ID: 532384
Sample Name: SRLTX-1266305223.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:37:14
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SRLTX-1266305223.xlsb 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
System Summary: 4
Jbx Signature Overview 4
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 12
General 12
File Icon 12
Static OLE Info 12
General 12
OLE File "SRLTX-1266305223.xlsb" 12
Indicators 12
Macro 4.0 Code 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 13
Code Manipulations 13
Statistics 13
Behavior 13
System Behavior 13
Analysis Process: EXCEL.EXE PID: 2244 Parent PID: 596 13
General 13
File Activities 13
File Created 13
File Deleted 13
File Written 13
File Read 13
Registry Activities 13
Key Created 14
Key Value Created 14
Analysis Process: regsvr32.exe PID: 1172 Parent PID: 2244 14
General 14
File Activities 14
Analysis Process: regsvr32.exe PID: 2092 Parent PID: 2244 14
General 14
File Activities 14
Analysis Process: regsvr32.exe PID: 2300 Parent PID: 2244 14
General 14
File Activities 15
Disassembly 15

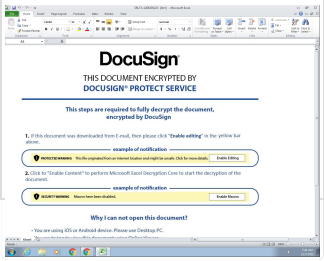
Windows Analysis Report SRLTX-1266305223.xlsb

Overview

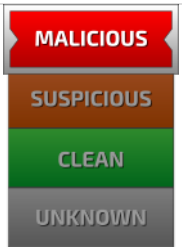
General Information

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

Most interesting Screenshot:



Detection



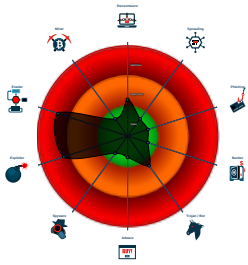
Hidden Macro 4.0

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…
- May sleep (evasive loops) to hinder …
- Tries to connect to HTTP servers, b…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2244 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1172 cmdline: regsvr32 C:\ProgramData\Volet1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2092 cmdline: regsvr32 C:\ProgramData\Volet2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2300 cmdline: regsvr32 C:\ProgramData\Volet3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

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

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

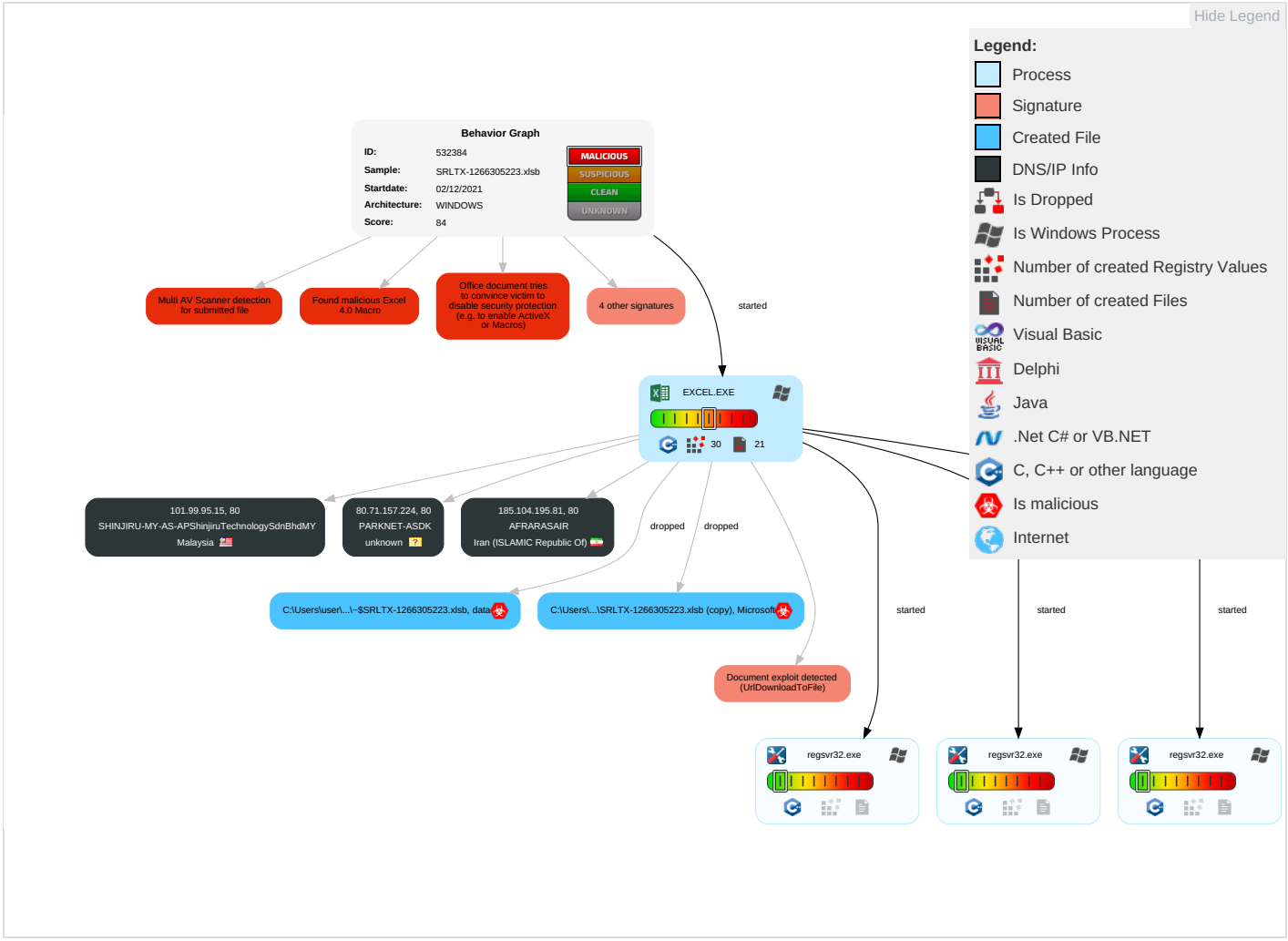
Found Excel 4.0 Macro with suspicious formulas

