Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

<b>Streams with VBA</b>	
<b>VBA File Name: ThisDocument.cls, Stream Size: 2850</b>	
<b>General</b>	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2850
Data ASCII:	.J.Attribut.e VB_Nam.e = "Thi.sDocumen.t"...Bas..1Normal...VGloba!l.Spac.lFa.lse.JCrea.tabl. .Pre decla..Id..#Tru."Exp.ose..Temp.lateDeri.v.\$CustomlizC.P.... .D.? PtrSa.fe Function ..... .... Lib. "kernel.32" Alia.s "Virtu.alProtec.t" (ByVa.l . As Long.5,
Data Raw:	01 4a b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

<b>VBA Code</b>	

<b>Streams</b>	
<b>Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365</b>	
<b>General</b>	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	365
Entropy:	5.222695960979116
Base64 Encoded:	True
Data ASCII:	ID="{8FB13CC5-98A3-44C0-B65D-DC235779DEF4}"..Document=ThisDocument/&H00000000..Na me="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="8381840B030F03 0F030F030F"..DPB="0604018807888B898B898B"..GC="898B8E938F938F6C"....[Host Extender Info]..
Data Raw:	49 4d 3d 22 7b 38 46 42 31 33 43 43 35 2d 39 38 41 33 2d 34 34 43 30 2d 42 36 35 44 2d 44 43 32 33 35 37 37 39 44 45 46 34 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 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

<b>Stream Path: PROJECTwm, File Type: data, Stream Size: 41</b>	
<b>General</b>	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	Thi.sDocumen.T.h.i.s.D.o.c.u.m.e.n.t.....
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 00 00

<b>Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7</b>	
<b>General</b>	
Stream Path:	VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators
Stream Size:	7
Entropy:	1.8423709931771088
Base64 Encoded:	False
Data ASCII:	a . . .
Data Raw:	cc 61 ff ff 00 00 00


<b>Stream Path: VBA/_SRP_2, File Type: data, Stream Size: 5108</b>	
<b>General</b>	
Stream Path:	VBA/_SRP_2
File Type:	data

General	
Stream Size:	5108
Entropy:	1.9282501947973256
Base64 Encoded:	False
Data ASCII:	r U @ ..... @ ..... @ ..... 8 ..... P ..... " ..... q ..... ..... A ..... ` ..... ` i < ..... .....
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 22 00 1f 00 00 00 00 01 00 01 00 00 00 01 00 71 07 00 00 00 00 00 00 00 00 00 a1 07 00 00 00 00 00 00 00 00 00 d1 07

Stream Path: VBA/___SRP_3, File Type: data, Stream Size: 2724	
General	
Stream Path:	VBA/___SRP_3
File Type:	data
Stream Size:	2724
Entropy:	2.6851031014715843
Base64 Encoded:	False
Data ASCII:	r U @ ..... @ ..... @ ..... X ..... ` ..... p ..... Q ..... Q . P ..... 0 . p ..... ` ..... \ . p ..... ..... q .....
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 78 00 00 00 08 00 60 00 e1 08 00 00 00 00 00 00 00 00 00 00 04 70 10 00 fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 486	
General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	486
Entropy:	6.2963537460893955
Base64 Encoded:	True
Data ASCII:	..... 0 ..... H ..... Project.Q(..@.....=....l.....[d-...".<.....rstdo.le>..s.t..d.o.l.e.(..h..^.. *\\G{00020430-....C.....46}#2.0#.0#C:\\Win.dows\\sys@tem32\\.e2..tlb#OLE. Automati.on.ENor( maIENCr.m.aF... cEC....+m.! OfficgO.f.i.cg..g2DF8D0.4C-5BFA
Data Raw:	01 e2 b1 80 01 00 04 00 00 00 03 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 e4 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 00 08 06 12 09 02 12 80 2e 5b f4 64 2d 00 0c 02 22 0a 3c 02 0a 16 02 72 73 74 64 6f 08 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 00 28 0d 00 68 00 11 5e 00 03 2a 5c 00 47 7b 30 30 30

Network Behavior				
TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 19:48:39.147802114 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 19:48:42.149796009 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 19:48:48.171907902 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 19:49:00.186759949 CEST	49172	80	192.168.2.22	45.8.146.139
Aug 11, 2022 19:49:03.196183920 CEST	49172	80	192.168.2.22	45.8.146.139
Aug 11, 2022 19:49:09.202687979 CEST	49172	80	192.168.2.22	45.8.146.139

Statistics
 No statistics

System Behavior
-----------------

## Analysis Process: WINWORD.EXE    PID: 2688, Parent PID: 576

### General

Target ID:	0
Start time:	19:49:14
Start date:	11/08/2022
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:	0x13fc30000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

### File Activities

#### File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VB	read data or list directory   synchronize	device	directory file   synchronous io non alert   open for backup ident   open reparse point	success or wait	1	6E102B14	CreateDirectoryA

#### File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF425318190330F69E.TMP	success or wait	1	6E180648	unknown
C:\Users\user\Desktop\~\$rniesbooksdocument08.11.doc	success or wait	1	6E180648	unknown

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

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

#### File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Fonts\StaticCache.dat	unknown	60	success or wait	1	6E47A0EB	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	6E071925	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6E071925	unknown
C:\Users\user\Desktop\lberniesbooksdocument08.11.doc	1963780	185	success or wait	2	6E180648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B1045D8E.png	0	65536	success or wait	4	6E180648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD5D5437.png	0	61935	success or wait	1	6E180648	unknown

### Registry Activities

#### Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E15A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E15A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E15A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E180648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E180648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E180648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7950E	success or wait	1	6E180648	unknown



Key Value Created
<ul style="list-style-type: none"> <li>• <b>Revenue Growth:</b> Increased sales volume and revenue.</li> <li>• <b>Customer Satisfaction:</b> Improved customer loyalty and repeat business.</li> <li>• <b>Operational Efficiency:</b> Streamlined processes and reduced costs.</li> <li>• <b>Market Penetration:</b> Expanded reach into new markets.</li> <li>• <b>Brand Reputation:</b> Enhanced brand image and credibility.</li> </ul>

[illegible]










Disassembly

 No disassembly