



ID: 356276
Sample Name: document-550193913.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:35:25
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report document-550193913.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
System Summary: 5
Signature Overview 5
AV Detection: 5
Compliance: 5
Software Vulnerabilities: 5
System Summary: 5
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
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 8
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 14
General 14
File Icon 15
Static OLE Info 15
General 15
OLE File "document-550193913.xls" 15
Indicators 15
Summary 15
Document Summary 15
Streams 16
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 16
General 16
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 16
General 16

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 83101 16
General 16
Macro 4.0 Code 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 17
UDP Packets 17
DNS Queries 17
DNS Answers 17
HTTPS Packets 18
Code Manipulations 18
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: EXCEL.EXE PID: 2404 Parent PID: 584 18
General 18
File Activities 19
File Created 19
File Deleted 19
File Moved 20
File Written 20
File Read 27
Registry Activities 27
Key Created 27
Key Value Created 28
Analysis Process: rundll32.exe PID: 2560 Parent PID: 2404 35
General 35
File Activities 36
Disassembly 36
Code Analysis 36

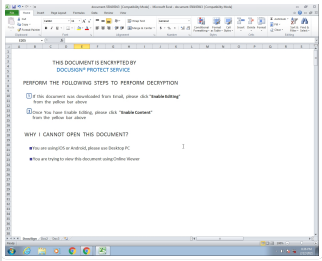
Analysis Report document-550193913.xls

Overview

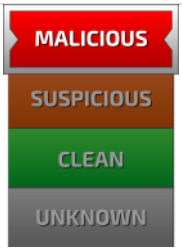
General Information

Sample Name:	document-550193913.xls
Analysis ID:	356276
MD5:	4107cd071635b4..
SHA1:	cf6dea64431b614.
SHA256:	d49b40d468269f5.
Tags:	bokbot, IcedID, macros, xls

Most interesting Screenshot:



Detection



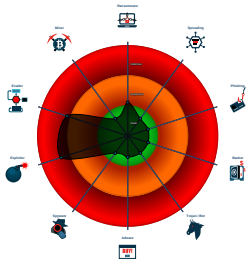
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Yara signature match

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2404 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2560 cmdline: rundll32 ..\rieuro.vnt,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

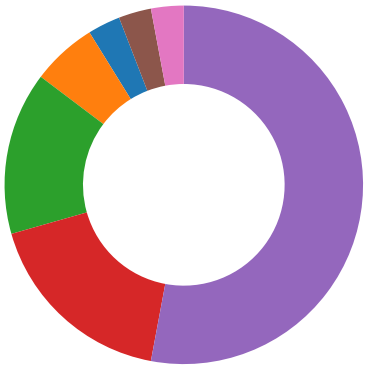
Source	Rule	Description	Author	Strings
document-550193913.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x11dab:$e1: Enable Editing • 0x11e20:$e2: Enable Content
document-550193913.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x148a2:$s1: Excel • 0x15906:$s1: Excel • 0x3802:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 00 01 3A
document-550193913.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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

HIPS / PFW / Operating System Protection Evasion:

