ID: 433278
Sample Name: audit-528010081.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:15:45
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

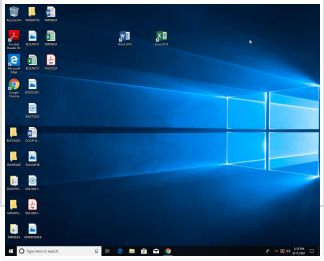
Analysis Report audit-528010081.xlsb

Overview

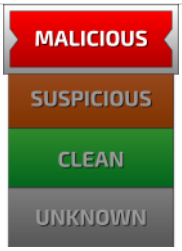
General Information

Sample Name:	audit-528010081.xlsb
Analysis ID:	433278
MD5:	c5d1fad39a32ee2.
SHA1:	71978bfb9a4735e.
SHA256:	1ce2211bfbcb462..
Infos:	

Most interesting Screenshot:



Detection



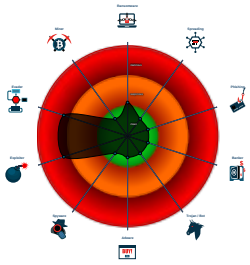
Hidden Macro 4.0

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Found a high number of Window / Us…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Registers a DLL

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6912 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - splwow64.exe (PID: 7132 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
  - regsvr32.exe (PID: 6072 cmdline: regsvr32 -s ..\covi1.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5612 cmdline: regsvr32 -s ..\covi2.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **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

Signature Overview

Signature Overview

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

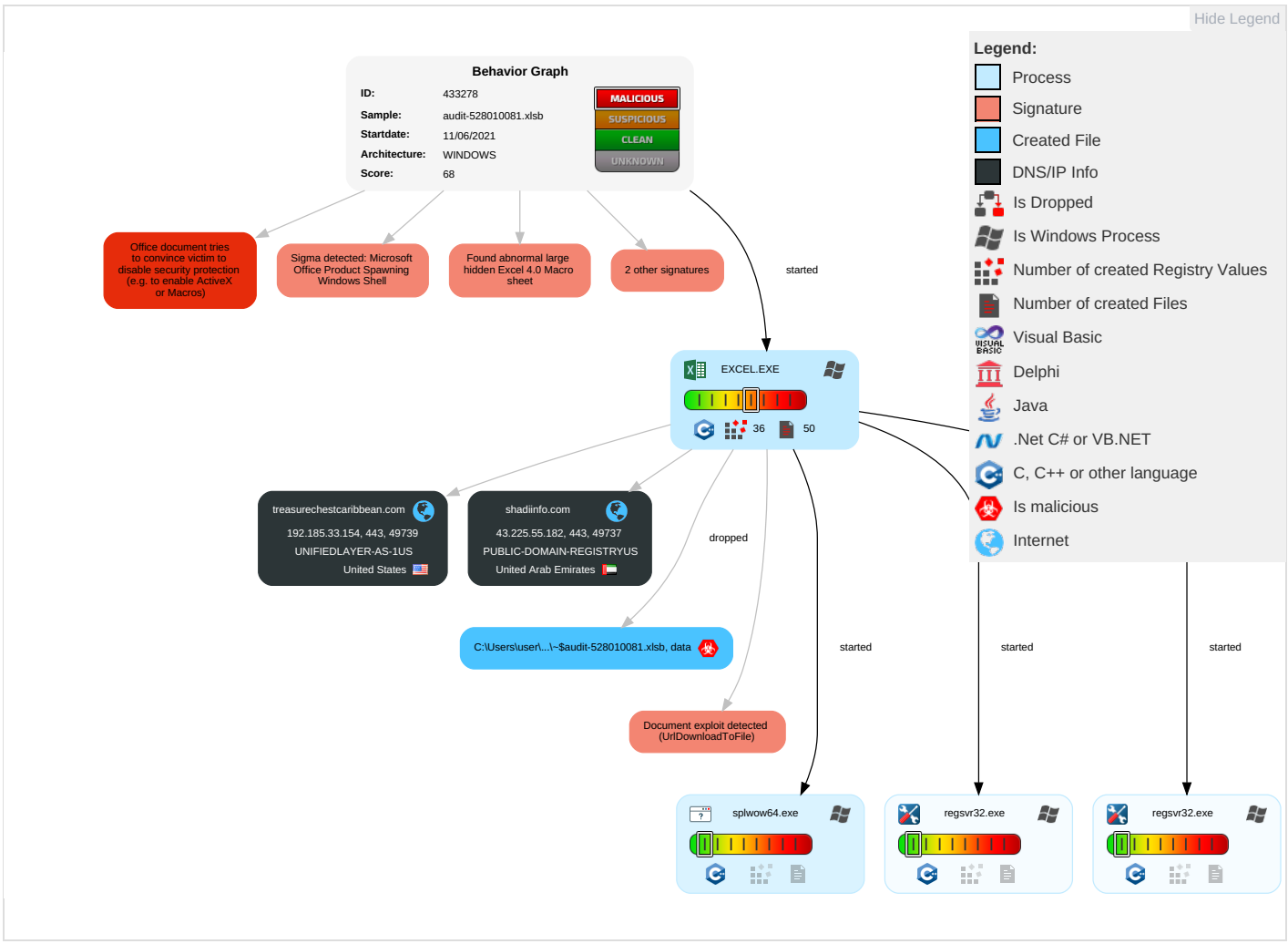
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

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	Scripting 2	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communicatio
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Application Window Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Regsvr32 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

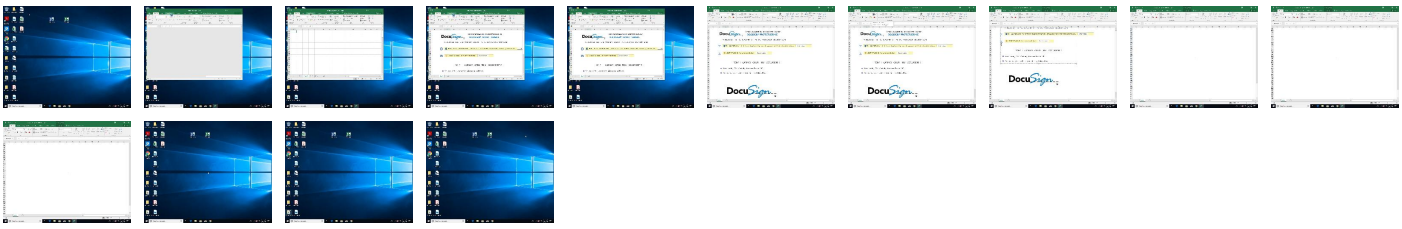
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
treasurechestcaribbean.com	0%	Virustotal		Browse
shadiinfo.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
treasurechestcaribbean.com	192.185.33.154	true	false	• 0%, Virustotal, Browse	unknown
shadiinfo.com	43.225.55.182	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
43.225.55.182	shadiinfo.com	United Arab Emirates		394695	PUBLIC-DOMAIN-REGISTRYUS	false
192.185.33.154	treasurechestcaribbean.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433278
Start date:	11.06.2021
Start time:	15:15:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	audit-528010081.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
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:	mal68.expl.evad.winXLSB@7/10@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: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:16:38	API Interceptor	1174x Sleep call for process: splwow64.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
43.225.55.182	#Ubb38#Uc7ac#Uc778 #Ub300#Ud1b5#Ub839 #Uc2e0#Uc0c1#Uc815#Ubcf4.pdf.exe.exe	Get hash	malicious	Browse	• www.mytargethub.com/s0h/
192.185.33.154	audit-1133808478.xlsb	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
treasurechestcaribbean.com	audit-1133808478.xlsb	Get hash	malicious	Browse	• 192.185.33.154
shadiinfo.com	audit-1133808478.xlsb	Get hash	malicious	Browse	• 43.225.55.182

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Purchase_Order.exe	Get hash	malicious	Browse	• 162.241.253.69
	audit-1133808478.xlsb	Get hash	malicious	Browse	• 192.185.33.154
	my_attach_82862.xlsb	Get hash	malicious	Browse	• 50.87.220.158
	Fax_Doc#01_5.html	Get hash	malicious	Browse	• 162.241.7.171
	WcCEh3daIE.xls	Get hash	malicious	Browse	• 162.241.77.193
	KCTC International Ltd.exe	Get hash	malicious	Browse	• 192.254.185.244
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 74.220.199.8
	supply us this product.exe	Get hash	malicious	Browse	• 50.87.146.199
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 192.185.74.169
	3arZKnr21W.exe	Get hash	malicious	Browse	• 192.254.235.195
	6b6zVfqxbk.xlsb	Get hash	malicious	Browse	• 216.172.184.23

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HM-20210428 HBL.exe	Get hash	malicious	Browse	• 192.254.180.165
	INQUIRY. ZIP.exe	Get hash	malicious	Browse	• 50.87.190.227
	audit-78958169.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	research-1315978726.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	ExHNIXd73f.exe	Get hash	malicious	Browse	• 108.167.142.232
	research-2012220787.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	research-2012220787.xlsb	Get hash	malicious	Browse	• 216.172.184.23
	viVrtGR9Wg.xlsb	Get hash	malicious	Browse	• 192.185.113.120
	DEMLwnv0Nt.xlsb	Get hash	malicious	Browse	• 192.185.113.120
PUBLIC-DOMAIN-REGISTRYUS	NEW URGENT ENQUIRY.exe	Get hash	malicious	Browse	• 208.91.199.223
	Recibo de banco.exe	Get hash	malicious	Browse	• 208.91.198.143
	KC8ZMn81JC.exe	Get hash	malicious	Browse	• 208.91.199.224
	audit-1133808478.xlsb	Get hash	malicious	Browse	• 43.225.55.182
	Factura PO 1541973.exe	Get hash	malicious	Browse	• 208.91.199.223
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	NEW ORDER 112888#.exe	Get hash	malicious	Browse	• 208.91.199.224
	oRSxZhDFLi.exe	Get hash	malicious	Browse	• 208.91.199.225
	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	Get hash	malicious	Browse	• 208.91.199.223
	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	• 208.91.199.223
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 207.174.212.247
	SecuriteInfo.com.MachineLearning.Anomalous.97.15449.exe	Get hash	malicious	Browse	• 208.91.198.143
	lFccIK78FD.exe	Get hash	malicious	Browse	• 208.91.198.143
	Order10 06 2021.doc	Get hash	malicious	Browse	• 162.215.241.145
	PO187439.exe	Get hash	malicious	Browse	• 119.18.54.126
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	• 208.91.199.225
	JK6Ul6IKioPWJ6Y.exe	Get hash	malicious	Browse	• 208.91.198.143
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.832.15445.exe	Get hash	malicious	Browse	• 208.91.198.143

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	3.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	audit-1133808478.xlsb	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	tXkin8g4sy.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	xGrfj8RvYg.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	my_attach_82862.xlsb	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	document-47-2637.xls	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	logo.png.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	document-47-2637.xls	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	Fax_Doc#01_5.html	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	wa71myDkbQ.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	Current-Status-062021-81197.xlsb	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	logo.png.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	3F97s4aQjB.xlsx	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	WcCEh3daIE.xls	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ATT00005.htm	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	kxjeAvsg1v.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	VSA75RUmYZ.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	iX22xMeXIc.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154
	QWkt5w3cO2.exe	Get hash	malicious	Browse	• 43.225.55.182 • 192.185.33.154

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\86CA0570-570E-45EB-89AD-3E5582F24DA2	
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):	134922
Entropy (8bit):	5.369099574686396
Encrypted:	false
SSDEEP:	1536:WcQIKNEeBXA3gBwlpQ9DQW+z7534ZliKWXboOilX5ENLWME9:mEQ9DQW+ziXOe
MD5:	F3AE32D1B695C465CD8E84DD4BA446CA
SHA1:	3CA25B5D3A6D2054E0FB0AF734FFAD6DBC0A3D9F
SHA-256:	7EB8BF780AE3BBC2D237F835F0E5EF746BDC0B4FCEB4EE4A66B3C6478C881DE2
SHA-512:	EAB04BCAF30153E7F4D89A70506894F2DE01E718CE584B279D7E4DF4EFBDF4ED1D3D2F55690E8A9FCC5EA3177B28AD0D8076091AB77F48814DDCB4D33BBC923
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="2021-06-11T13:16:36">.. Build: 16.0.14209.30527-->.. <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\15B60C59.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 521 x 246, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	32996
Entropy (8bit):	7.975478139053759
Encrypted:	false
SSDEEP:	768:N4k48AnTViUidx37OODgvnrxtxAudMN1VTRVHdB4K7K:NE8m+L37OOwrCXN1VTR1PK
MD5:	4E69B72B0CE87CC7EE30AA1A062147FE
SHA1:	09B0AA5414E08756E0AE53E1BE5C70DB4DEAF2E8
SHA-256:	77A1F749389CBF771D5197FF0FF17113FCA1D91989ADCADF2852876A6CC14988
SHA-512:	6246AF2137E773F7719033AFE75F0B00FF3A4B5543DBA53737FC8D33EE42478E3D8A5CF166E9EFD2F54A2F3E0D62417BDDC1CB824642305B59AB1229313D2D79
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....[.J....sRGB.....pHYs.....+.....IDATx^.].`.....{%.$..A...R.P@z....O...S.<;.VT.REA.(...I...{.....m...]..r./.....~.[]h.Z....P.(.....E."@...P.(.v.P.@..E."@.....#@y.....E."@y.....E."...*78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3..P.(.....B.{..E.".y.P..ykNgL...P..!@y.3.....E....."@...8C...g...).....!@y..9.1E."@.p.....S.(....C....[s:c..E.".....!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3..P.(.....B.{..E.".y.P..ykNgL...P..!@y.3.....E....."@...8C...g...).....!@y..9.1E."@.p.....S.(....C....[s:c..E.".....!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x..P.(.....B.{..E.".y.P..ykNgL...P..!@y.3.....E....."@...8C...g...).....!@y..9.1E."@.p.....S.(....C....[s:c..E.".....!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\165B7932.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 490 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	18547
Entropy (8bit):	7.9850486438978985

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\165B7932.png	
Encrypted:	false
SSDEEP:	384:kBCIQCloAwCZDy0xOTn6/g6l4NpWfw9nHk6Ka01f7Y/H:kBCIQpAwODPMT6/gfOUKN70
MD5:	ED31C7053D581EDC4C98D222CE02EDEF
SHA1:	6BA7A49CC6FF8FE00E9C5BC75F48AB7E679536DD
SHA-256:	0FCF61397154DF01CFAECA362BD643D88AAD5FEDD07B52DC8A921CC0D7236534
SHA-512:	929BF13F2A050B33D0EABDAC97CAAFDDE612AD521027FEE4DD51E28A3CF61198D6C045E00AB85223C73D74D18BB4EAA1681C7AFA917946DC08A3C75FB2AB4935
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....l{.....sRGB.....pHYs.....+....H.IDATx^...U....."x....U...."...Tc.{...M1M..In....TATb4F,`oD..Q..3.....g.3..Lr.D....a8....~.z....Z...yyF..9...:.H .Q2..)/L.....Q.}....(J..,...w2>R.$..G2..m>..|...0.M.g.Xnjj...P.v..x....S.....B..p.=.Lz.^..Wi..2U.V'.a..*DE.'..rT.z....#.;..]....[?.C...o.m`]..m][;.:<..]F.9..u..Q]c.Ue.9....(.F.Z.~s..Q:..B.. .)..LZ.TTo..P.gc.l.'.X.}..H....Q.h\|....L..rcd.2dN..co..5.....w.U.4..}.....{.Q.....D2.J.z~..:Y3,.H..(#.J.Q.....N.._7....w.....].2w.6...._....u.....9-.7.f9...E9...p.A..f....=....Bqu....A .u.JG>b"...%..0..W.H=...G#.DR.....P.\|FD).NJ....)>.;...M...T*.dW..t:[.xT..M.\|S...O..."M.4u7.uS...]4..R.vK....*).ZK.. J.=.9C.].kr..ES..6..f.(.....N':..t..^.S....kn[s.#..(.....m.....~....6>.... :u.J.mO.....%D...Q...6%....!......H.....v..^%....$.._..V.....[o5.H8.....n.~M.z.RL.0p:.iC.k.1..$.....3[....mS5.....E...2.&...k]...A.....K.8...5..O.@7.[-.F4*7...i....in...y....A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\33236C84.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 246 x 108, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	10270
Entropy (8bit):	7.975714699744477
Encrypted:	false
SSDEEP:	192:3sXvKLMbye/PEXiKTUgCto9h4F6NwfU6vGDpdYNbcQZgkbd4cgc:3iLh/gJ59CDfU6LocbGK
MD5:	9C4F09E387EA7B36C8149EA7C5F8876E
SHA1:	FF83384288EB89964C3872367E43F25FAFF007CC
SHA-256:	A51C1D65092272DAEB2541D64A10539F0D04BC2F51B281C7A3296500CFCA56DE
SHA-512:	0FDDE22CFDDE8BB1C04842D2810D0FD6D42192594E0D6120DE401B08B7E2CFFB5333792BC748E93CD70FA14734CC7D950620CB977DDBBDB52D92BDA8F3552F8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....l.....sRGB.....pHYs.....+....'.IDATx^.].|.U...%...J."....H.&Ui.....E.....D.7....U.i..FH#=.....3..$K...'{3....7.....0.H.....H..03.,....8.q.....'@\. ..S@.../.0=....\|....}\|.....0.... ...,LO.....q._`az.....8..... .`..) @...X...q..>N...>.....q.....'@\...S@.../.0=....\|....}\|.....0.... ...,LO.....q._`az.....8...I..m.i'Sj.W.i.S.TJ....D.D._%...] ..i.;J..b..T.).Ik.L6..L.mN....!*..\..'{$.o._b..h....t"@.?...y...d..h..|..B9D..CJD..t."......bR"....I)H....z.....>|.....E.x..r....J.U..[...p:D....XF.....A...E.....b..C...C..C.....=.Z..$.=../....Y ..x5CY.0l...,~.W. .?.....;...$.'....<.H.2...z..6(.E.....kw8w^.\~..."..C,gl&.m..J2.).HI.....b.r...'.....r.H...P....'...A.^.q..j).cZ.^1~.|.....dv^.^v..X..v..6/^.$rR. iK..H.Uu.Pvk....U.....'.Fd..Z .]mu*1.Zb.\b...N..P..&tr;.W....J.K(@.^A..R.S.[~.v.R.YO...0-...2..h."..............7..Ng...R...e.&..@..t..N...{5...W.x./#.%..}t...F8-..M1..(4b1....&.....)B...6.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4EED1AB5.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 934 x 29, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	42557
Entropy (8bit):	**7.992800895943226**
Encrypted:	**true**
SSDEEP:	768:Pfsq4UmepRdblCFcXhw9KnRTRews6xD0FvBlwAS1A8x7BcS0OvD230:PR3ZblCF28KRsws6CFv0AYx7Bl3b230
MD5:	B1F262A694930ADB699FA94E3394887F
SHA1:	9C9B66D3A3F09AECA45DB94304CDD6FB3C5BD4C9
SHA-256:	9C99EC61392B9022A38C1354124360147E8185065095BD2EC92B1416CF9F4B68
SHA-512:	1CA7E6750178B88EC3AA7A0B83348EA389E26C27E0D7E919D807BE470714E5B4F04ACEB69D391F0498D4E465E6620E9449CA2F40755B5CE8196E683502EBF5F4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....6.....sRGB.....pHYs.....+.....IDATx^....dU....S.:ON.0.0....s0 ....$..%#HR.T.....$..0C...Su...[.TM..{.....C.S}..^{.....].^..ZX.Wb.W....X!..A.P... .0..u...X.V.3.....z..tiO{GW..?...A.....ca2Y.... ...cAX..zZ..2M.$..g.O.e..r?z&.....*....*.=..Z.A.....a.Z..ka<..N.R.c...../.[..j.^...Nk.(..y.,..z"...R..Z+..D1Q....z....0..u~. .jU_..b.Z.V....:.5:.(.....-...A2.O.{..p.j..].<.....0..0..+...E...^...z....#..j.d...X._..1..M.5..O.^..^..".."..l....G....U1.....X.6.Z.\.&..h..m*..T..xH.j..3<$.H...a..n....}t.A.jT.6G.h@..<.x..x...cb.. ....C..{.D.'QW<.o~..?.....4F_...B..h.\...y8..)....j.Z.d..#P..P..O.....(.0...f....B_z>.E .w../..(...'.Fw..yT..G..)...b9..g.AA`.a..v.zfY.F....._r.i.d.`....Q.g.m"..\..&.t.X.q1}.$.S....2..~...d."..1.. (.0.F....t...i..@f.. ...(..8..q.....I.....ad.....z%....;...y.O...X<Q..X.....B..H.....<)....4.&9.4.....1.h..#B.....g.....bO.59.A..M.....J..vX3*5..X....(G.A.u...8.. .{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\742F88CF.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\742F88CF.png	
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.IR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g...._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. I@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D7DB1686.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.].....O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."....y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S...~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Temp\0CB40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	159443
Entropy (8bit):	7.962645940015211
Encrypted:	false
SSDEEP:	3072:y89VlUBWA6CFvA7brCxAVIKuSkmxVymd1xXP8lTkdm3bGeAxiyDz:y83liWA6FiYpxVyWxf8lTkeGKG
MD5:	E0CAD220B73456AE95191134C888EB92
SHA1:	55C394BB614512A78F0402D3002A2C17D39D97C0
SHA-256:	F431D94B21413C6EC8C0051B371FCC41161FFED3C74602190235017DA1FF2778
SHA-512:	AEAE752C821B320D406EB975CFA0044A57155DE50480005F357FD59D2A3BD2CD7E229164306BDDE3F34A8A9083C9BE9CAA91C630A934194A6505B8C45DCA145 4
Malicious:	false
Preview:	.U.n.0....?.....(..r.mzl.$...\K....I..V.6Pl.6.^.....v.7.k.'...k.U3c.8.v].~=\|.?...pJ..e[@v.x.n.....E;lY.R..9.....pt...D...A..._.f.....Ku..l1..+.hRu...;%K.X.u._.j...h)...ON."..j.%(/.-A7."..=@ ...Q.c...(1d\|.3.....Ys.>....4....E.T...?.Yo0.}..~R..VP..~.Kn...>..... .L.5l$..8.X!..ubi..v/..0.H..vu..Mr.~9..<Q....Q.....3'...C...r$.Q.Sr. ..)]6).DC.x...W.....=....>.....o.#:T..Y.....}.:.K....." Lw.e...:...a?[.&..v.....n^...7.....PK.....!..:.....m.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3 342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$audit-528010081.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data

C:\Users\user\Desktop\~$audit-528010081.xlsb	
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.955291352167221
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	audit-528010081.xlsb
File size:	158780
MD5:	c5d1fad39a32ee229d259535bc2932f0
SHA1:	71978bfb9a4735e33395d4ac5dfaa967cb83b43f
SHA256:	1ce2211bfbcb4628c6b3bd5f3c702d58f803c5f6a2407d512e0d4b66b46d7975
SHA512:	499f30dadebf91f9335528d97b1ca4e0b7aace07cc582e7aa61cb2fcca493e45cef665f0fac292364750b8846c6131324d49a3089c751395b1650108e673e491
SSDEEP:	3072:TtbU9VlUBWA6CFvA7bRCxAVIK2xVymd1xXP+Ph9vajtC1gBbZP6i:ZU3liWA6FsY2xVyWxf+QegBbd
File Content Preview:	PK.....!.^.~.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "audit-528010081.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:	

Indicators

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
Jun 11, 2021 15:16:43.331973076 CEST	192.168.2.4	8.8.8.8	0x5f7a	Standard query (0)	shadiinfo.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:16:44.959717035 CEST	192.168.2.4	8.8.8.8	0xfc28	Standard query (0)	treasurechestcaribbean.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 15:16:43.399655104 CEST	8.8.8.8	192.168.2.4	0x5f7a	No error (0)	shadiinfo.com		43.225.55.182	A (IP address)	IN (0x0001)
Jun 11, 2021 15:16:45.140634060 CEST	8.8.8.8	192.168.2.4	0xfc28	No error (0)	treasurechestcaribbean.com		192.185.33.154	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 15:16:43.923721075 CEST	43.225.55.182	443	192.168.2.4	49737	CN=shadiinfo.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri May 14 13:03:47 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Thu Aug 12 13:03:47 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 15:16:45.476648092 CEST	192.185.33.154	443	192.168.2.4	49739	CN=*.treasurechestcaribbean.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat May 15 10:36:32 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Aug 13 10:36:32 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6912 Parent PID: 800

General

Start time:	15:16:35
Start date:	11/06/2021
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:	0x1130000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: splwow64.exe PID: 7132 Parent PID: 6912

General

Start time:	15:16:37
Start date:	11/06/2021
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff610d60000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: regsvr32.exe PID: 6072 Parent PID: 6912

General

Start time:	15:16:46
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s ..\covi1.dll
Imagebase:	0xd70000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 5612 Parent PID: 6912

General

Start time:	15:16:46
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s ..\covi2.dll
Imagebase:	0xd70000

File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis