ID: 532384
Sample Name: SRLTX-1266305223.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:45:35
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

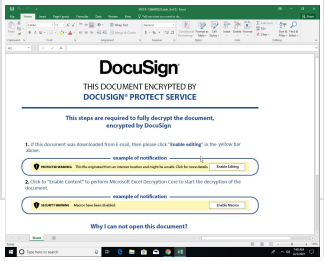
Windows Analysis Report SRLTX-1266305223.xlsb

Overview

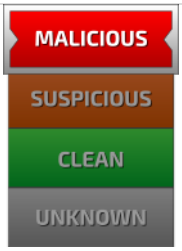
General Information

Sample Name:	SRLTX-1266305223.xlsb
Analysis ID:	532384
MD5:	9a33b86fa2ee237.
SHA1:	d94101917d187d..
SHA256:	141a23ce14ba67..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection



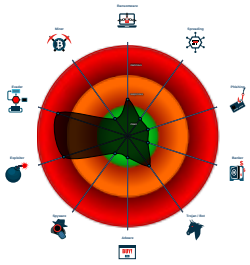
Hidden Macro 4.0

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for subm…
- Found malicious Excel 4.0 Macro
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Found protected and hidden Excel 4…
- Found a hidden Excel 4.0 Macro she…
- Potential document exploit detected…
- Tries to load missing DLLs
- Tries to connect to HTTP servers, b…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 7036 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 336 cmdline: regsvr32 C:\ProgramData\Volet1.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6812 cmdline: regsvr32 C:\ProgramData\Volet2.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 1328 cmdline: regsvr32 C:\ProgramData\Volet3.ocx 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

Jbx Signature Overview

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary:

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

Found malicious Excel 4.0 Macro

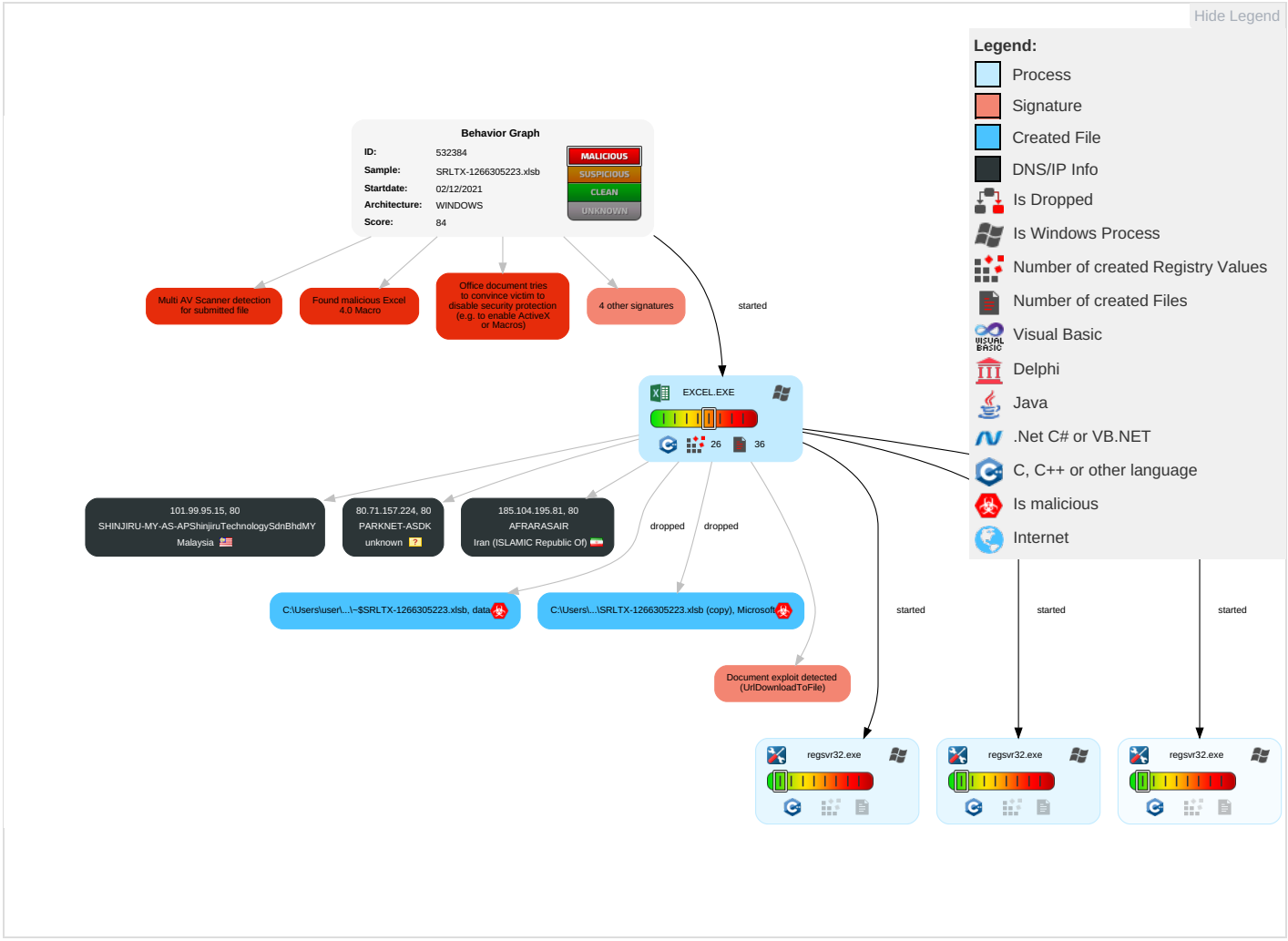
Found Excel 4.0 Macro with suspicious formulas

Found protected and 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	Remote Service Effects	In
Valid Accounts	Command and Scripting Interpreter 2	DLL Side-Loading 1	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	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	Exploitation for Client Execution 2 1	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	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B Fi
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R o

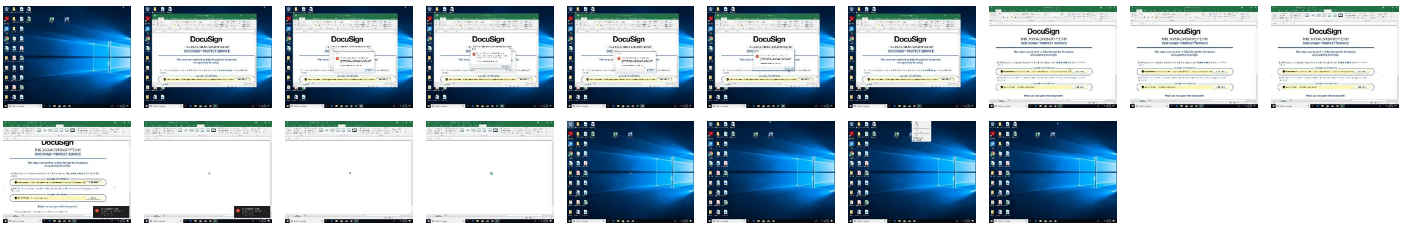
Behavior Graph

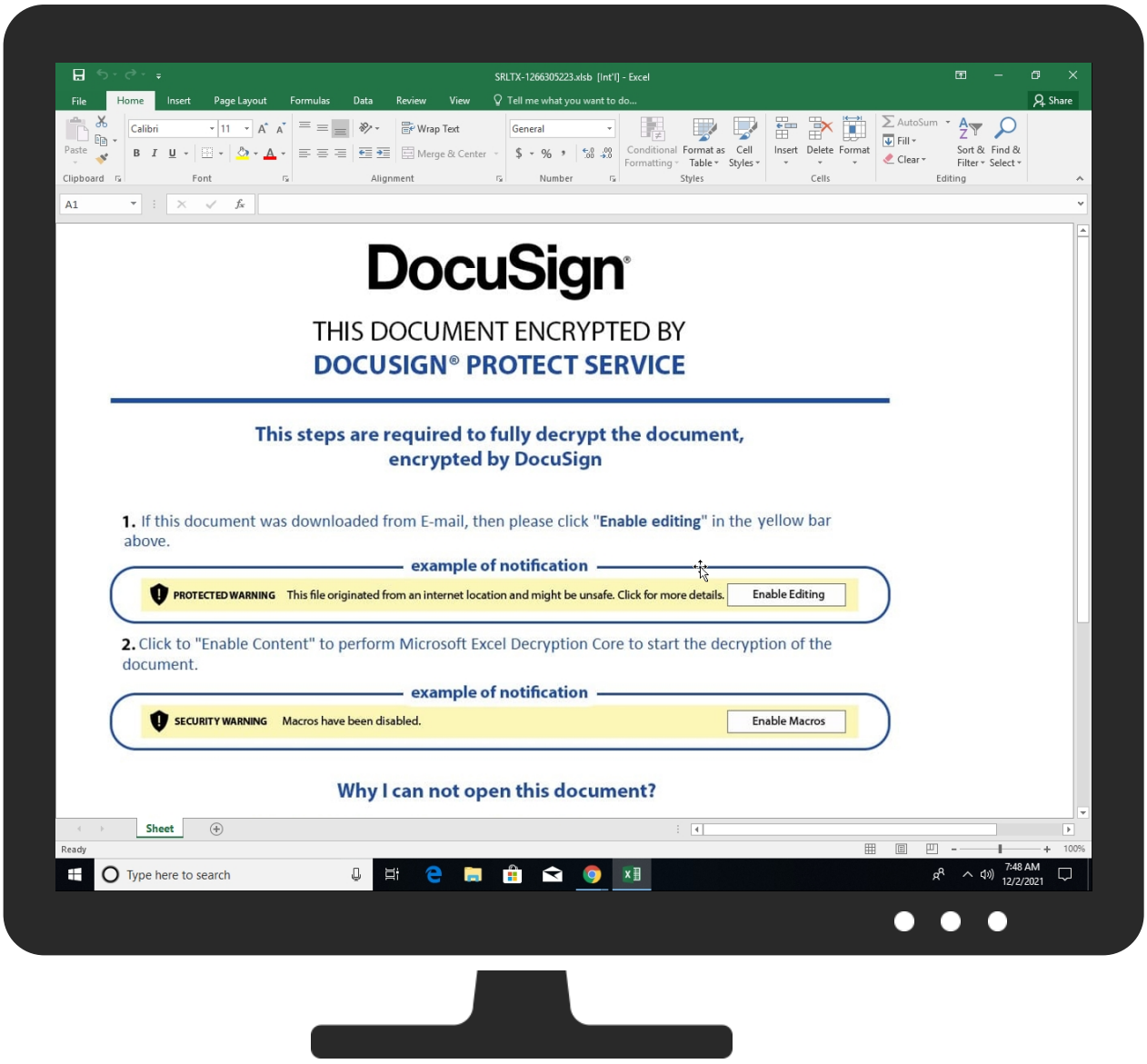


Screenshots

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
SRLTX-1266305223.xlsb	15%	Virustotal		Browse
SRLTX-1266305223.xlsb	33%	ReversingLabs	Document-Excel.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://incidents.diagnosticssdf.office.comt	0%	Avira URL Cloud	safe	
http://https://token.cp.micr9	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://api.office.netQ#	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://api.powerbi.	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://schemas.open	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://login.wind	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://80.71.157.224/819077238125.dat	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://api.onedrive.comcent	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptioneventsEi5	0%	Avira URL Cloud	safe	
http://https://outlook.office.com2BFEE2(	0%	Avira URL Cloud	safe	
http://https://management.azure.comg	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://substrate.office.comP	0%	Avira URL Cloud	safe	
http://80.71.157.224/819077238125=	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://staging.cortana.ai.c	0%	Avira URL Cloud	safe	
http://https://augloop.of	0%	Avira URL Cloud	safe	
http://https://api.diagnosticssdf.office.comA	0%	Avira URL Cloud	safe	
http://80.71.157.224/	0%	Avira URL Cloud	safe	
http://https://outlook.of	0%	Avira URL Cloud	safe	
http://https://outlook.office	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.104.195.81	unknown	Iran (ISLAMIC Republic Of)		202391	AFRARASAIR	false
101.99.95.15	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	false
80.71.157.224	unknown	unknown		197301	PARKNET-ASDK	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532384
Start date:	02.12.2021
Start time:	07:45:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 25s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SRLTX-1266305223.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	27
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:	mal84.expl.evad.winXLSB@7/6@0/3
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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.104.195.81	SRLTX-827324351.xlsb	Get hash	malicious	Browse	• 185.104.195.81/767224823161.dat
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	• 185.104.195.81/319199189746.dat
101.99.95.15	SRLTX-1266305223.xlsb	Get hash	malicious	Browse	
	SRLTX-207074251.xlsb	Get hash	malicious	Browse	
	SRLTX-207074251.xlsb	Get hash	malicious	Browse	
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	
80.71.157.224	SRLTX-1266305223.xlsb	Get hash	malicious	Browse	
	SRLTX-207074251.xlsb	Get hash	malicious	Browse	
	SRLTX-207074251.xlsb	Get hash	malicious	Browse	
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	SRLTX-1266305223.xlsb	Get hash	malicious	Browse	• 101.99.95.15
	SRLTX-207074251.xlsb	Get hash	malicious	Browse	• 101.99.95.15
	SRLTX-207074251.xlsb	Get hash	malicious	Browse	• 101.99.95.15
	exel.exe	Get hash	malicious	Browse	• 111.90.143.12
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	• 101.99.95.15
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	• 101.99.95.15
	jydygx.arm	Get hash	malicious	Browse	• 101.99.125.127
	9LC8BVglps.exe	Get hash	malicious	Browse	• 111.90.158.95
	purchase_order.exe	Get hash	malicious	Browse	• 111.90.149.196
	24390844104405462,pdf.exe	Get hash	malicious	Browse	• 111.90.149.196
	YaMfg60AB4.exe	Get hash	malicious	Browse	• 111.90.149.196
	EDyyOwFu2Y.rtf	Get hash	malicious	Browse	• 111.90.149.196
	PaymentCopy-18112021.exe	Get hash	malicious	Browse	• 111.90.149.196
	Halkbank,pdf.exe	Get hash	malicious	Browse	• 111.90.149.196
	ACILISTEK.exe	Get hash	malicious	Browse	• 111.90.149.196
	111821 New Order_xlxs.exe	Get hash	malicious	Browse	• 111.90.149.196
	invoice.pdf.exe	Get hash	malicious	Browse	• 111.90.149.196
	ujbZuYEbJR.exe	Get hash	malicious	Browse	• 111.90.149.196
	INVOICE - FIRST 2 CONTAINERS 111.xlsx	Get hash	malicious	Browse	• 111.90.149.196
	#Ud83d#Udcdewav_audio__Atlanticare__#985850.HTM	Get hash	malicious	Browse	• 111.90.145.235
PARKNET-ASDK	SRLTX-1266305223.xlsb	Get hash	malicious	Browse	• 80.71.157.224
	SRLTX-207074251.xlsb	Get hash	malicious	Browse	• 80.71.157.224
	SRLTX-207074251.xlsb	Get hash	malicious	Browse	• 80.71.157.224
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	• 80.71.157.224
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	• 80.71.157.224
	F2433DFBA69148A0C3A5A5951D360B6C3C045090DE06F.exe	Get hash	malicious	Browse	• 80.71.158.167
	0PTqb4jxab.exe	Get hash	malicious	Browse	• 80.71.158.106
	QJX8FxGICW.exe	Get hash	malicious	Browse	• 80.71.158.106
	CbQPj4t8t8.exe	Get hash	malicious	Browse	• 80.71.158.106
	ykHVrz0Rhn.exe	Get hash	malicious	Browse	• 80.71.158.106
	BW3YgASkbP.exe	Get hash	malicious	Browse	• 80.71.158.106
	ZxsTMGzhcI.exe	Get hash	malicious	Browse	• 80.71.158.106
	CI + PL.docx	Get hash	malicious	Browse	• 80.71.158.94
	4o6tbR4nsF	Get hash	malicious	Browse	• 194.62.170.231
	wFob8Dpa4z	Get hash	malicious	Browse	• 80.71.137.238
	taugif.exe	Get hash	malicious	Browse	• 80.71.138.195
AFRARASAIR	SRLTX-1266305223.xlsb	Get hash	malicious	Browse	• 185.104.195.81
	SRLTX-207074251.xlsb	Get hash	malicious	Browse	• 185.104.195.81
	SRLTX-207074251.xlsb	Get hash	malicious	Browse	• 185.104.195.81
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	• 185.104.195.81
	SRLTX-827324351.xlsb	Get hash	malicious	Browse	• 185.104.195.81
	Hilix.arm7	Get hash	malicious	Browse	• 185.49.104.0
	BitmCvTrdO	Get hash	malicious	Browse	• 185.49.104.4
	17Rom1F3MY	Get hash	malicious	Browse	• 185.49.104.8
	Yx8iF6YZtN	Get hash	malicious	Browse	• 185.49.104.3
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	• 185.118.15.137
	SecuriteInfo.com.Exploit.Siggen3.10048.14515.xls	Get hash	malicious	Browse	• 185.118.15.137

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\AC8CAF02-683E-48A7-A700-0718A72BFEE2	
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):	140372
Entropy (8bit):	5.357229829528279
Encrypted:	false
SSDEEP:	1536:YcQIfgxrBdA3gBwtnQ9DQW+zUA4Ff7nXmvid1XiE6LWmE9:EuQ9DQW+zmXfH
MD5:	27E11A15A6ED929ECB395BFD8F745FCC
SHA1:	C7399E97144390A957EA450AD718A38034F101F0
SHA-256:	390FAF8C103292F08B6437A91A9F7E5F2A4B4A3217E21104CEF89BF91E989660
SHA-512:	038B3E9455E8415DB102FFB945E6DCB26D046D4D6CF9C0DA701E4DD999F2D0606941DFFF7B0031B1FF43B8C3FBC0C6865F29992C3E86750471928AC960F33B2
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="2021-12-02T06:46:26">.. Build: 16.0.14729.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\5725A463.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1098x988, frames 3
Category:	dropped
Size (bytes):	85681
Entropy (8bit):	7.915850776614707
Encrypted:	false
SSDEEP:	1536:wB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUw:Pc6EehCfCZpUHKGXbBKsiit
MD5:	4F100E2CEFED046B44EC799015B454EF
SHA1:	5149E5D1B5212C77B3548914E9B47D67B4BEA574
SHA-256:	D30B441AB0E88A1487F29A80D63E2A4865A3F5DF7854FB8359B354397F807E2C
SHA-512:	153581151434815CC17E88D587FF6A6AF8F7154B4A05146453A9814F662C68D79F1063BDD9F789A1DB2F5818D199EF600703F8BC35785B0705332EC231F35A14
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....'.....'#*" "*#>1++1>H<9<HWNNWmhm.....'.....'#*" "*#>1++1>H<9<HWNNWmhm.....J.."..... .....".....q.[..+...*...K.... .....?.....g....6..)....=~.....w5.....7_.-.....k.../..;.....!.z%o..w!...,.....?...Gs?.].....C..P~i._.=. .`....{...w.....".-.....:..d.....;z7)...~g.....C....v..\..O.....0...v.....v... .....A...;.~Y.}.....MsC.~..5..?.;.....V7....G...b..~.....@.....O.}...o4.s_...z78.1.yl.. .X~.u..~..S....J..V~S..x.u~.. .....@....u..m....rGrf.P.._+Z..?AW..~..u.G.....o&.....9.0...H.Zx...M.y.[kW..o.....;.....z.....}v.m.. [R.i....R..m....+.J.....r6.P....|s..].vO._.}..K.]-V.U=9}.....W.....3.....G.t}Y

C:\Users\user\Desktop\6FC30000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	99214
Entropy (8bit):	7.8296133896152025
Encrypted:	false
SSDEEP:	1536:IhyB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUwPK:Inc6EehCfCZpUHKGXbBKsiiXS
MD5:	93D04DC3942D1A4D5DF6B05DA0CD184F
SHA1:	372C04075B369906E325B24994FEACFBF6B7C2BC
SHA-256:	8C707A624467594965109FE09A059984BDCEC23F98E0C7C8F4655AC536E443B2
SHA-512:	91277E3C7004D1CE21B1CECBD4091ECF418A9857B3FE43AC2C23CCAE653426860A516CCC85D17739DCDADC1A81E4B423663878AAA9461E897D5E7F2B58CD041
Malicious:	false
Reputation:	low
Preview:	PK.....!.V.....[Content_Types].xml ...(..... ....U.n.0.}G..".....BM..C.....^|.x8.....v...&kTx.....{..e....jg+...V.....{V`.VI.,TI...._.n... ...1..B`.B'.;...I\.d.ah...O..X,....6.1q....I..UO.w+....w.T..F.2. B.U..... r.....M..".....0.....N..l..7dsD!..w0.....&I}...ZAq-C.&;.F.Fd.9...F._.)...h....r..../VA?K.p...O...../.s....?.d.....S.v...K>].c...6.].r.CG...4O.4R....p...b.....M.t..c..8!..... D/d..Q.p.1f....n..0....}..>...d0S.....X...

C:\Users\user\Desktop\6FC30000:Zone.Identifier	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\Desktop\6FC30000:Zone.Identifier	
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Desktop\SRLTX-1266305223.xlsb (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	99214
Entropy (8bit):	7.8296133896152025
Encrypted:	false
SSDEEP:	1536:IhyB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUwPK:Inc6EehCfCZpUHKGXbBKsiiXS
MD5:	93D04DC3942D1A4D5DF6B05DA0CD184F
SHA1:	372C04075B369906E325B24994FEACFBF6B7C2BC
SHA-256:	8C707A624467594965109FE09A059984BDCEC23F98E0C7C8F4655AC536E443B2
SHA-512:	91277E3C7004D1CE21B1CECBD4091ECF418A9857B3FE43AC2C23CCAE653426860A516CCC85D17739DCDADC1A81E4B423663878AAA9461E897D5E7F2B58CD041
Malicious:	**true**
Reputation:	low
Preview:	PK.....!.V.....[Content_Types].xml ...(..... .....U.n.0.}G..".....BM..C.....^|.x8.....v...&kTx.....{..e....jg+...V.....{V`.VI.,Tl...._.n... ...1..B`.B'.;...l\.d.ah...O..X,....6.1q....l..UO.w+....w.T..F.2. B.U..... r.....M.."...0.....N..l..7dsD!..w0.....&I}...ZAq-C.&;.F.Fd.9...F._.)...h....r..../VA?K.p...O...../.s....?.d.....S.v...K>].c...6.].r.CG...4O.4R....p...b.....M.t..c..8!..... D/d..Q.p.1f....n..0....}..>...d0S.....X...

C:\Users\user\Desktop\~$SRLTX-1266305223.xlsb	
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:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.829454136800251
TrID:	• Microsoft Excel Office Binary workbook document (40504/1) 83.51% • ZIP compressed archive (8000/1) 16.49%
File name:	SRLTX-1266305223.xlsb
File size:	99421

General

MD5:	9a33b86fa2ee2372023d418129238b25
SHA1:	d94101917d187df6bd710f2abf288cf9f2ee86c9
SHA256:	141a23ce14ba6702fdba9d074fe66eab9f9084be7030033b0258656942a3c660
SHA512:	28d7272b22f2745a1ee9dae5d904125cce3bd1e6fcd4e106cf2e32cf2be9b09198596f02043a03ce03158e9674dd4e80b91a706e7a35699cc7b6507f2acf0c9b
SSDEEP:	1536:cA/B5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsU/B:cAic6EehCfCZpUHKGXbBKsii+B
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 "SRLTX-1266305223.xlsb"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 7036 Parent PID: 744

General

Start time:	07:46:23
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:	0xfd0000
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: regsvr32.exe PID: 336 Parent PID: 7036

General

Start time:	07:47:31
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet1.ocx
Imagebase:	0x140000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 6812 Parent PID: 7036

General

Start time:	07:47:31
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet2.ocx
Imagebase:	0x140000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 1328 Parent PID: 7036

General

Start time:	07:47:33
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet3.ocx
Imagebase:	0x140000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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