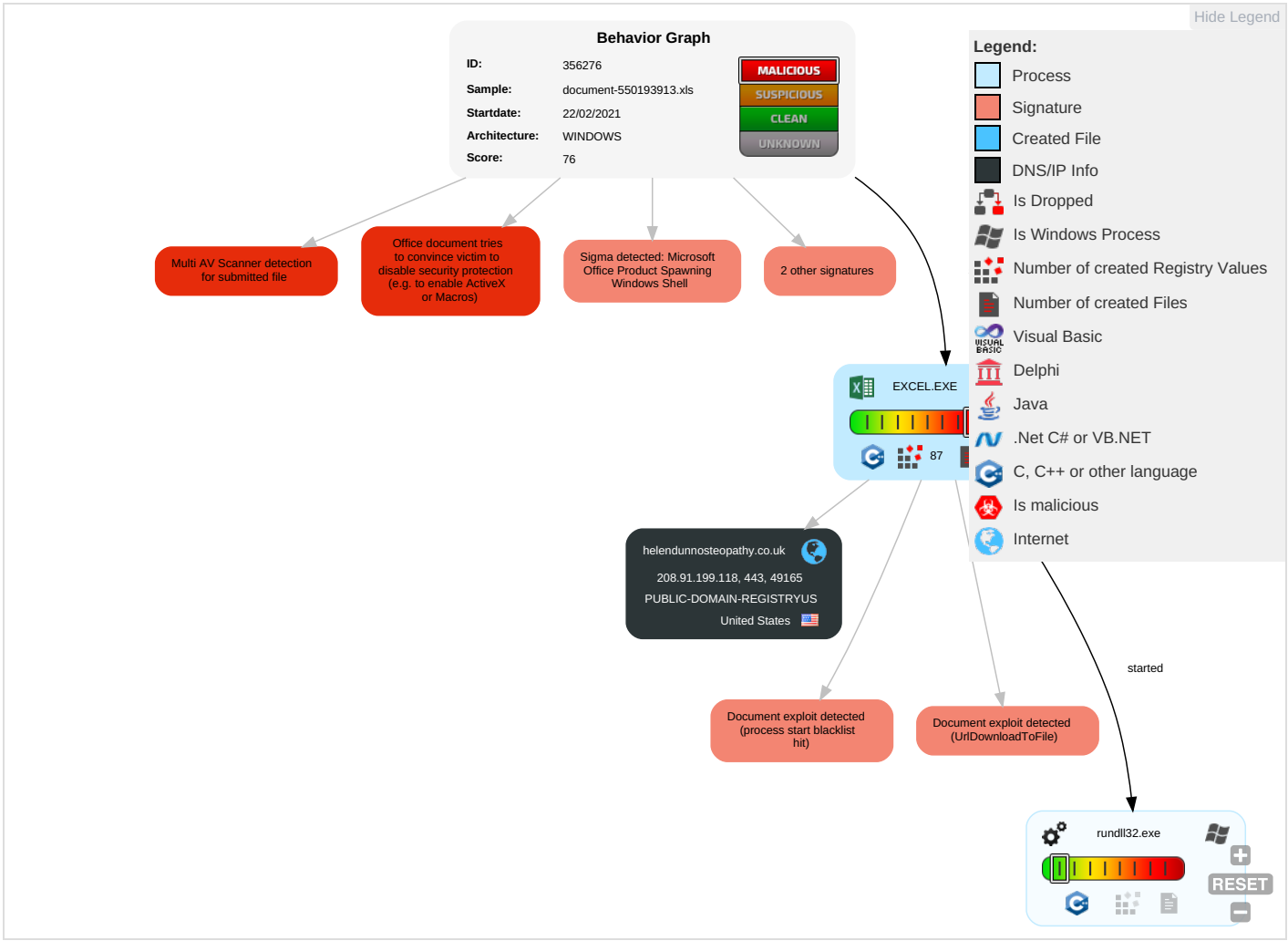
Yara detected hidden Macro 4.0 in Excel

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	Im
Valid Accounts	Scripting 1 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

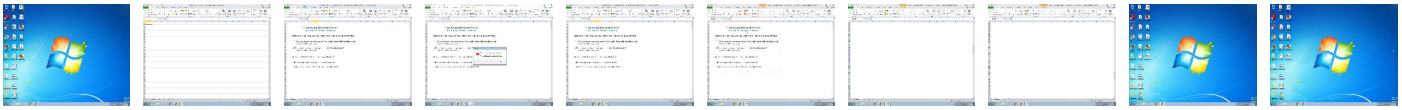
Behavior Graph



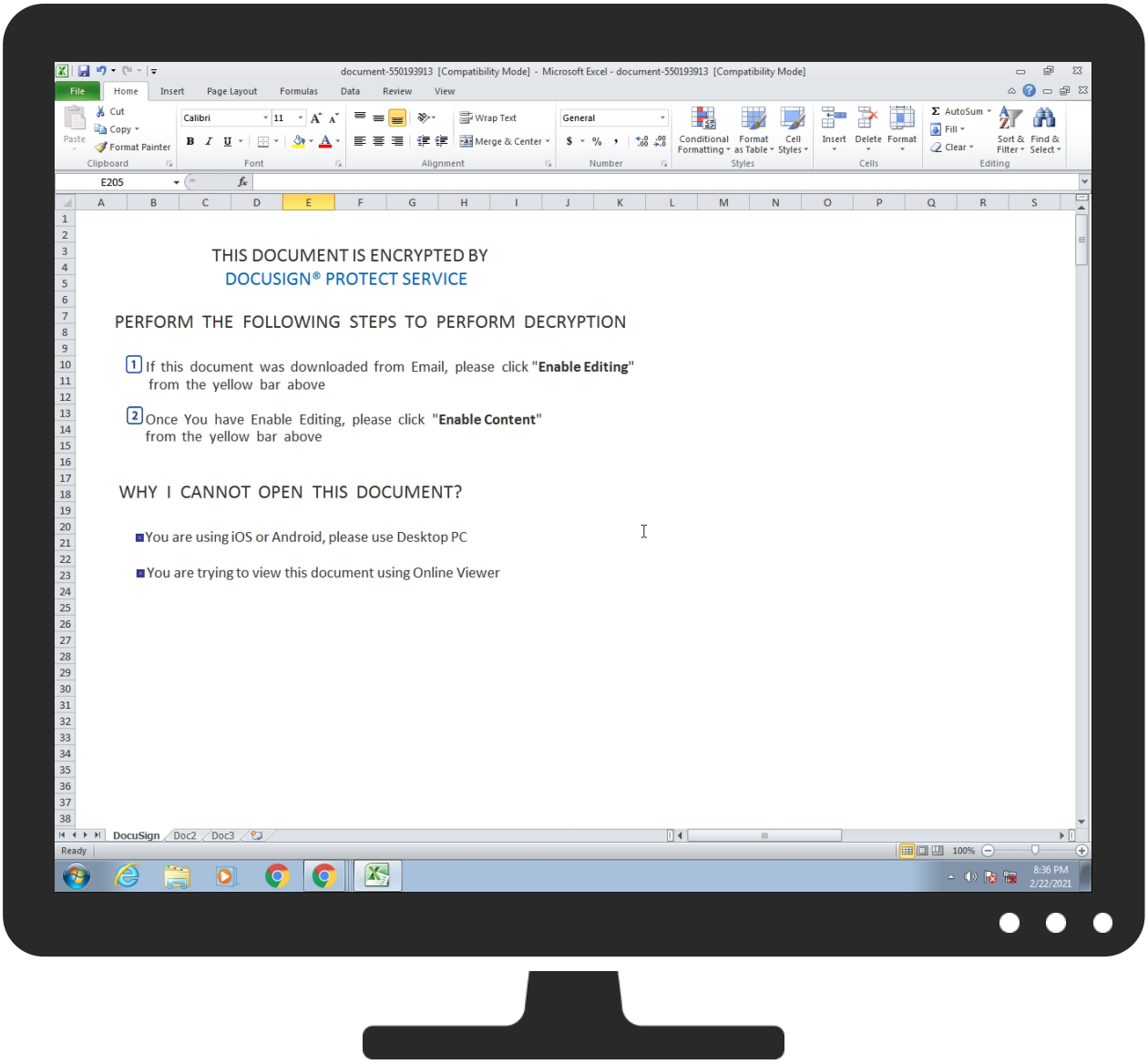
Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
document-550193913.xls	10%	Virustotal		Browse
document-550193913.xls	6%	ReversingLabs	Document-Excel.Exploit.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
helendunnosteopathy.co.uk	1%	Virustotal		Browse

Copyright null 2021

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	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	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://helendunnosteopathy.co.uk/ds/2202.gif	2%	Virustotal		Browse
http://https://helendunnosteopathy.co.uk/ds/2202.gif	0%	Avira URL Cloud	safe	

Domains and IPs

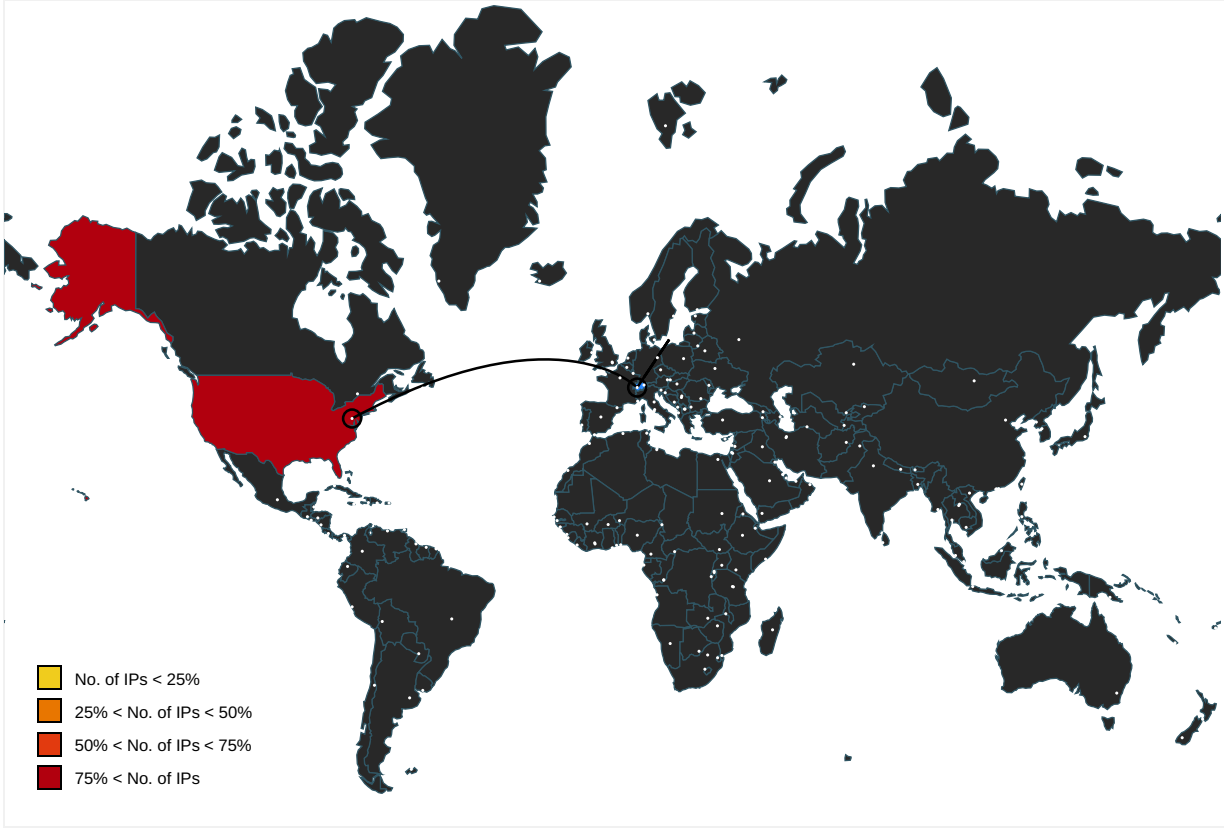
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
helendunnosteopathy.co.uk	208.91.199.118	true	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2102081381.0000000001DF7000. 00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000003.0000000 2.2101861194.0000000001C10000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2101861194.0000000001C10000. 00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2101861194.0000000001C10000. 00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2102081381.0000000001DF7000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2102081381.0000000001DF7000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2101861194.0000000001C10000. 00000002.00000001.sdmp	false		high
http://https://helendunnosteopathy.co.uk/ds/2202.gif	document-550193913.xls	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2101861194.0000000001C10000. 00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.118	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356276
Start date:	22.02.2021
Start time:	20:35:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-550193913.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	mal76.expl.evad.winXLS@3/11@1/1
EGA Information:	Failed

