ID: 532378
Sample Name: Invoice.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:10:36
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

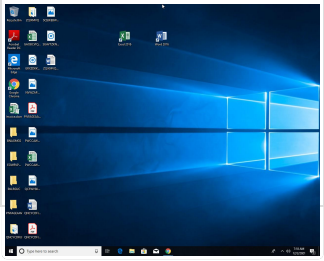
Windows Analysis Report Invoice.xlsm

Overview

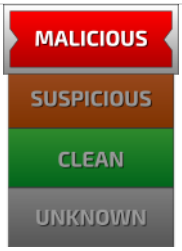
General Information

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

Most interesting Screenshot:



Detection



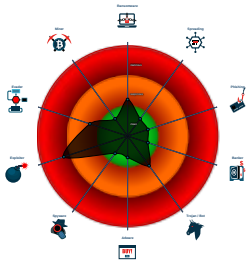
Hidden Macro 4.0

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 w10x64**
- EXCEL.EXE (PID: 6032 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6072 cmdline: C:\Windows\SysWow64\rundll32.exe ..\besta.ocx,44532.2997003472 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **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)

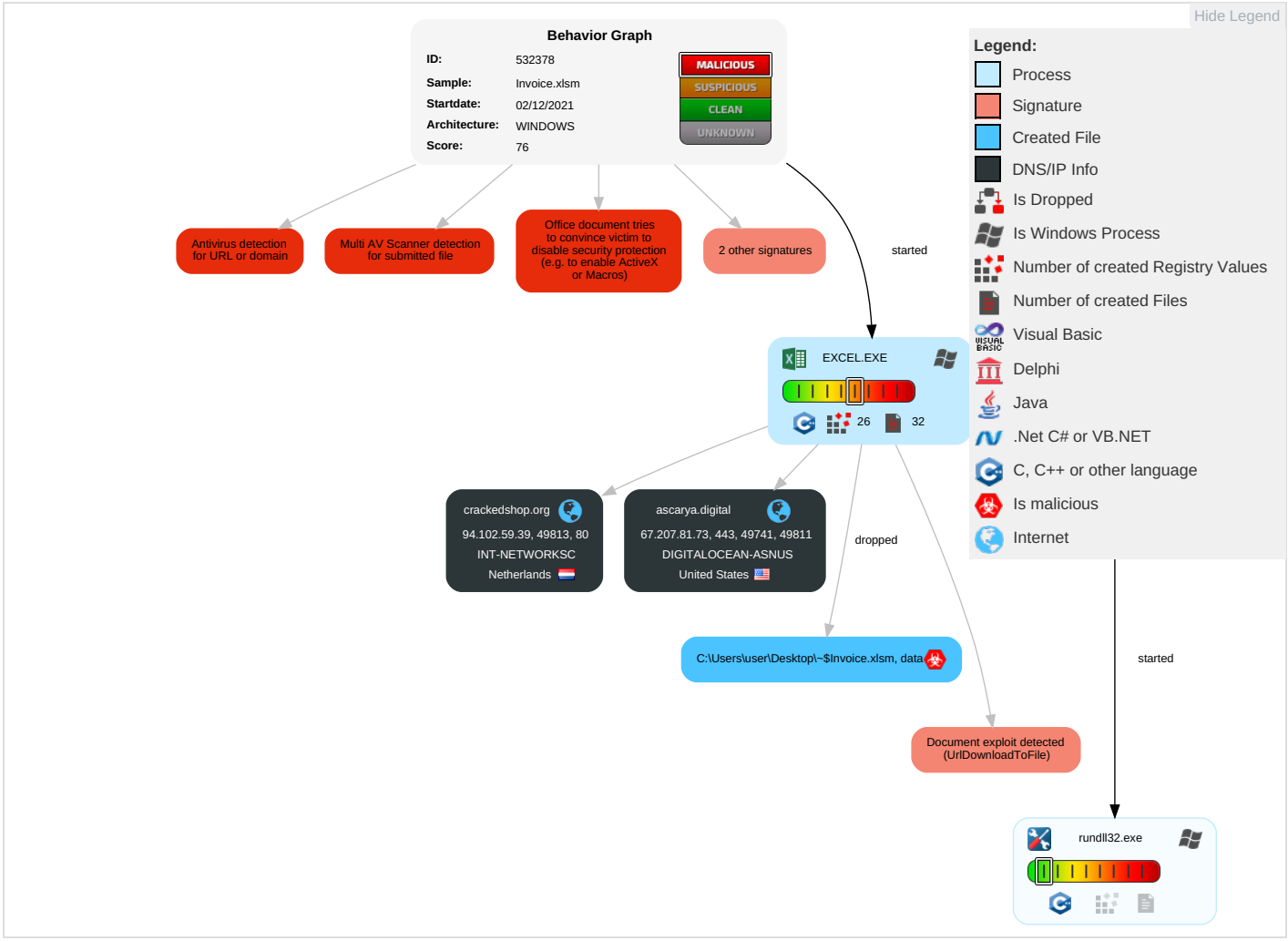
System Summary:

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	In
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 1	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 S P
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	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	Remotely Wipe Data Without Authorization	D L
Domain Accounts	Exploitation for Client Execution 2 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 2	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	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap		C B Fi
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 A R or

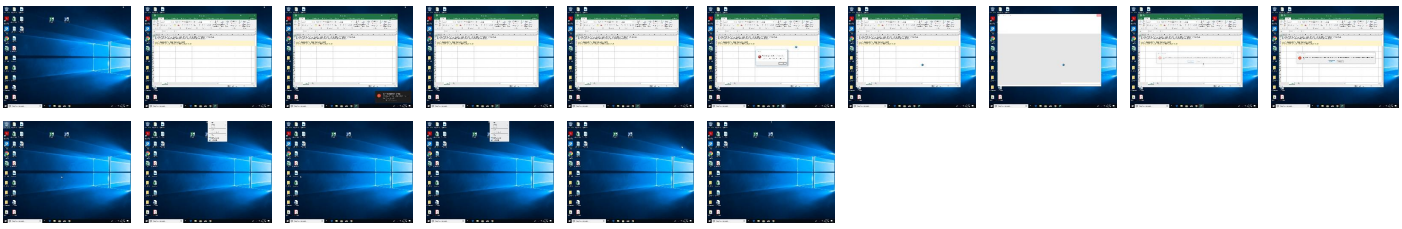
Behavior Graph



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	29%	Virustotal		Browse
Invoice.xlsm	20%	ReversingLabs	Document-Office.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://officesetup.getmicrosoftkey.com:U	0%	Avira URL Cloud	safe	
http://https://nam.learn	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://shell.suite.office.com:1443fU	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://ascarya.digital/wp-con	0%	Avira URL Cloud	safe	
http://https://autodiscover-s.o	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.comZ6	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://substrate.office.com7A	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://ascarya.digital/wp-c	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://www.odwebp.svc.msmhC	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://ascarya.digit	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://ascarya.digital/wp-conte	0%	Avira URL Cloud	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://api.diagnostics.office.com_U	0%	Avira URL Cloud	safe	
http://https://ascarya.digital/w	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ascarya.digital	0%	Avira URL Cloud	safe	
http://https://substrate.office.comP	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filterin	0%	Avira URL Cloud	safe	
http://https://outlook.office.comSharepointFilesHostFormat	0%	Avira URL Cloud	safe	
http://https://devnull.onenote.comMBI_SSL_SHORT	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://crackedshop.org/9/q080U0ARYYL/	100%	Avira URL Cloud	malware	
http://https://ascarya.digital/wp-content%https://ascarya.digital/wp-content/ZH&https://ascarya.digital/wp-	0%	Avira URL Cloud	safe	
http://https://dataservice.o365	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		unknown
ascarya.digital	67.207.81.73	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://crackedshop.org/9/q080U0ARYYL/	true	• 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:	07:10:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice.xlsm
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:	30
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@3/5@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 • Unable to detect Microsoft Excel • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
94.102.59.39	Invoice.xlsm	Get hash	malicious	Browse	• crackedshop.org/cgi-sys/suspendedpage.cgi
67.207.81.73	Invoice.xlsm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ascarya.digital	Invoice.xlsm	Get hash	malicious	Browse	• 67.207.81.73

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	Invoice.xlsm	Get hash	malicious	Browse	• 67.207.81.73
	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
	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
INT-NETWORKSC	Invoice.xlsm	Get hash	malicious	Browse	• 94.102.59.39
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\40484C98-D3A3-480D-91A7-412F4910F605	
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):	140183
Entropy (8bit):	5.357917218722275
Encrypted:	false
SSDEEP:	1536:icQIfgxrBdA3gBwtnQ9DQW+zCA4Ff7nXbovidXiE6LWmE9:KuQ9DQW+zcXfH
MD5:	BEAE9C80966C97CAD37FECAACB55B80A
SHA1:	D08705AE299F59F0033290D5F00A22E8E5260655
SHA-256:	3E00F0607A09972EED9165A44589B27C0DFC69D4B7002B8F8FCD16DA351FCF14
SHA-512:	B7BFC6DDCF0A541467F3DF01E6F56A84DBBE63120C685BF42F16E532346B582B3C2B45B9B4157F5790176F567685D767DD54D2DBC176AC69EB2FE0E4D69E1D7C
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="2021-12-02T06:11:30">.. 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\28CAD6F4.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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\Microsoft\Windows\INetCache\IE\PSUEOSZZ\suspendedpage[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\suspendedpage[1].htm	
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\Desktop\~$Invoice.xlsm	
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:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\besta.ocx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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
File size:	38156
MD5:	41b25400c2b31b922dd090e1251b37b8
SHA1:	b543cbb86a4e50506fb9be2ac455e4e606948d65
SHA256:	734577b2ffb53ddf37d71db650178c94c017f8749a9f9497d2f76abd876418a6
SHA512:	54e9149a93dc7ab334251be6d193c4c08f0b6fd93f717e54873c99eab60d1627f55191e2b4ba5b3e1514eecd0875b5ce0446cd0730160dcf57743e0e02ae458

General

SSDEEP:	768:oi/I83SgrjevZCwVIpvxmUxjfC30+kS4QyoO0VIMo+zl:oinZIIpvxXYk4pTVIQ
File Content Preview:	PK.....!.L#li.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

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 07:11:34.287858009 CET	192.168.2.3	8.8.8.8	0xec1f	Standard query (0)	ascarya.digital	A (IP address)	IN (0x0001)
Dec 2, 2021 07:15:55.350747108 CET	192.168.2.3	8.8.8.8	0xae1a	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 07:11:34.306016922 CET	8.8.8.8	192.168.2.3	0xec1f	No error (0)	ascarya.digital		67.207.81.73	A (IP address)	IN (0x0001)
Dec 2, 2021 07:15:55.372935057 CET	8.8.8.8	192.168.2.3	0xae1a	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	192.168.2.3	49813	94.102.59.39	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 07:15:55.401859999 CET	5658	OUT	GET /9/q080U0ARYYL/ 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: crackedshop.org Connection: Keep-Alive
Dec 2, 2021 07:15:55.429369926 CET	5658	IN	HTTP/1.1 302 Found Date: Thu, 02 Dec 2021 06:15:55 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 07:15:55.434375048 CET	5659	OUT	GET /cgi-sys/suspendedpage.cgi 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: crackedshop.org Connection: Keep-Alive
Dec 2, 2021 07:15:55.480427980 CET	5659	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 06:15:55 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: 6032 Parent PID: 744

General

Start time:	07:11:28
Start date:	02/12/2021
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:	0xc90000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 6072 Parent PID: 6032

General

Start time:	07:15:55
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\rundll32.exe ..\besta.ocx,44532.2997003472
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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