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
Valid Accounts	Scripting 3	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	Eavesdrop on Insecure Network Communicatior
Default Accounts	Exploitation for Client Execution 2 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 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	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	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 3	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatior
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

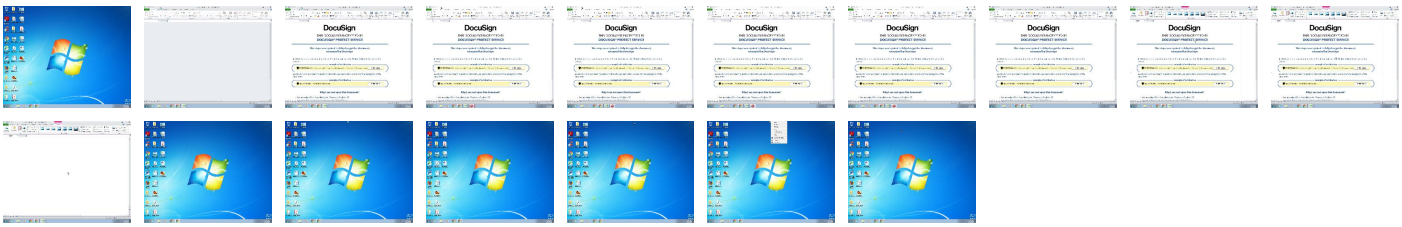
Behavior Graph

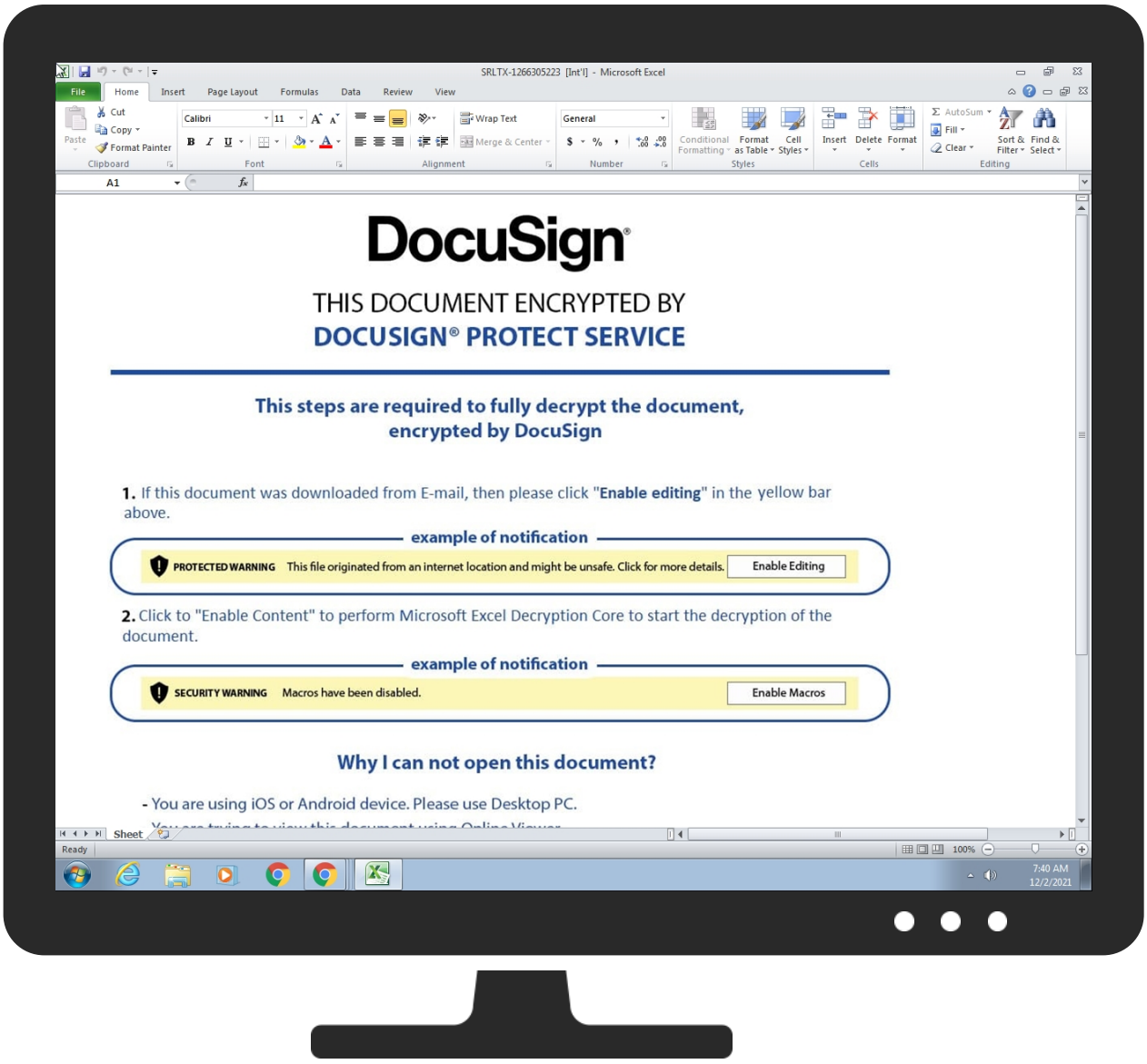


Screenshots

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://185.104.195.81/650918116841.datl	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://101.99.95.15/650918116841.datu	0%	Avira URL Cloud	safe	
http://101.99.95.15/650918116841.dat0	0%	Avira URL Cloud	safe	
http://185.104.195.81/650918116841.dat	0%	Avira URL Cloud	safe	
http://80.71.157.224/650918116841.dat	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://101.99.95.15/650918116841.dat	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://80.71.157.224/650918116841.dat$	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	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:	07:37:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SRLTX-1266305223.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
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@7/5@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 • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:40:30	API Interceptor	3x Sleep call for process: regsvr32.exe modified

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-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-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-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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 111.90.158.95
PARKNET-ASDK	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
	F2433DFBA69148A0C3A5A5951D360B6C3C045090 DE06F.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-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\Windows\Temporary Internet Files\Content.MSO\E5B98A58.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E5B98A58.jpg	
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\11750000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	99173
Entropy (8bit):	7.829749204687144
Encrypted:	false
SSDEEP:	1536:IIB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsULkFKJ:I3c6EehCfCZpUHKGXbBKsiiJgJ
MD5:	C827763DB12655106D4C2A35D67B6142
SHA1:	E9BC340F643F9D8372D27F7D53848CD5AA6B92F1
SHA-256:	A1B5A84C413D1C25DBEF36E0E0EF2D2837D7D94398B985279BE932A31B6B186B
SHA-512:	11179E2DA1D3C7BBB1E2FFA5D608693FD28014990599D2C3581B8F023C59A094FF3330089C3E25B60F1D8A329EFAAB216FEA5FAEC562FA4717761A3B64870950
Malicious:	false
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....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\11750000:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
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\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	99173
Entropy (8bit):	7.829749204687144
Encrypted:	false
SSDEEP:	1536:IIB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsULkFKJ:I3c6EehCfCZpUHKGXbBKsiiJgJ
MD5:	C827763DB12655106D4C2A35D67B6142
SHA1:	E9BC340F643F9D8372D27F7D53848CD5AA6B92F1
SHA-256:	A1B5A84C413D1C25DBEF36E0E0EF2D2837D7D94398B985279BE932A31B6B186B
SHA-512:	11179E2DA1D3C7BBB1E2FFA5D608693FD28014990599D2C3581B8F023C59A094FF3330089C3E25B60F1D8A329EFAAB216FEA5FAEC562FA4717761A3B64870950
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....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\~$SRLTX-1266305223.xlsb	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data

C:\Users\user\Desktop\~$SRLTX-1266305223.xlsb	
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58[
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.829454136800251
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
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:	e4e2ea8aa4b4b4b4

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

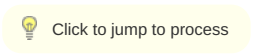
Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2244 Parent PID: 596

General

Start time:	07:38:11
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:	0x13f880000
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 Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 1172 Parent PID: 2244

General

Start time:	07:40:20
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 C:\ProgramData\Volet1.ocx
Imagebase:	0xff340000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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: 2092 Parent PID: 2244

General

Start time:	07:40:21
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 C:\ProgramData\Volet2.ocx
Imagebase:	0xff340000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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: 2300 Parent PID: 2244

General

Start time:	07:40:21
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 C:\ProgramData\Volet3.ocx
Imagebase:	0xff340000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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