Copyright null 2021

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: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 192.35.177.64, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	SecuriteInfo.com.Trojan.Packed2.42850.3598.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.Inject4.6572.1879.exe	Get hash	malicious	Browse	• 208.91.199.224
	ffkjg5CVrO.exe	Get hash	malicious	Browse	• 208.91.199.223
	7Lf8J7h7os.exe	Get hash	malicious	Browse	• 208.91.199.223
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	YKRAB010B_KHE_Preminary Packing List.xlsx.exe	Get hash	malicious	Browse	• 208.91.199.225
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	• 208.91.198.143
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	• 208.91.199.223
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	• 208.91.199.223
	PAYMENT INVOICE-9876543456789.exe	Get hash	malicious	Browse	• 208.91.199.224
	SecuriteInfo.com.Artemis249E62CF9BAE.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Exploit.Siggen3.10204.3307.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-573042818.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-573042818.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-573042818.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-750895311.xls	Get hash	malicious	Browse	• 103.50.162.157

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	19_02_2021.exe	Get hash	malicious	Browse	• 111.118.215.254
	inquiry.doc	Get hash	malicious	Browse	• 208.91.199.224
	SecuriteInfo.com.Artemis1A08A3826D57.exe	Get hash	malicious	Browse	• 208.91.199.225
	BL COPY.exe	Get hash	malicious	Browse	• 208.91.198.143

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	document-1915351743.xls	Get hash	malicious	Browse	• 208.91.199.118
	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	• 208.91.199.118
	Subconract 504.xlsm	Get hash	malicious	Browse	• 208.91.199.118
	upbck.xlsx	Get hash	malicious	Browse	• 208.91.199.118
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 208.91.199.118
	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• 208.91.199.118
	_a6590.docx	Get hash	malicious	Browse	• 208.91.199.118
	Small Charities.xlsx	Get hash	malicious	Browse	• 208.91.199.118
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• 208.91.199.118
	notice of arrival.xlsx	Get hash	malicious	Browse	• 208.91.199.118
	22-2-2021 .xlsx	Get hash	malicious	Browse	• 208.91.199.118
	Shipping_Document.xlsx	Get hash	malicious	Browse	• 208.91.199.118
	Remittance copy.xlsx	Get hash	malicious	Browse	• 208.91.199.118
	CI + PL.xlsx	Get hash	malicious	Browse	• 208.91.199.118
	RFQ_Enquiry_0002379_.xlsx	Get hash	malicious	Browse	• 208.91.199.118
	124992436.docx	Get hash	malicious	Browse	• 208.91.199.118
	document-1900770373.xls	Get hash	malicious	Browse	• 208.91.199.118
	AswpCUetE0.doc	Get hash	malicious	Browse	• 208.91.199.118
	EIY2otZ3r8.doc	Get hash	malicious	Browse	• 208.91.199.118
	Invoice.ppt	Get hash	malicious	Browse	• 208.91.199.118

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....l.l6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....l.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..l..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U.....0...U.....{.q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0824531991978708
Encrypted:	false
SSDEEP:	6:kK1c4wPbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:m1W3kPlE99SNxAhUeo+aKt
MD5:	9112B408D189084239739EAE8118F62F
SHA1:	7EE8197E23024152C459FF68ACB000A7D888612D
SHA-256:	ADA71E0ADDC1FF4AA299127CB136914DDD6CD69AAF84E72DB0500A6D804F0D8B
SHA-512:	7979D21F8E899121443AFE0D5E886118D70ADCC91B6B2CFD2258BFA41F4C353EBEA4F625180DB160910E879A696C892372D06E9E64E4C9AAB9AF086788B5548
Malicious:	false
Reputation:	low
Preview:	p..... ....."Y....(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0139867481437155
Encrypted:	false
SSDEEP:	3:kkFklf9kkltfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKOfnliBAIdQZV7eAYLit
MD5:	28DE676481E9713D8E60012F0719B676
SHA1:	856C4FD41D44EA9190C5F4ACCF9C919807CEB35C
SHA-256:	465AC91E180F9C6C74EC1C28D3C4C9951CE6585D98AE41C8AF87CE2B53487B84
SHA-512:	01DF566B09975FD427F2741736CE66EF52620AE29885EF110605683556B6F079E795321F0D24701C6218C9B633852C06D319A36AFDAD6B281EA451F581AA0103
Malicious:	false
Reputation:	low
Preview:	p..... ....`...c..X....(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Temp\CBDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	65280
Entropy (8bit):	7.696599199500836
Encrypted:	false
SSDEEP:	1536:wqcJEaiqSiBjAdwroSgiB9uCbMljf2fu9X9bGi2vK6WXfkb:wqGEySOjVuiTuColjf2faNbov/WMb
MD5:	58B024C10F6E73A5C26740D81ED61038
SHA1:	A24C2DDFBA84AD9207CCD1C5EC9D4AC075C10E54
SHA-256:	9DBE7F8D59B5C7BCD3F42DE2312DEB325F88E2AE6E2D425A91CB2E1BA167C4C2
SHA-512:	4E8CA43AF7C1E10C67963AA081A2957150083FA5874995954898019F423EADE99672FA85262414B2F9BAED139DBF81FAF9C79F00EE1685DCCD3CFD3A576307B1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\CBDE0000	
Preview:	..N.0...W..".....j.....$....4..?....q..P...J.4m.s.7.t<.\.]<c....U.V..N*.....o...1.....1.....c,Hmc...o.h.@..GK+...$....A,.A~>.\p.IB..=.I....Sq.....o.V\m..Q5S&..}.S1WvK..k% Qi...-..-.J.t...L .}@..ELFW>(b.....''~..P..B.>T...b.|<.f}..W...mU..60(....t....W.....;.....X.J....+.''.k.s.....I.w..OD..I..F..3...{..?.i.....2.7`.e..S...?..#...y...7.....%..P.'.....z.p../..._....h$W..W-M.#7...O3 ..8.. .x8.....p..f.H.....1'Q...:.....PK.....!...l.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabE5AF.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&. [<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a.,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r.. I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\TarE5B0.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..210115004237Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue Feb 23 03:35:41 2021, atime=Tue Feb 23 03:35:41 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.485120499512926
Encrypted:	false
SSDEEP:	12:85QZ3WHcLgXg/XAlCPCHaXtB8XzB/0kiX+WnicvbkGeObDtZ3YilMMEpxRljKtTg:85wGq/XTd6j4Ye3eCDv3qwrNru/
MD5:	5716FCBCF49473B7E0DA6C6C0C4532E7
SHA1:	2B40EB010C5F7323D577A1DA37964FD1D46BCF96
SHA-256:	4C386546A9B805DCB2585CEADA06D1E92587182E13F3D0599AC30C10E133FF40
SHA-512:	C2025D5B84DDF8D232FEDE497CF7706AD019C9B24604DA7F344BC7598D18E8CD4FB4556C2289E74C5A75891116A801026B4DE0E4566944364DFEDE17E565E3D
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G.....W.....W..... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....WRu$..Desktop.d.....QK.XWRu$*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\899552\Users.user\Desktop.....\.....\.....\.....\.....\D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....899552.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-550193913.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:16 2020, mtime=Tue Feb 23 03:35:41 2021, atime=Tue Feb 23 03:35:41 2021, length=93184, window=hide
Category:	dropped
Size (bytes):	2108
Entropy (8bit):	4.528033883396002
Encrypted:	false
SSDEEP:	48:8Za/XT0jqOAjMCsSwQh2Za/XT0jqOAjMCsSwQ/:8Za/XojqOABwQh2Za/XojqOABwQ/
MD5:	63FCE306E198EA4256E660312C9938A2
SHA1:	ED457BEBEE3B0300C50E372D914024B3B814D9B9
SHA-256:	2786F3CC08E726B768C679676BA391D2C3FEC85315D271B8FA71108EDA611041
SHA-512:	49DCE70DEA6A90A1A083DD4BA7566043E32D62059FACDBE1EB8F43F8C997E6380F516F871C6649B631F7A16CE37D6F528CF28D0F9AA5A5540A81D67EB225EB 1
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....(...{.....W....cO.W.....l.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2 .1.7.6.9.....v.2..n..WRr$ .DOCUME~1.XLS..Z.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.5.5.0.1.9.3.9.1.3...x.l.s.....-...8...[.....?J.....C:\Users\..#..... .....\\899552\Users.user\Desktop\document-550193913.xls.-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.5.5.0.1.9.3.9.1.3...x.l.s.....:.,.LB.)...Ag.....1S PS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....899552.....D_....3N...W..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	107
Entropy (8bit):	4.704136640648724
Encrypted:	false
SSDEEP:	3:oyBVomMY9LRzcWl2ulZELRzcWl2ulmMY9LRzcWl2ulv:dj6Y9LVl1ELVlPY9LVlL
MD5:	59D6E0A6C21A61366968A28C51B556C3
SHA1:	49C4F33DF0D414B6C8B50FE89D9AA393E44F207D
SHA-256:	540F24527642B86B694E23E030BA76E54DDE40B7862F356D9E284A6A232FC0A2
SHA-512:	A1DF2037139ABADB3EF4067A28C9E7272BA61224F2A8589D440586B7B945EB5BBAF2D9DF3DB53611B373AF0DD9BA6020DF865F0FBE7CD9C8D94988F13E2022 3
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-550193913.LNK=0..document-550193913.LNK=0..[xls]..document-550193913.LNK=0..

C:\Users\user\Desktop\ACDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	143400
Entropy (8bit):	4.4844677313630505
Encrypted:	false
SSDEEP:	3072:oJxEtjPOtioVjDGUU1qfDlaGGx+cL2QnAFV1XU8mJxEtjPOtioVjDGUU1qfDlaGh:ixEtjPOtioVjDGUU1qfDlavx+W2QnAFi
MD5:	3BFBAD31205430D69DB51B2F5130C358
SHA1:	07777FAAFE7F2071CA21026BD1C563A2E538DA87
SHA-256:	03B7624902D8B7BFCBFB1D4E1743A710D325169DDB263D3C03A6EF8795DE861C
SHA-512:	768FBB51D44CA2975199171CA673B3480722E0613399C58B3FDD76FEDB41862EC16D725F2C40FC03E388F4A19EDB036D32A09C96955505B615BFFDCF60CBB3B
Malicious:	false
Preview:	.....g2.....\.p.... B.....a.....=.....=.....i..9J.8.....X.@.. ....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.. .....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b .r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C .a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

Static File Info

General

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Mon Feb 22 11:59:11 2021, Security: 0
Entropy (8bit):	3.4738983608957428
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-550193913.xls
File size:	93696
MD5:	4107cd071635b4cc3689f77c688f57c3
SHA1:	cf6dea64431b614757906f32d3d1f016b5afdbb5
SHA256:	d49b40d468269f57fb87ea6ad7fd8bb303fbeb033dbd45fb 4967c34c5dfbc2ed
SHA512:	ae568d93ef0c9cea430e18bdf5a27cb5e71fe2e13cfca9c 508f196aead42d7a1e68dd863587a0549391b7c08af85de 9e6db574c9d819422482ed6529df52c0fb
SSDEEP:	1536:ca7uDphYHceXVhca+fMHLtyeGxcl8O9pTINXUO mRwb05SXw1OTsRKvoNGrEJq7TT:ca7uDphYHceXVh ca+fMHLtyeGxcl8O9m
File Content Preview:	.....>..... ....

File Icon



Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-550193913.xls"

Indicators

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

Summary

Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-22 11:59:11
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

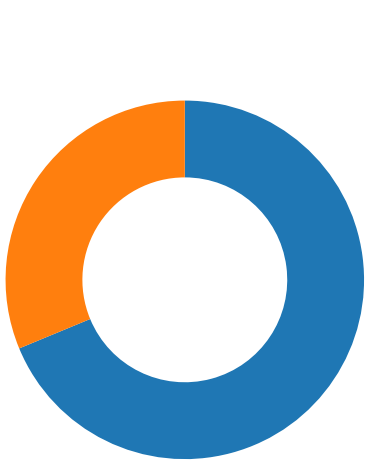
General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.337819969156
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . D o c 2 . . . . . D o c 3 . . . . . D o c 1 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 a8 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.250492291218
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . ! . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 83101

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	83101
Entropy:	3.68114146554
Base64 Encoded:	True
Data ASCII:	. . . . . g 2 . . . . . \\ . p . . . . B . . . . . a . . . . . = ... = ... i . . J . 8 . . . . . X . @ . . . . . " . . . . .
Data Raw:	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 00 20 20 20



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:36:20.178004026 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:20.354383945 CET	443	49165	208.91.199.118	192.168.2.22
Feb 22, 2021 20:36:20.354538918 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:20.377919912 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:20.552006006 CET	443	49165	208.91.199.118	192.168.2.22
Feb 22, 2021 20:36:20.559294939 CET	443	49165	208.91.199.118	192.168.2.22
Feb 22, 2021 20:36:20.559331894 CET	443	49165	208.91.199.118	192.168.2.22
Feb 22, 2021 20:36:20.559365988 CET	443	49165	208.91.199.118	192.168.2.22
Feb 22, 2021 20:36:20.559446096 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:20.559478998 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:20.597441912 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:20.768651009 CET	443	49165	208.91.199.118	192.168.2.22
Feb 22, 2021 20:36:20.768876076 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:22.337011099 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:22.552406073 CET	443	49165	208.91.199.118	192.168.2.22
Feb 22, 2021 20:36:22.809874058 CET	443	49165	208.91.199.118	192.168.2.22
Feb 22, 2021 20:36:22.809968948 CET	443	49165	208.91.199.118	192.168.2.22
Feb 22, 2021 20:36:22.810028076 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:22.810611963 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:22.810627937 CET	49165	443	192.168.2.22	208.91.199.118
Feb 22, 2021 20:36:22.976635933 CET	443	49165	208.91.199.118	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:36:20.104002953 CET	52197	53	192.168.2.22	8.8.8.8
Feb 22, 2021 20:36:20.164762974 CET	53	52197	8.8.8.8	192.168.2.22
Feb 22, 2021 20:36:21.079830885 CET	53099	53	192.168.2.22	8.8.8.8
Feb 22, 2021 20:36:21.139955044 CET	53	53099	8.8.8.8	192.168.2.22
Feb 22, 2021 20:36:21.163115978 CET	52838	53	192.168.2.22	8.8.8.8
Feb 22, 2021 20:36:21.212127924 CET	53	52838	8.8.8.8	192.168.2.22
Feb 22, 2021 20:36:21.754522085 CET	61200	53	192.168.2.22	8.8.8.8
Feb 22, 2021 20:36:21.815949917 CET	53	61200	8.8.8.8	192.168.2.22
Feb 22, 2021 20:36:21.829842091 CET	49548	53	192.168.2.22	8.8.8.8
Feb 22, 2021 20:36:21.896408081 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 20:36:20.104002953 CET	192.168.2.22	8.8.8.8	0xb648	Standard query (0)	helendunno steopathy.co.uk	A (IP address)	IN (0x0001)

DNS Answers

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 20:36:20.164762974 CET	8.8.8.8	192.168.2.22	0xb648	No error (0)	helendunno steopathy.co.uk		208.91.199.118	A (IP address)	IN (0x0001)

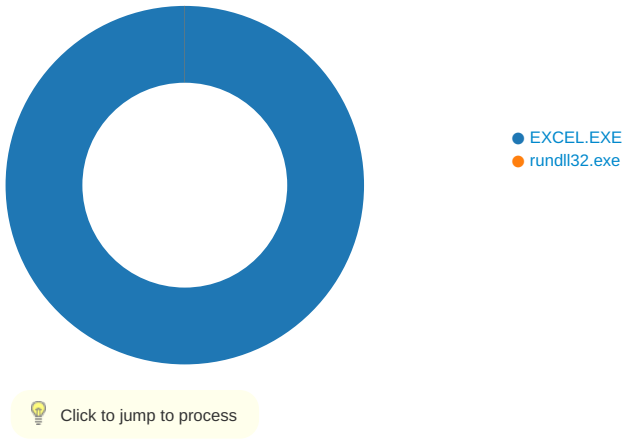
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 20:36:20.559365988 CET	208.91.199.118	443	192.168.2.22	49165	CN=cpcalendars.helendunnosteopathy.co.uk CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 30 12:12:51 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Apr 30 13:12:51 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2404 Parent PID: 584

General

Start time:	20:35:39
Start date:	22/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding

Copyright null 2021

Imagebase:	0x13fe00000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DAD5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14014EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\CBDE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B2828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B2828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B2828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B2828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B2828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B2828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B2828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B2828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B2828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\7AAF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14014EC83	GetTempFileNameW

File Deleted

Copyright null 2021

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DAD5.tmp	success or wait	1	1403BB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image007.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\7AAF.tmp	success or wait	1	1403BB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CBDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\ACDE0000	C:\Users\user\Desktop\document-550193913.xls.	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image007.png	C:\Users\user\AppData\Local\Temp\imgs_files\image007.pn~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image008.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image008.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image009.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image009.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CBDE0000	569	463	c4 95 dd 4e e3 30 10 85 ef 57 e2 1d 22 df a2 c4 85 95 d0 6a d5 94 0b 96 bd 04 24 e0 01 a6 f6 34 b1 ea 3f d9 06 da b7 df 71 1a b2 50 95 86 8a 4a dc 34 6d 9c 73 ce 37 e3 74 3c bd 5c 19 5d 3c 63 88 ca d9 9a 9d 55 13 56 a0 15 4e 2a db d4 ec f1 e1 6f f9 8b 15 31 81 95 a0 9d c5 9a ad 31 b2 cb d9 c9 8f e9 c3 da 63 2c 48 6d 63 cd da 94 fc 6f ce a3 68 d1 40 ac 9c 47 4b 2b 0b 17 0c 24 fa 19 1a ee 41 2c a1 41 7e 3e 99 5c 70 e1 6c 42 9b ca 94 3d d8 6c fa 07 17 f0 a4 53 71 bd a2 db 1b 12 6f 1b 56 5c 6d 9e cb 51 35 53 26 eb f3 7d be 53 31 57 76 4b 01 de 6b 25 20 51 69 fc d9 ca 2d ac d2 2d 16 4a a0 74 e2 c9 10 4c 15 7d 40 90 b1 45 4c 46 57 3e 28 62 0c f7 98 12 b5 22 7e 90 19 50 c7 c3 42 fb 3e 54 a4 ec c0 62 ab 7c 3c a5 66 7d 90 90 57 de f7 e1 6d 55 bd ee 96 36 30 28 89	...N.0...W.."......j.....$... .4..?.....q..P...J.4m.s.7.t<.\.] <c.....U.V..N*.....o...1.... ...1.....c,Hmc....o..h.@..G K+...$....A,.A~>.\p.lB...=.l.. ...Sq.....o.V\m..Q5S&..}.S1 WvK..k% Qi...-..- .J.t...L.}@..ELFW> (b....."~..P..B.>T...b.|<.f} ..W...mU...60(.	success or wait	30	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\CBDE0000	1032	2	03 00	..	success or wait	19	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\CBDE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 a1 83 6c 9f d1 01 00 00 97 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CBDE0000	60361	677	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1e 08 02 00 00 00 b4 52 39 f5 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 12 74 00 00 12 74 01 de 66 1f 78 00 00 02 4a 49 44 41 54 48 4b 63 fc ff ff 3f 03 03 c3 83 67 1f 17 6c bf 3b 6b fd 15 06 46 46 06 86 ff 40 48 1a 00 6a 62 60 64 f8 ff 3f 2d 50 27 c1 53 59 41 8a 1f c4 07 1a bd 66 d7 cd 9a b9 e7 bf fc e1 fc ff f7 27 c3 bf 3f a4 19 8a ac 9a 89 85 91 99 9d 87 e5 7b 4b 8a 61 88 ab 3a e3 d3 57 9f 9d 73 b6 7e fe cd c6 fc ff 7b b0 83 bc 97 a5 3c 0b 0b d3 bf 7f a4 39 9b 89 89 f1 ef df 7f 5b 8f 3d 5c 7b e0 e1 5f 46 4e 5e b6 5f 7b 27 7b 33 56 4d 3f be 70 f7 0b 76 a6 5f bd b9 a6 01 76 8a e4 3b 19 ac 73 c3 a1 fb c5 93 4f ff fc c7 16 ef 2a c1 7c 87 c1 0e 18 be a1 0e d2 79	.PNG........IHDR..... R9.....sRGB.....pHYs...t.. .t..f.x...JIDATHKc...?....g..l .;k...FF...@H..jb`d..?- P'.SYA.....f.....'..?..... ...{K.a..:..W..s.~.....{.....< .....9.....[.=\{..._FN^._{'{ 3VM?.p..v._....v..;..s.....O.. ...*.|.....y	success or wait	2	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\CBDE0000	63808	1472	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 a1 83 6c 9f d1 01 00 00 97 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 2d f3 92 7c 4e 01 00 00 e5 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 80 8a 1a 89 b9 01 00 00 25 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 be 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!...l..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.-..|N..... .....0...xl/_rels/wor kbook.xml.relsPK..-.....!. .....%..... xl/workbook.xml	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ACDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 00 20 20 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ACDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ACDE0000	unknown	974	02 04 00 00 00 2c 01 81 00 02 00 c1 04 14 00 00 00 15 00 00 00 83 00 02 00 00 00 84 00 02 00 00 00 26 00 08 00 66 66 66 66 66 66 66 e6 3f 27 00 08 00 66 66 66 66 66 66 e6 3f 28 00 08 00 00 00 00 00 00 00 e8 3f 29 00 08 00 00 00 00 00 00 00 e8 3f a1 00 22 00 00 00 2c 01 01 00 01 00 01 00 04 00 02 00 01 ff 33 33 33 33 33 33 d3 3f 33 33 33 33 33 33 d3 3f 0f 00 9c 08 26 00 9c 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 33 00 00 00 00 00 00 00 00 55 00 02 00 08 00 00 02 0e 00 60 00 00 00 6d 00 00 00 00 00 02 00 00 00 08 02 10 00 60 00 00 00 02 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 61 00 00 00 02 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 62 00 00 00 02 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 63 00 00 00 02 00	.....,..... ...&....ffffff.?'...ffffff.?(.. .....?).....?.."..... .....333333.? 333333.?... .&..... <3.....U.....`...m.... .....`.....,.....a .....,.....b.....,.... .....c.....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\ACDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 00 20 20 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ACDE0000	unknown	200	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 80 8c 4e 57 9d 09 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....T.....`..... ..x..... ....Microsoft Excel.@.....|.#... @.....NW.....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\ACDE0000	unknown	284	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 ec 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 a8 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 05 00 00 00 44 6f 63 32 00 05 00 00 00 44 6f 63 33 00 05 00 00 00 44 6f 63 31 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 03 00 00 00 1e 00 00 00	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign.....Doc2.....Doc3 .... .Doc1.....Workshee ts.....	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ACDE0000	unknown	1536	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!...''...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\ACDE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 b4 00 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 b2 00 00 00 b3 00 00 00 ff ff ff

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDAF4	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDC4B	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD06	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7BE4	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7DC7	success or wait	1	7FEEAA29AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAA29AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDAF4	EDAF4	binary	04 00 00 00 64 09 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 36 00 2E 00 32 00 38 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 D0 EE E5 53 9D 09 D7 01 F4 DA 0E 00 F4 DA 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAA29AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDC4B	EDC4B	binary	04 00 00 00 64 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 7F 5D AC 57 9D 09 D7 01 4B DC 0E 00 4B DC 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD06	EDD06	binary	04 00 00 00 64 09 00 00 2D 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 35 00 35 00 30 00 31 00 39 00 33 00 39 00 31 00 33 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 63 4F CB 57 9D 09 D7 01 06 DD 0E 00 06 DD 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7BE4	F7BE4	binary	04 00 00 00 64 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 AC 52 EC 6F 9D 09 D7 01 E4 7B 0F 00 E4 7B 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAA29AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7DC7	F7DC7	binary	04 00 00 00 64 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 AC 52 EC 6F 9D 09 D7 01 C7 7D 0F 00 C7 7D 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00

Wow64 process (32bit):	false
Commandline:	rundll32 ..\rieuro.vnt,DllRegisterServer
Imagebase:	0xffdb0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis