ID: 532378
Sample Name: Invoice.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:00:37
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

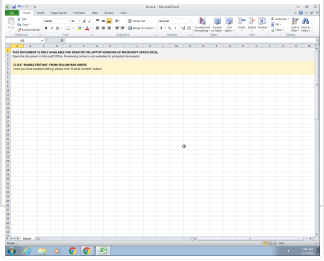
Windows Analysis Report Invoice.xlsm

Overview

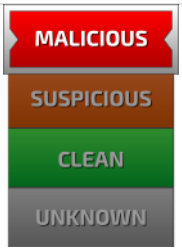
General Information

Sample Name:	Invoice.xlsm
Analysis ID:	532378
MD5:	41b25400c2b31b..
SHA1:	b543cbb86a4e50..
SHA256:	734577b2ffb53dd..
Infos:	

Most interesting Screenshot:



Detection



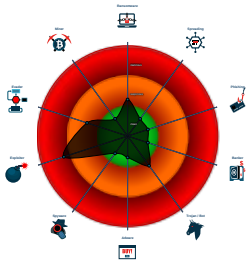
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Found a hidden Excel 4.0 Macro she…
- Potential document exploit detected…
- Uses a known web browser user age…
- Yara detected Xls With Macro 4.0
- Detected potential crypto function
- Excel documents contains an embe…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2208 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - rundll32.exe (PID: 1724 cmdline: C:\Windows\SysWow64\rundll32.exe ..\besta.ocx,44532.2932256944 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **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	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

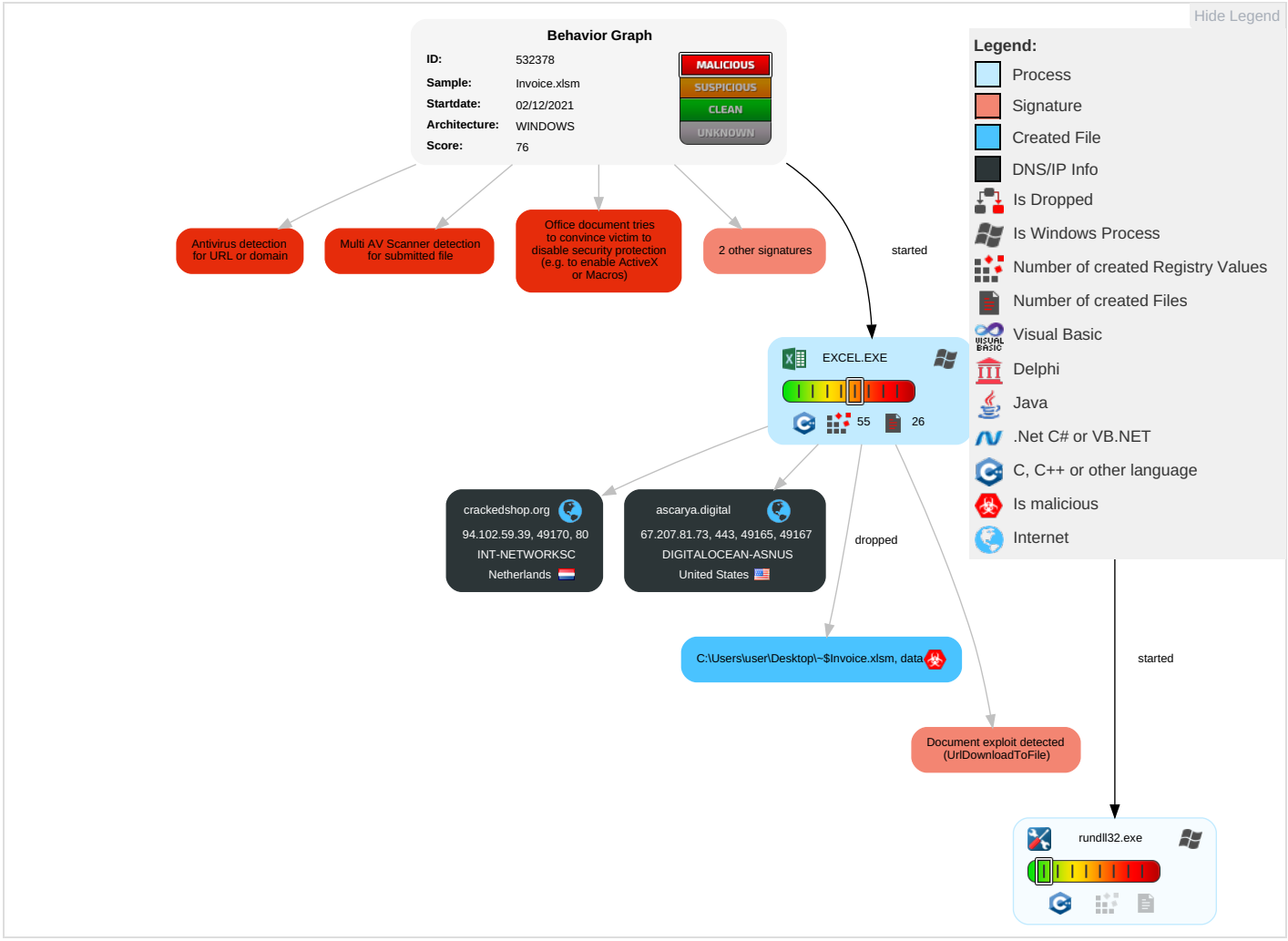
System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Valid Accounts	Scripting 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	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 to Track Device Location	Obtain Device Cloud Backups	De De Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap		Ca Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

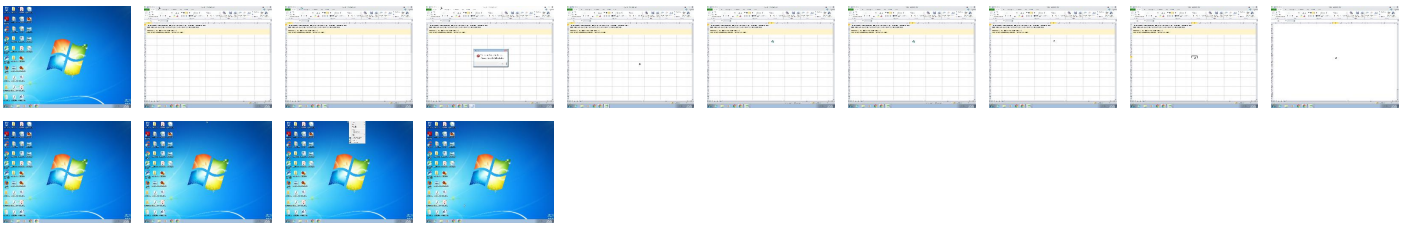
Behavior Graph

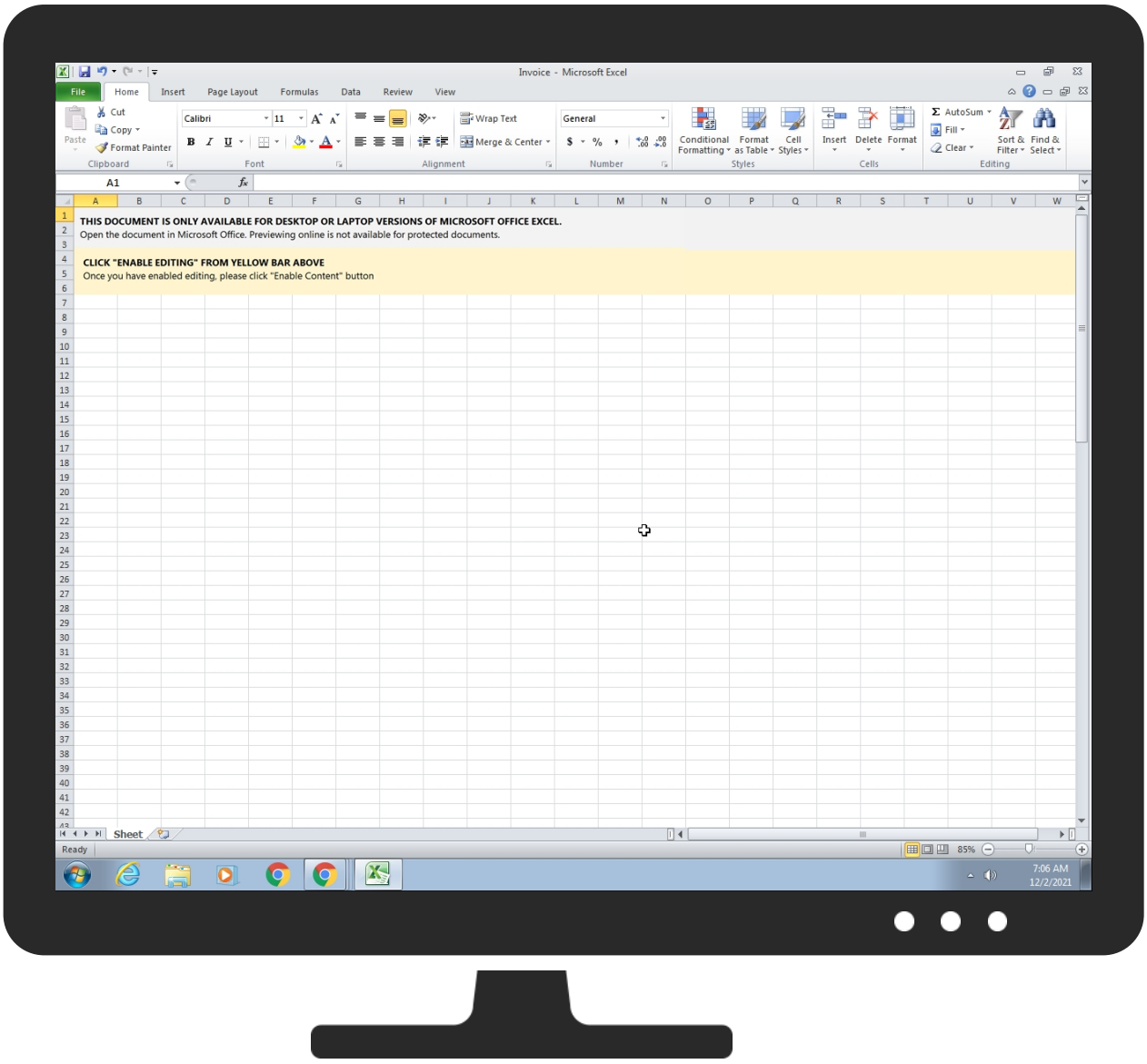


Screenshots

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
Invoice.xlsm	23%	Virustotal		Browse
Invoice.xlsm	20%	ReversingLabs	Document-Office.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
crackedshop.org	0%	Virustotal		Browse
ascarya.digital	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crackedshop.org/cgi-sys/suspendedpage.cgi	4%	Virustotal		Browse
http://crackedshop.org/cgi-sys/suspendedpage.cgi	0%	Avira URL Cloud	safe	
http://crackedshop.org/9/q080U0ARYYL/	4%	Virustotal		Browse
http://crackedshop.org/9/q080U0ARYYL/	100%	Avira URL Cloud	malware	
http://purl.or	0%	Avira URL Cloud	safe	
http://crackedshop.org/cgi-sys/suspendedpage.cgi5	0%	Avira URL Cloud	safe	
http://https://ascarya.digital/wp-con	0%	Avira URL Cloud	safe	
http://https://ascarya.digit	0%	Avira URL Cloud	safe	
http://https://ascarya.digital/wp-content/ZH4rirU	100%	Avira URL Cloud	malware	
http://https://ascarya.digital/wp-conte	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://schemas.open	0%	URL Reputation	safe	
http://https://ascarya.digital/wp-content%https://ascarya.digital/wp-content/ZH&https://ascarya.digital/wp-	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://schemas.openformatrg/package/2006/r	0%	URL Reputation	safe	
http://https://ascarya.digital/w	0%	Avira URL Cloud	safe	
http://https://ascarya.digital	0%	Avira URL Cloud	safe	
http://https://ascarya.digital/	0%	Avira URL Cloud	safe	
http://https://ascarya.dig	0%	Avira URL Cloud	safe	
http://https://ascarya.digital/wp-content/ZH4rirU/	100%	Avira URL Cloud	malware	
http://https://ascarya.digital/wp-c	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
crackedshop.org	94.102.59.39	true	false	• 0%, Virustotal, Browse	unknown
ascarya.digital	67.207.81.73	true	false	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://crackedshop.org/cgi-sys/suspendedpage.cgi	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://crackedshop.org/9/q080U0ARYYL/	true	• 4%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.102.59.39	crackedshop.org	Netherlands		202425	INT-NETWORKSC	false
67.207.81.73	ascarya.digital	United States		14061	DIGITALOCEAN-ASNUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532378
Start date:	02.12.2021
Start time:	07:00:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 21s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice.xlsm
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:	7
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:	mal76.expl.winXLSM@3/6@2/2
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: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	56449657.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	3762.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	56449657.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	08676789691.xlsm	Get hash	malicious	Browse	• 157.230.250.107

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	3762.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	55339.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	08676789691.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	55339.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	SecuriteInfo.com.Heur.8342.xls	Get hash	malicious	Browse	• 157.230.250.107
	SecuriteInfo.com.Heur.17052.xls	Get hash	malicious	Browse	• 157.230.250.107
	SecuriteInfo.com.Heur.8342.xls	Get hash	malicious	Browse	• 157.230.250.107
	57949616735.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	57949616735.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	44307.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	44307.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	77859564213.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	77859564213.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	1762311.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	1762311.xlsm	Get hash	malicious	Browse	• 157.230.250.107
	88985.xlsm	Get hash	malicious	Browse	• 157.230.250.107
INT-NETWORKSC	yakuza.x86	Get hash	malicious	Browse	• 94.102.52.200
	yakuza.arm7	Get hash	malicious	Browse	• 94.102.52.207
	JWCIQ6dmiX	Get hash	malicious	Browse	• 196.16.9.109
	g3XlmknqG3	Get hash	malicious	Browse	• 196.16.37.18
	re2.x86	Get hash	malicious	Browse	• 196.16.25.46
	jew.arm7	Get hash	malicious	Browse	• 94.102.52.203
	ef5rWphlBV.exe	Get hash	malicious	Browse	• 89.248.173.187
	6czjyyvzVM.exe	Get hash	malicious	Browse	• 145.249.106.195
	7NDorjJtM6.exe	Get hash	malicious	Browse	• 145.249.106.195
	7NDorjJtM6.exe	Get hash	malicious	Browse	• 145.249.106.195
	Reciept_20438048.xlsb	Get hash	malicious	Browse	• 145.249.106.39
	Reciept_20438048.xlsb	Get hash	malicious	Browse	• 145.249.106.39
	Reciept_20438048.xlsb	Get hash	malicious	Browse	• 145.249.106.39
	7spunOMzSK	Get hash	malicious	Browse	• 196.16.25.39
	VtlQkDgDjE	Get hash	malicious	Browse	• 196.16.9.117
	Reciept 5528051.xlsb	Get hash	malicious	Browse	• 145.249.106.39
	Reciept 5528051.xlsb	Get hash	malicious	Browse	• 145.249.106.39
	Reciept 8767556.xlsb	Get hash	malicious	Browse	• 145.249.106.39
	9TW5TjqwON.dll	Get hash	malicious	Browse	• 80.82.67.127
	Cib5IX5kD5.dll	Get hash	malicious	Browse	• 80.82.67.127

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\suspendedpage[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7624
Entropy (8bit):	5.6428645067252985
Encrypted:	false
SSDEEP:	192:olVZHCkA26xd3Q4JRveuTtMy47R/Ga0kVhFuPwf8Pn9wHHyJZS:QJvVGaRF8I8Q
MD5:	EB2F7C463E3BEFAD0174E89C10451BCD
SHA1:	80C6604E30655B9BA949210122CCFAF9C7D67766
SHA-256:	5E6DEB3C5AD4E6AB599A3B1A86FCAF25F721C32ED65E83128E9EC0F7ACB1CA0E
SHA-512:	108CF3C4FEE5CC37A16B8A1EF302F66ED6FBE0E5638127689E2F904837688813D8EE424A53A1AABE18034E54B2695852F6DF8B62E792D74B1CD343ECA3A134C
Malicious:	false
Reputation:	low
IE Cache URL:	http://crackedshop.org/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5EEDDA76.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1714 x 241, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	14200
Entropy (8bit):	7.855440184003825
Encrypted:	false
SSDEEP:	384:aeN0UV6iAmjeSvWFL3SdwHEpS4Q24kc49+Tb:jmUxjfC30+kS4Qyob
MD5:	4FE798EE522800691796BC9446918C90
SHA1:	1E01CDE49D0B1B5E2F0DFBAD568DC2ECFBEDEAD3
SHA-256:	EC0BC049D3D30C29567806EB2D555589CD2E1B6B30E9145F77B73A32EC1C1087
SHA-512:	FF968DA2D921DA198E93E82E2FB15583CFA4696455755A6674BC321CD90AE5502ADDC445A0F8C630D9DC780E77EEC6FFC83F55CD2C16DDE7F465BFD0D89BFAA
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....-.....sRGB.....gAMA.....a.....PLTE....6...6.....6..a..a..6.....a.....a...aa....6....6...66666.6aa..a..6aaa...a....66.....aaaa..aaaa6a....a....66...6.a.....S.b.....6.:...b....f....S.....t:...6t...f.....:6...S:6.:bS.....fbS..Sf.t.....:t..t....bS..tfb..6.f...Sfb.....:.S.....6l...WtRNS.....c5.....pHYs.....o.d..5.IDATx^.....q....R.A...[.l...'@. .....G..'..;...%..]U]3s....x.s.;.]]..W.....~..|...../~...?.{...~fe./...).H....Og1.6g....1T+v..'"h.._(Z;.Zh.bo.....rip..5.>..).h..(F....Z.[.q2B.WZz,...M}@..n$.dO.VK?.....YZ...."-o#.K..q..-#5.JT1.K.H..]se.M+.!...R..m{..Q#lO..^ev.R:...0.>.....\....=.>.Op.<..p....qN.Vfq,..\F..6.1..+.. .J....c.4?.Jx...u..X+.E.D...Ko.}...s..G..8I.v...8'B....y..).

C:\Users\user\AppData\Local\Temp\3F61.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....>.....

C:\Users\user\AppData\Local\Temp\~DFF5ECB97273E842F1.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DFF5ECB97273E842F1.TMP	
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34E FE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\Desktop\~$Invoice.xlsm	
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:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\user\besta.ocx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7624
Entropy (8bit):	5.6428645067252985
Encrypted:	false
SSDEEP:	192:olVZHCkA26xd3Q4JRveuTtMy47R/Ga0kVhFuPwf8Pn9wHHyJZS:QJvVGaRF8I8Q
MD5:	EB2F7C463E3BEFAD0174E89C10451BCD
SHA1:	80C6604E30655B9BA949210122CCFAF9C7D67766
SHA-256:	5E6DEB3C5AD4E6AB599A3B1A86FCAF25F721C32ED65E83128E9EC0F7ACB1CA0E
SHA-512:	108CF3C4FEE5CC37A16B8A1EF302F66ED6FBE0E5638127689E2F904837688813D8EE424A53A1AABE18034E54B2695852F6DF8B62E792D74B1CD343ECA3A134C
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;.

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.626730610857962
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 51.52% • Excel Microsoft Office Open XML Format document (40004/1) 40.40% • ZIP compressed archive (8000/1) 8.08%
File name:	Invoice.xlsm

General

File size:	38156
MD5:	41b25400c2b31b922dd090e1251b37b8
SHA1:	b543cbb86a4e50506fb9be2ac455e4e606948d65
SHA256:	734577b2ffb53ddf37d71db650178c94c017f8749a9f9497d2f76abd876418a6
SHA512:	54e9149a93dc7ab334251be6d193c4c08f0b6fd93f717e54873c99eab60d1627f55191e2b4ba5b3e1514eecd0875b5ce0446cd0730160dcf57743e0e02ae458
SSDEEP:	768:oi/I83SgrjevZCwVIpvxmUxjfC30+kS4QyoO0VIMo+zl:oinZIIpvxXYk4pTVIQ
File Content Preview:	PK.....!.L#li.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Invoice.xlsm"

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

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 07:01:24.320739985 CET	192.168.2.22	8.8.8.8	0x6371	Standard query (0)	ascarya.digital	A (IP address)	IN (0x0001)
Dec 2, 2021 07:05:45.000212908 CET	192.168.2.22	8.8.8.8	0xcf16	Standard query (0)	crackedshop.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 07:01:24.341840029 CET	8.8.8.8	192.168.2.22	0x6371	No error (0)	ascarya.digital		67.207.81.73	A (IP address)	IN (0x0001)
Dec 2, 2021 07:05:45.022912025 CET	8.8.8.8	192.168.2.22	0xcf16	No error (0)	crackedshop.org		94.102.59.39	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- crackedshop.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49170	94.102.59.39	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 07:05:45.054043055 CET	2	OUT	GET /9/q080U0ARYYL/ 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: crackedshop.org Connection: Keep-Alive
Dec 2, 2021 07:05:45.080452919 CET	2	IN	HTTP/1.1 302 Found Date: Thu, 02 Dec 2021 06:05:45 GMT Server: Apache Location: http://crackedshop.org/cgi-sys/suspendedpage.cgi Content-Length: 232 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 63 72 61 63 6b 65 64 73 68 6f 70 2e 6f 72 67 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body></html>
Dec 2, 2021 07:05:45.083730936 CET	3	OUT	GET /cgi-sys/suspendedpage.cgi 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: crackedshop.org Connection: Keep-Alive
Dec 2, 2021 07:05:45.128349066 CET	3	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 06:05:45 GMT Server: Apache Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2208 Parent PID: 596

General

Start time:	07:02:11
Start date:	02/12/2021
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:	0x13fe60000
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 Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 1724 Parent PID: 2208

General

Start time:	07:06:36
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\rundll32.exe ..\besta.ocx,44532.2932256944
Imagebase:	0xdf0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

File Read

Disassembly

Code Analysis